FUNDAÇÃO UNIVERSIDADE FEDERAL DO PAMPA
CAMPUS SANTANA DO LIVRAMENTO
BACHARELADO EM RELAÇÕES INTERNACIONAIS

JÚLIA GOMES LANZETTA

CIBERESPAÇO E O SISTEMA INTERNACIONAL: UMA ANÁLISE DA SEGURANÇA CIBERNÉTICA DO ESTADO

Santana do Livramento

2022

JÚLIA GOMES LANZETTA

CIBERESPAÇO E O SISTEMA INTERNACIONAL: UMA ANÁLISE DA SEGURANÇA CIBERNÉTICA DO ESTADO

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais pela Universidade Federal do Pampa - UNIPAMPA.

Orientador: Prof. Dr. Renato José da Costa.

Santana do Livramento

2022

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

LL297cc Lanzetta, Júlia Gomes
Ciberespaço e o Sistema Internacional: Uma análise da Segurança Cibernética do Estado / Júlia Gomes Lanzetta.
82 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, RELAÇÕES INTERNACIONAIS, 2022.
"Orientação: Renato José da Costa".

1. Ciberespaço. 2. Sistema Internacional. 3. Segurança Cibernética. 4. Capacidade. 5. Vulnerabilidade. I. Título.

JÚLIA GOMES LANZETTA

CIBERESPAÇO E O SISTEMA INTERNACIONAL: UMA ANÁLISE DA SEGURANÇA CIBERNÉTICA DO ESTADO

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do título de Bacharel em Relações Internacionais pela Universidade Federal do Pampa - UNIPAMPA.

Trabalho de Conclusão de Curso defendido e aprovado em: 18 de janeiro de 2023.

Banca examinadora:

_____

Prof. Dr. Renato José da Costa
Orientador
(UNIPAMPA)

_____

Prof. Dr. Flávio Augusto Lira Nascimento
(UNIPAMPA)

_____

Profa. Dra. Kamilla Raquel Rizzi
(UNIPAMPA)

Dedico este trabalho aos meus pais que sempre me incentivaram a estudar e me deram coragem para ser quem sou hoje.

AGRADECIMENTOS

Agradeço a minha família por sempre ter me incentivado aos estudos. Obrigada pai e mãe, sou muito grata por acreditarem nas minhas ideias e me ajudarem a buscar o que acredito ser meu caminho. Aos meus irmãos, Felippe e Henrique, agradeço por existirem, isso já torna meus dias mais leves, e por escutarem as minhas opiniões sempre (mesmo que não concordem). Gostaria de agradecer as minhas amigas e amigo que deixei em Santa Luzia quando decidi me mudar. Vitória, Luíza, Bruna, Kelbert, vocês me acompanharam em toda a minha jornada de estudos quando estiveram por perto e em cada momento com vocês fui feliz. Aos novos amigos que vieram: Ana Maria, Anna Paula, Bruno, Manoela, Marcela e Juliana; vocês me acolheram e tornaram meus momentos mais fáceis. Vítor, obrigada pelo carinho, estímulo nos meus estudos e pela família que me apresentou. Por fim, agradeço ao Jorge que passou todas as noites de estudos comigo (sem falhar em nenhuma). Obrigada, amo vocês!

RESUMO

O seguinte trabalho aborda a maneira de atuação do Estado no sistema internacional frente ao Ciberespaço como um novo elemento parte dessa estrutura. Por meio de uma revisão teórica nos ESI a partir da Escola de Copenhague e da Teoria Neorrealista foi debatido sobre as definições e característica do Ciberespaço. Ainda, analisa-se o comportamento do Estado de militarização no espaço virtual ponderando sobre o investimento de recursos tecnológicos para a redução da vulnerabilidade cibernética.

Palavras-chave: Ciberespaço; Segurança; Neorrealismo; Sistema Internacional.

ABSTRACT

The following work approaches the State's way of acting in the international system in face of Cyberspace as a new element part of this structure. Through a theoretical review in the ESI from the Copenhagen School and the Neorealist Theory, the definitions and characteristics of Cyberspace were debated. Furthermore, the behavior of the militarized state in virtual space is analyzed, considering the investment of technological resources to reduce cybernetic vulnerability.

Keywords: Cyberspace; Security; Neorealism; International System.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ARPA – *Advanced Research Projects Agency*

BBN – *Bolt, Beranek and Newman*

C&T – Ciência e Tecnologia

CiberRI- Relações Internacionais Cibernéticas

CS-Net Project – *The Computer Science Network Project*

DCA – *Defense Communication Agency*

EE- Estudos Estratégicos

ESI- Estudos de Segurança Internacional

EUA – Estados Unidos da América

IBM – *International Business Machines Corporation*

IEC- *Israel Electric Corporation*

IPTO – *Information Processing Techniques Office*

ISDS- *International Security and Defenses Systems*

NSF – *National Science Foundation*

PC – *Personal Computer*

RI- Relações Internacionais

SRI – *Stanford Research Institute*

TIC- Tecnologias da Informação e Comunicação

SUMÁRIO

1. INTRODUÇÃO

Quinze anos já se passaram do evento com duração de 22 dias e que ficou conhecido como a série de ataques cibernéticos contra a Estônia em 2007. O estopim dos ataques foi a decisão do governo estoniano de mudar de lugar um monumento – representante da tomada das tropas soviéticas na Estônia durante a Segunda Guerra Mundial – de um cruzamento movimentado no centro de Tallinn para um cemitério militar próximo (OTTIS, 2008). A partir disso é possível ponderar sobre o significado atribuído à escultura e relacioná-lo com o motivo da revolta dos civis estonianos. Para a minoria russa local na época, o monumento representa o "libertador", enquanto para os estonianos representa o "opressor" (OTTIS, 2008). Devido a essa dualidade, o local ficou marcado por uma série de manifestações e confrontos de ambos os lados e a decisão do governo estoniano foi de mover a escultura e cessar os conflitos levando-a para uma região menos movimentada. Porém, o governo estoniano não esperava por um levante de *hackers*, responsáveis por um dos primeiros ciberataques de grande visibilidade midiática no início do século XXI.

A retomada desse acontecimento depois de alguns anos, mesmo havendo outros exemplos de ciberataques existentes, fundamenta-se na perspectiva de analisar a fundo o desenrolar e as consequências dele para o Estado estoniano. Esse tipo de conflito é cada vez mais frequente no dia-a-dia dos Estados, talvez a maioria não chegue a ocorrer de fato como na Estônia, mas se torna evidente a presença de ameaças vindas do Ciberespaço. Então, a presença do Ciberespaço a partir do século XXI cria desafios para as disciplinas de Relações Internacionais (RI) (LOPES, 2013) como campo teórico fundamentado no papel central do Estado, sendo necessário reformular paradigmas teóricos das RI para se explicar o novo cenário social (MEDEIROS, 2019).

O conflito na Estônia, em 2007, parecia se desenrolar como qualquer outro acontecimento no sentindo de haver movimentações armadas e embates entre as partes envolvidas, porém novos elementos advindos da esfera tecnológica foram atribuídos ao conflito quando *hackers* invadiram as redes de computadores do país. Eles atacaram os serviços de navegação (ataques "*DDoS"*[1]),

[1] *Denial-of-service attack*, traduzido como Ataque de negação de serviço.

desconfiguraram sites oficiais e não-oficiais, atacaram servidores de nomes e dados (ataque "*DNS*"[2]) e enviaram e-mails de *spam*[3] em massa (DONALD, 2020). Isso posto, um dos elementos a considerar ao estudar esse evento é o espaço cibernético como um meio e método de ataque/defesa diferente do tradicional, assim como a maior notoriedade de novos atores no sistema internacional (participação dos grupos de *hackers* organizados).

Os ataques cibernéticos dos *hackers* contra o Estado da Estônia foram capazes de gerar grandes consequências econômicas para o país ao afetar seu espaço cibernético (MCGUINESS, 2017). Com acesso quase que universal à Internet na época, a Estônia se encontrou vulnerável frente à série de ataques coordenados que desestabilizaram seus sistemas, em grande maioria interligados, provocando um cenário de descontrole e insegurança durante o período dos ataques (DONALD, 2020; OTTIS, 2008). A participação desses grupos organizados demonstra a capacidade criada de novos elementos interferirem no funcionamento do sistema internacional, seja por autoria própria ou não, ocasionando todo um desdobramento por detrás das ações cibernéticas e que interferem no comportamento dos Estados.

O tipo de problemática exposta no ciberataque contra a Estônia tende a se repetir diariamente, alguns com grandes repercussões e outros em menor escala. Porém, todos causam danos e demonstram a vulnerabilidade dos Estados frente à presença perseverante das tecnologias no sistema internacional, ainda que em graus distintos. Dessa maneira, percebe-se a necessidade de tratar os assuntos sobre Defesa e Segurança frente ao Ciberespaço, também, como parte da atualização do novo paradigma no sistema internacional. Então, surge a problemática da pesquisa: A maneira de atuação do Estado, no sistema internacional, se repete no Ciberespaço?

Assim, busca-se utilizar os conceitos de vulnerabilidade e capacidade cibernética como indicadores das questões voltadas à Segurança dos Estados. Isso nos permite ponderar sobre seu comportamento no sistema internacional perante a presença do Ciberespaço e suas consequências para a sociedade internacional. Portanto, a conduta do Estado adotada perante essas questões pode ser a militarização deste espaço virtual (SINGER *et al*, 2014;) e seu uso como um ponto central para manter a sobrevivência do mesmo.

---

[2] *Domain Name Server*, traduzido como servidor de nomes de domínio
[3] *Spam* é o ato de enviar muitas mensagens e de maneira repetitiva.

Com a finalidade de sobreviver às ameaças do sistema internacional os Estados se beneficiam do Ciberespaço por ser um elemento maleável no qual pode ser tratado como ferramenta ou ambiente (ACÁCIO, 2016). Por causa disso, será feita a análise sobre a atuação dos Estados frente ao sistema internacional ponderando sobre seus modos de defesa e ataque na esfera virtual. A adesão de temáticas *cyber* na agenda interna dos países é cada vez mais frequente, logo isso reflete nas discussões de política internacional inserindo debates acerca desse mesmo tema. A seguinte pesquisa busca analisar a possível vulnerabilidade cibernética dos Estados e sua necessidade de busca por essas capacidades (TIC's - Tecnologias da Informação e Comunicação) para resguardar a paz ou exercer poder.

Sendo assim, parte-se da hipótese de que os Estados buscam agir em contraponto com as três principais características do Ciberespaço para lidar com os desafios de Defesa e Segurança: (1) a desterritorialidade; (2) multiplicidade de atores; e (3) incerteza (MEDEIROS, 2019). Isso ocorria a fim de regulamentar e tornar esse espaço cada vez mais previsível. Para isso, os países buscariam se capacitar e desenvolver estratégias específicas voltadas para a militarização do Ciberespaço para sanar suas vulnerabilidades neste meio, ambicionando evitar o conflito e exercer poder.

Portanto, as questões de Defesa e Segurança dos Estados também precisam se adaptar ao desenvolvimento das tecnologias de rede e informação. Com a finalidade de facilitar o entendimento, parte-se da premissa neorrealista de análise do comportamento dos Estados, acrescida de uma breve análise da estruturação das estratégias de Defesa e Segurança cibernética desenvolvida, ou que vem sendo desenvolvida pelos Estados.

Tal questionamento se torna pertinente ao se observar a quantidade de tecnologia envolvida no dia a dia das pessoas, sendo as tecnologias da comunicação e informação (TIC's) uma das invenções que mais impactaram no comportamento mundial, e que aumenta a quantidade de usuários diariamente (WE ARE SOCIAL; HOOT SUITE, 2022). Para além disso, infere-se, que uma parte dos atores do sistema internacional que domina esses mecanismos pode usufruir de vantagens estratégicas e se beneficiar delas também. Portanto, outro fator que justifica a importância dessa pesquisa é a preocupação em se entender, a partir de uma análise aprofundada, o funcionamento do Ciberespaço e a atuação dos Estados frente às questões de

segurança cibernética no sistema internacional. Essas supostas vantagens terminariam por alimentar a ordem anárquica do sistema internacional e levariam à busca por poder.

Portanto, o Ciberespaço se tornou um elemento importante, requerido e presente para os Estados ao tratarem da temática sobre Segurança, Defesa e Estratégia Nacional. Ainda, cabe destacar outros fatores pertinentes para o estudo proposto, quais sejam, as capacidades dos Estados e a vulnerabilidade deles no âmbito do Ciberespaço. Daí passa a ser indispensável o estudo do Estado no cenário internacional, a fim de entender suas adequações comportamentais e aplicá-las nas teorias do campo de estudo das RI, além de averiguar se isso contribuí para manter a ordem. Desse modo, justifica-se a pesquisa pela necessidade de buscar maior entendimento acerca do Ciberespaço, pontuando seus impactos no funcionamento e uso pelo Estado.

Para isso optou-se por utilizar uma abordagem metodológica qualitativa, uma vez que predomina a interpretação desenvolvida pela pesquisadora diante da compreensão do estudo observando seu objeto a partir de "aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais" (SILVEIRA; CÓRDOVA, 2009, p.32). Em primeiro momento haverá o emprego de pesquisa bibliográfica, devido à utilização de materiais produzidos anteriormente e que servirão para embasar o trabalho, e pesquisa documental, em função da análise de documentos oficiais e reportagens atuais ligados ao problema de pesquisa. Posteriormente, será realizado um breve mapeamento das estruturas de Defesa e Segurança cibernética do Estado e se elas contribuem na propagação de conflitos violentos ou para a paz. Ademais, o método que irá direcionar o estudo será o hipotético-dedutivo, visto que buscou-se criar uma hipótese por meio de um problema inicial, como apresentado mais acima nesta introdução.

Para a compreensão da temática abordada no trabalho faz-se necessário realizar uma revisão teórica e conceitual, destacando alguns conceitos e definições importantes com o intuito de fundamentar a hipótese apresentada. Nesse sentido, optou-se analisar o funcionamento do sistema internacional a partir da teoria Neorrealista com aprofundamento nos estudos desenvolvidos por Kenneth N. Waltz em sua obra "Teoria da Relações Internacionais" (1979). Tal estudo foi selecionado para embasar a pesquisa, devido aos princípios utilizados pelo autor (e que serão exposto mais a frente) para explicar as RI por meio de uma abordagem sistêmica e que,

mediante o desenvolvimento deste trabalho, será introduzido o Ciberespaço como um novo elemento dessa estrutura capaz de influenciar na ordem do sistema.

Além da discussão sobre a estrutura, busca-se abordar a questão da Segurança dos Estados frente a essas alterações. Em vista disso e sobre a crescente falta de previsibilidade a partir do espaço cibernético, serve-se dos Estudos de Segurança Internacional (ESI) sobre o princípio da Segurança como uma prática autorreferencial desenvolvido pela Escola de Copenhague (BUZAN; WÆVER; DE WILDE, 1998) para justificar o aumento da incerteza com o Ciberespaço. As teorias apresentadas acima serão abordadas no primeiro capítulo afim de expor e relacionar a temática aos conteúdos programáticos das RI.

Dando continuidade à estrutura da pesquisa, o segundo capítulo aprofunda na temática do Ciberespaço e seu histórico, com o objetivo de estabelecer o objeto a ser estudado e sua influência na sociedade contemporânea. Neste momento, busca-se entender e delinear as relações atuais da tecnologia com a população, sendo a população um componente importante presente na teoria geral do Estado. Assim, são debatidos os conceitos do Ciberespaço e a maneira sobre como o Estado foi inserido nesse sistema moldando seu comportamento. Além do modo comportamental, começa a se relacionar as questões de Segurança e Defesa por meio das características apresentadas do espaço virtual.

Seguindo a lógica necessária para o trabalho, o terceiro capítulo aborda o comportamento dos atores no Ciberespaço por fim. Assim, investiga-se o uso das tecnologias e do Ciberespaço por meio do Estado, dando ênfase na utilização do poder cibernético com relação as questões voltadas para a segurança no cenário internacional. Ainda neste capítulo, para trazer esclarecimento sobre o modo de atuação dos Estados, serão desenvolvidos os conceitos de vulnerabilidade e capacidade cibernética com a finalidade de justificar as decisões do Estado sobre o uso das tecnologias. Neste momento, será debatido o estabelecimento do poder cibernético como um domínio operacional afim de incitar a guerra (aprimorando outros meios de poder, por exemplo). Assim, serão abordados os conceitos de ciberguerra e armas cibernéticas, expondo os conceitos utilizados pelos estudiosos, aliados à maneira como o Estado lida com suas questões de segurança para o Ciberespaço.

Para encerrar o trabalho, o quarto capítulo será o de conclusões finais. Nele será feita uma retomada nas principais questões levantadas durante o estudo e seus desdobramentos, permitindo analisar seus resultados e findar a pesquisa.

2. TEORIAS DAS RELAÇÕES INTERNACIONAIS PARA O CIBERESPAÇO

A busca por entender o funcionamento das Relações Internacionais (RI) e teorizar sobre ela, parte do aumento da complexidade adquirida no mundo. Desde as primeiras organizações políticas da antiguidade até o sistema dos Estados modernos, percebe-se o incremento de assuntos debatidos acerca da importância estabelecida cada qual em sua época. Por isso, pode-se afirmar que "o núcleo tradicional das RI está relacionado a questões sobre a dinâmica e a mudança da condição do Estado soberano no contexto de um sistema maior ou sociedade de Estados" (JACKSON; SORENSEN, 2007, p.60). Portanto, diferentes temas surgem para estudo nas RI quando esses causam algum tipo de impacto ou auxiliam no entendimento de acontecimentos ou partes presentes no sistema internacional e sua sociedade.

Com isso, o aparecimento de temas diversos a partir da abordagem da disciplina das RI ocorre devido ao pensamento dessa área do conhecimento ser influenciado por outras matérias acadêmicas (JACKSON; SORENSEN, 2007), como é o caso do presente trabalho, ao beber de temáticas voltadas ao sistema de informações e informática. Em consequência dessa interdisciplinidade, a partir do advento das Relações Internacionais Cibernéticas (CiberRI), o termo ciberinternacionalismo se mostra cada vez mais presente, sendo ele relacionado "ao estudo sistemático do Ciberespaço a partir de um elemento metateorético de RI" (VILAR-LOPES, 2017, p.3). Portanto, esse meio de análise torna possível o uso de conceitos e teorias das RI para esclarecer objetos específicos das questões levantadas pelos impactos do espaço cibernético no ordenamento do sistema internacional.

Em vista disso, a emergência da temática voltada para o Ciberespaço perpassa desde a década de 1990 quando o termo "*cyberwar*" foi mencionado por Arquilla e Ronfeldt (1993 apud LOPES, 2013) e segue se desenvolvendo nos anos 2000, após o atentado do 11 de Setembro, criando a ideia da conexão do Ciberespaço como uma fonte de insegurança para o sistema internacional. Posteriormente, em 2010, devido "a importantes acontecimentos internacionais, envolvendo ataques cibernéticos e políticas públicas de Segurança e Defesa Cibernética" (LOPES, 2016, p.64), essa temática continua presente no dia a dia dos Estados Modernos. Logo, esse capítulo busca retomar alguns conceitos da Escola de Copenhague direcionados para a

Segurança Cibernética e delinear semelhanças do campo de atuação do Estado no sistema internacional, no que tange ao espaço cibernético a partir de uma visão do Realismo Estrutural.

2.1 A abordagem de Segurança e Estratégia no espaço cibernético

Acontecimentos históricos significativos são capazes de gerar mudanças no sistema internacional. Considerando isso, o fim da Guerra Fria e o atentado do 11 de setembro são responsáveis por intensificar a complexidade do sistema internacional que, além de lidar com crises humanitárias, guerras civis, e a unipolaridade estadunidense, passou a enfrentar, simultaneamente, a espionagem, guerra cibernética, vazamento de banco de dados, etc. (LEHMANN, 2012). Com a ocorrência desses novos episódios, emergem-se novas pautas inclusas dos Estudos de Segurança Internacional (ESI) e Estudos Estratégicos (EE) sobre o advento do espaço cibernético. Do mesmo modo, o subcampo internacionalista de Relações Internacionais Cibernéticas (CiberRI) mostra-se interessante para ser estudado e suas discussões são colocadas em prática a partir do aprofundamento nos debates acerca do Ciberespaço (VILAR-LOPES, 2017).

No âmbito dos primórdios da disciplina voltada para a segurança internacional, após a Segunda Guerra Mundial, debates sobre como preservar os Estados de ameaças internas e externas manifestaram-se a partir da subárea dos ESI (BUZAN; HANSEN, 2012). O pensamento da estratégia por meios tradicionais, ou militares, passa a ser visto como ultrapassado e a criação e fortificação do conceito de segurança serve para distinguir os ESI das disciplinas de Estudo da Guerra e História Militar durante a Guerra Fria (BUZAN; HANSEN, 2012).

Portanto, busca-se o aprofundamento do debate sobre segurança e a ampliação de seu conceito, considerando que, “assim como a política, a Segurança deve ser vista como a partir de um contexto social” (VALENÇA, 2010, p.76). Sendo assim, justifica-se a atualização da temática da segurança voltada para o Ciberespaço por ser possível afirmar que o desenvolvimento das tecnologias da informação e comunicação acarretaram em significantes mudanças sociais e políticas (e que serão aprofundas no segundo capítulo).

A perspectiva da Escola de Copenhague é bastante interessante, “(...) pois ele [Buzan] olha para a segurança de todos os ângulos do micro ao macro, abordando também os aspectos

sociais da segurança e como as pessoas ou sociedades constroem ou ‘securitizam’ ameaças” (STONE, 2009, p.2, tradução nossa)[4].

Para categorizar ainda mais a ideia de evolução dos ESI, Silva e Pereira (2019) pontuam os três fatores fundamentais da teoria que as diferenciam dos debates estruturalistas. A primeira divergência se encontra no conceito chave de segurança, como já abordado, deixa de ser sinônimo de defesa e dá abertura para que questões políticas e sociais sejam amplamente estudadas. O segundo fator foi pensado a partir da objeção das armas nucleares, pois os meios militares se mostraram insuficientes para compreender o uso, ou não, dessas armas. A terceira diferença aborda a natureza das questões de segurança, anteriormente tratadas de modo puramente militar e que passaram a envolver diversos temas relacionados à segurança também, como por exemplo as questões econômicas.

A contar essas mudanças de perspectiva, a teoria de securitização foi desenvolvida pela Escola de Copenhague. Ao reconhecer a característica anárquica do sistema e considerar o Estado seu objeto de estudo, a Escola se alinha à teoria realista ao mesmo tempo em que sua essência se respalda no Construtivismo (SILVA; PEREIRA, 2019; THUDIUM et. al., 2020). Esse cruzamento teórico determina um ponto crucial da teoria da securitização pois, “demonstra que as relações interestatais, ainda que um elemento extremamente importante, não são os únicos determinantes das dinâmicas securitárias que caracterizam a política internacional” (THUDIUM et. al., 2020, p.6).

Ao se tratar da abordagem de segurança voltada para o Ciberespaço, a segurança cibernética aborda assuntos que lidam com a ascensão de outros atores diferente do Estado no sistema internacional com a capacidade de agir e abalar as estruturas do cenário internacional e interno dos países. Por se tratar disso, o enfoque da securitização se torna relevante na tomada de decisões dos governos e *policymakers*, pois além das relações interestatais há outras relações na qual os Estados devem se preocupar sobre as ameaças.

Porém, mesmo com a maior possibilidade de ascensão de outros atores, o Estado não deixa de ser a peça crucial no momento de lidar com as questões de segurança e deve reformular

[4] “(…) as he looks at security from all angles going from micro to macro, also addressing the social aspects of security and how people or societies construct or ‘securitize’ threats” (STONE, 2009, p. 2).

sempre que necessário suas políticas de defesa e estratégia. Portanto, a ligação entre as noções básicas de segurança e estratégia são inevitáveis (BUZAN; HANSEN, 2012).

Destarte, a dissociação dos ESI para com os Estudos sobre a guerra sinalizou, também, a distinção entre os conceitos de segurança e estratégia, sendo a ideia de segurança tida como uma inovação e a concepção de estratégia relacionada a algo ultrapassado (DAVID, 2000), o que não se consolida dessa maneira. Para além dessa interpretação, tal pensamento estava relacionado ao fato da dissociação das disciplinas e suas substâncias sobre as questões militares, ou seja, existia a necessidade de se repensar a segurança a partir de novas estratégias para além das militares. Assim,

> durante a guerra fria, eles [os estudo estratégicos] centravam-se essencialmente na compreensão da dimensão militar da segurança. Agora dão lugar aos estudos de segurança, ao mesmo tempo alargados e não militares, que redefinem na medida do possível o uso da estratégia. (DAVID, 2000, p.20)

Embora tenha havido o distanciamento da visão unicamente militar a partir dos ESI, não se pode afirmar o abandono da concepção de estratégia, mas sim uma nova percepção dela. Decorrendo disso, a caracterização da segurança está rodeada de conceitos, sendo eles: paralelos, opositores e complementares (como é o caso da estratégia) (BUZAN; HANSEN, 2012, p. 41). Esses conceitos ajudam a ampliar os debates da disciplina, no qual a ideia central é “segurança”, mas a partir desses outros conteúdos se permite debater sobre distintas temáticas ligadas aos ESI, como por exemplo a “paz” (conceito opositor) para se debater o desarmamento e controle das armas nucleares, e mais próximo dessa pesquisa, o controle das armas cibernéticas (BUZAN; HANSEN, 2012).

Levando em consideração os conceitos complementares para se entender tal melhoria nos ESI, o cientista político canadense Charles Philippe David (2000) afirma que as “estratégias transformam as questões de segurança” (2000, p.20). Portanto, o autor apresenta três evoluções dos Estudos Estratégicos que são consideradas importantes para se entender a mudança desse campo nas Relações Internacionais (Figura 1). Considerando isso, as evoluções tratam sobre: a análise das questões de segurança; a definição das estratégias na formulação das políticas; e a força utilizada para aplicar as estratégias e garantir a segurança.

Compreender tais evoluções é fundamental para se entender que mesmo após essas mudanças, a estratégia continua sendo um elemento importante ao se tratar de segurança, mesmo se diferenciando do arcabouço militar e adentrando as questões políticas e sociais.

Partindo da primeira mudança em relação à análise das questões de segurança, David (2000) discorre sobre a alteração da pauta militar do conflito armado e da guerra para outros assuntos como novos problemas securitários (o tráfico de drogas, ataques cibernéticos, etc.). Assim, outras perturbações passam a configurar o sistema internacional moderno e são colocadas em pauta nos ESI por se tornarem cada vez mais presentes no dia a dia das suas unidades.

Um caso que abalou o cenário internacional e acarretou grandes consequências aos países envolvidos foi o *Stuxnet*, um *worm*[5] de computador, exclusivamente com objetivos maliciosos, descoberto em junho de 2010. Esse *malware*[6] possuía a capacidade de interferir e burlar as centrífugas de motores industriais, sendo comprovado um ataque ciberfísico direcionado a um alvo específico e único como as usinas nucleares no Irã. Essa descoberta foi possível a partir da análise desse *worm* e suas semelhanças entre os números no código do *Stuxnet* e os componentes físicos da usina iraniana. Desse modo, o ciberataque fere a soberania do Irã a partir de uma ameaça à segurança de seu Estado fazendo usufruto de uma nova estratégia (CURLEY, 2016; LANGNER, 2021).

Como pode-se perceber, existem vários objetos de análise da segurança, logo, há mais de uma definição de estratégia que pode ser utilizada na elaboração dessas políticas. Para escolher os tipos de estratégia a serem empregadas, basta os atores terem conhecimento das ameaças que o perturbam e o tipo de resposta que pretendem operar (DAVID, 2000). As estratégias são as militares, ligadas diretamente ao conflito e a guerra; as coercivas, ligadas a sanções e projeção da força, visando ganho político antes do recurso à guerra; e as de paz e resolução de conflitos, na qual busca-se novos meios de atuação dos Estados, Organizações Internacionais (OI) e as

[5] A palavra "*worm*" vem do inglês e sua tradução é "verme". Na informática, os *worms* são programas maliciosos autônomos que se replicam e se propagam por redes de computadores. Sua principal característica está em sua autonomia, o que significa que este verme não necessita de atividade humana para se espalhar, basta apenas estar instalado em uma rede para se replicar (KASPERSKY, 2021a).

[6] *Malware* é a abreviação de "software malicioso" (em inglês, *malicious software*) e se refere a um tipo de programa de computador desenvolvido para prejudicar o computador infectado de formas à causa-lo prejuízo (KASPERSKY, 2021b).

Organizações Não Governamentais (ONG's) de prevenir o desencadeamento de conflitos armados (DAVID, 2000).

Em qualquer um dos tipos de estratégia apresentadas anteriormente, o Ciberespaço pode ser utilizado de maneiras diferentes. Na tática militar adquire aplicação integrada, uma vez que há possibilidade de agregar um sistema de controle cibernético com efeitos de armas cinéticas (DYKSTRA; INGLIS; WALCOTT, 2020). Essa técnica permite o acionamento de munições a longa distância, diminuindo as perdas do atacante no campo de guerra. A modalidade militar vem sendo cada vez mais utilizada pelos Estados que recorrerem ao desenvolvimento das TIC's visando resultados em cibersegurança.

Na condição coerciva, os Estados podem se beneficiar do Ciberespaço manipulando a informação afim de expansão de poder e outras vantagens, como por exemplo a movimentação da Organização Olimpíadas Sem Apartheid denunciando ao Estado de Israel sobre o uso dos Jogos Olímpicos de 2014 no Rio de Janeiro para realizar *sportwashing*[7] (OLIMPÍADAS SEM APARTHEID, 2015). Tal acusação alega que, por meio da empresa de inteligência israelense *International Security and Defenses Systems* (ISDS), Israel estaria trocando "tecnologia de controle por publicidade para limpar sua imagem" (MISLEH, 2021). Outra questão semelhante a anterior é um acordo fechado entre o Japão e a *Israel Electric Corporation* (IEC) havendo troca de soluções voltadas a cibersegurança em 2020, mesmo ano que as olimpíadas foram sediadas no país nipônico. A empresa é responsável pelo controle do fornecimento de energia na Palestina ocupada racionando esse recurso.

Uma estratégia diferente da tradicional que pode ser explorada pelos atores do sistema internacional, principalmente os Estados, diz respeito ao uso do Ciberespaço para atingir a paz e resolução de conflitos. Considerando esses dois conceitos estratégicos, o fenômeno da guerra pode ser transformado a partir do nascimento da Internet, revelando espaço a modalidade da ciberguerra e, por consequência, uma paz relativa à diminuição dos conflitos armados e perda humana (RID, 2013). Em contrapartida, para alguns autores a ciberguerra também contribui para o fomento de conflitos tradicionais (CLARKE; KNAKE, 2010). Essa dicotomia entre "guerra" e

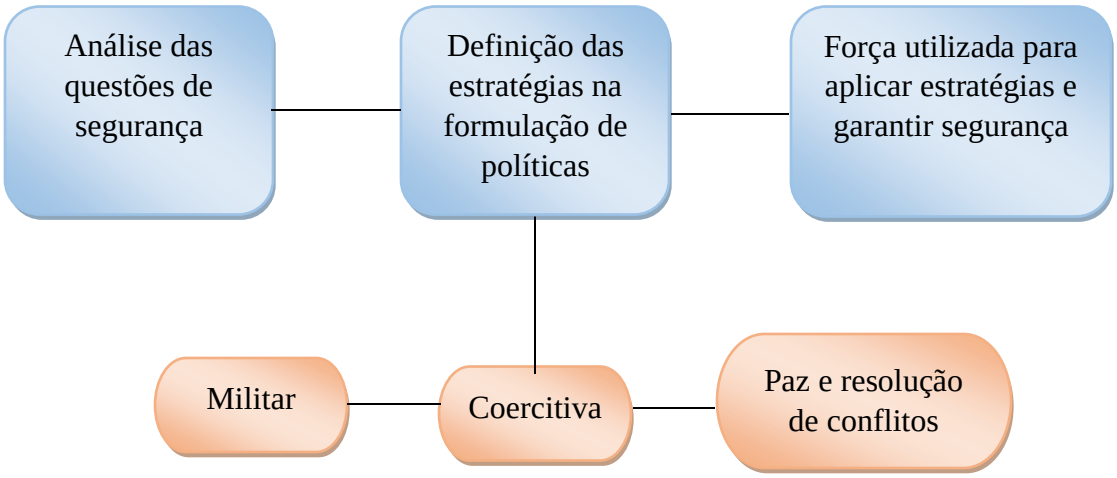
[7] O *sportwashing* é um termo criado por organizações de direitos humanos sobre a prática realizada pelos governos no intuito de limpar sua reputação por meio do esporte. Assim, aproveita-se do sentimento de cooperação e irmandade gerado pelos eventos esportivos com a finalidade de mostrar o outro lado (bom) dos envolvidos, sediando os eventos, por meio de investimentos e patrocínio, ou publicidade.

"paz" segue existindo dentro do espaço cibernético e, por isso evidencia-se mais um motivo para entender a importância da pesquisa e do desenvolvimento tecnológico em termos de segurança nacional e internacional[8].

Por fim, a terceira evolução dos Estudos Estratégicos entrelaçados aos ESI aborda a força aplicada nas estratégias para garantir a segurança, porque há uma preocupação acerca do desenvolvimento de tecnologias que disseminam e criam concorrência com o Estado sobre o uso da força, removendo o monopólio estatal (DAVID, 2000). Portanto, o espaço cibernético passa a ser cada vez mais utilizado pelos Estados a partir do desenvolvimento de novas tecnologias de dados e redes, desencadeando uma "corrida armamentista cibernética" que acaba por resultar na militarização desse plano a fim de garantir o poder de atuação do Estado (SINGER; FRIEDMAN, 2014). Assim, o Estado luta pelo protagonismo nesse local de atuação devido à facilidade de acesso que outros atores podem adquirir frente ao mundo globalizado pelas Tecnologias da informação e comunicação (TIC's). Por meio da Internet, as organizações terroristas conseguem recrutar membros recorrendo à publicidade de alta qualidade e poder de persuasão, como por exemplo uso das redes sociais por grupos terroristas, entre eles, o Estado Islâmico, possibilitando abarcar um grande número de pessoas com suas ideais (SENRA; KAWAGUTI, 2016).

[8] A abordagem, tanto da segurança nacional, quanto da segurança internacional é importante devido a presença da atuação no Ciberespaço a partir desses dois níveis de análise. Portanto, o modo como ocorrem mostra a necessidade dos Estados de reduzir sua vulnerabilidade frente as ameaças internas, fortalecendo sua segurança nacional e, em conjunto a isso, buscando enfraquecer as ameaças externas de modo mais eficaz (RUDZIT; NOGAMI, 2010).

Figura 1- Mapa teórico: As três evoluções dos EE para entender as mudanças do ESI nas RI aplicadas ao Ciberespaço



FONTE: Elaborado pela autora

Embora a análise do espaço cibernético seja viável a partir das teorias da Escola de Copenhague, seus pensadores não aprofundaram no tema do Ciberespaço. Desta forma, Helen Nissenbaum e Lene Hansen (2009) aplicaram essa teoria com o propósito de contribuir com o setor cibernético e suas análises sobre segurança internacional, conceituando Segurança Cibernética "como algo oriundo da agenda pós-Guerra Fria em resposta à mistura de inovações tecnológicas e às mudanças nas condições geopolítica internacionais" (NISSENBAUM; HANSEN, 2009 apud ACÁCIO, 2016). Além disso, as autoras comparam a atividade do setor econômico com a do cibernético "devido à constante interdependência e aos problemas em definir limites geográficos e competências, inclusive com o alto grau de responsabilidade da esfera privada" (ACÁCIO, 2016, p. 52). Contudo, o desenvolvimento das TIC's possui uma forte ligação com as questões de segurança militar e possuem uma função importante na "Revolução dos Assuntos Militares" (DAVID, 2000; NISSENBAUM; HANSEN. 2009).

A fim de buscar uma atualização acerca dos ESI a partir da Escola de Copenhague, Hansen e Nissenbaum (2009) ainda teorizam sobre a existência de uma gramática de segurança específica para o setor cibernético e elaboram três ideais a se considerar para análise: o ideal de hipersecuritização, sendo relacionado ao argumento de causa de danos catastróficos e

irreversíveis, comparado até com as abordagens no setor ambiental, e utilizado nos estudos de segurança cibernética; a ideia das práticas diárias de segurança, no qual é estabelecido uma relação dos aspectos da Segurança Cibernética e o cotidiano das pessoas[9], tornando a hipersecuritização mais aceitável; e por fim, as tecnificações, responsáveis pela utilização de discursos técnicos e especializados em Segurança Internacional que terminam por restringir a opinião dos outros especialistas em Segurança da Informação.

2.2 A teoria da securitização e o Estado no espaço cibernético

À luz da teoria construtivista, a segurança é estudada como uma construção social (SILVA; PEREIRA, 2019). Logo, securitizar a segurança é tratá-la como um processo intersubjetivo e construído socialmente, assim ela "não reside nos objetos ou nos sujeitos, mas *entre* os sujeitos" (AMARAL, 2008, p.73). A partir disso, reflete-se sobre esse processo voltado para o Ciberespaço a partir da impossibilidade de se desvincular os ESI de questões intrínsecas ligadas às TIC's, como por exemplo a globalização e o terrorismo (CEPIK; CANABARRO; BORNE, 2014).

Antes de pormenorizar a securitização no Ciberespaço, busca-se compreender melhor a teoria da securitização por meio de conceitos determinados por Buzan e Wæver em suas obras. Em vista disso, os autores definiram três categorias operacionais: (1) objetos referentes; (2) agente securitizador; e, (3) atores funcionais. Cada um deles é encarregado de uma parte do processo que irá resultar em seu andamento até atingir seu o estágio máximo: a securitização.

Um ator político que demonstra capacidade em determinar um tema e fazer o público reconhecê-lo como ameaça é classificado como agente securitizador. Tendo isso como base, esse ator utiliza de um ato de fala *(speech act*) para legitimar um discurso acerca de um objeto referencial, garantindo-o uma audiência notória (WÆVER, 1995). "Quando um ator securitizador usa uma retórica de ameaça existencial e, assim, tira uma questão do que, nessas condições, é 'política normal', temos um caso de securitização" (BUZAN; WÆVER; DE WILDE, 1998, p.

[9] Nesse caso considera-se como ocorridos do cotidiano: as fraudes bancárias, invasões a e-mail e servidores, além de outros crimes cibernéticos que possam atingir a população civil.

24).[10] O objeto referente pode ser o Estado, mas não se limita a ele. Organizações, indivíduos, grupos transnacionais e grupos sociais também podem ser alvos do agente securitizador. Finalmente, os atores funcionais são o público a ser convencido de que aquela temática é uma ameaça existencial, logo deve ser securitizada. Esta última categoria tem importância na teoria, porque perturbam indireta e diretamente as questões de segurança de algum setor (VILLA; SANTOS, 2011 apud SILVA; PEREIRA, 2019).

Por essa razão, para enquadrar uma questão como matéria de segurança é necessário considerá-la como "ameaça existencial" e, por isso, ela pode ser feita de maneira subjetiva com a finalidade de legitimar ações excepcionais e que vão além das regras políticas tradicionais (ACÁCIO, 2016). Um exemplo clássico é a securitização do terrorismo, após os ataques de 2001 às torres gêmeas, os discursos de George W. Bush repercutiram na sociedade internacional como atos de fala e movimentos de securitização culminaram na Guerra ao Terror e consequentes invasões do Afeganistão (2001) e Iraque (2003) (HOFF, 2017). Contanto que a mensagem desse agente atinja os atores e gere uma real comoção acerca do tema, o processo de securitização foi bem executado.

Sendo assim, qualquer assunto público pode ter o *status* de não politizado, politizado ou securitizado. Considera-se um assunto "não politizado" quando não há debate sobre o objeto ou não compartilha de decisão com o público. Para se tornar "politizado" o objeto faz parte da agenda de política públicas e está presente nas decisões governamentais. Finalmente, adquire a condição de "securitizado" quando é apontado como ameaça existencial que necessita de medidas emergenciais além dos procedimentos normais da tomada de decisão política (BUZAN; WÆVER; DE WILDE 1998, p.23 apud SILVA; PEREIRA, 2019). O tema securitizado pode voltar à fase de politização quando é dessecuritizado.

Em seguida, Silva e Pereira (2019) resumem tal questão na Tabela 1:

[10] "When a securitizing actor uses a rhetoric of existential threat and thereby takes an issue out of what under those conditions is "normal politics", we have a case of securitization." (BUZAN; WÆVER; DE WILDE, 1998, p. 24)

Tabela 1 – Securitização: a proposta da Escola de Copenhague

Continuum	Características
Não Politizado	- Estado não é envolvido - Não existe debate ou decisão pública
Politizado	- Há uma política pública - Há decisões governamentais - Há discurso sobre o tema
Securitizado	- É uma ameaça existencial - Exige uma medida de emergência - Justifica ações fora dos procedimentos políticos normais

Fonte: SILVA; PEREIRA apud SILVA, 2013

Desse modo, um princípio da Escola de Copenhague sustenta que a segurança é uma prática autorreferencial, portanto, a ameaça não é objetiva, sendo definida por um processo intersubjetivo (BUZAN; WÆVER; DE WILDE, 1998). Em consequência disso, a ideia de securitização é questionada devido a sua utilização para além das ameaças existenciais, pelo seu caráter flexível em razão da possibilidade de tratar qualquer questão pública, desde que se encaixe em seus parâmetros, como um prenúncio.

> O que então é segurança? Com a ajuda da teoria da linguagem, podemos considerar "segurança" como um *ato de fala*. Nesse uso, a segurança não interessa como signo que se refere a algo mais real; o enunciado em si é o ato. Ao dizê-lo, algo é feito (como apostar, fazer uma promessa, nomear um navio). Ao proferir "segurança", um representante do estado move um determinado empreendimento para uma área específica e, assim, reivindica o direito especial de usar todos os meios necessários para bloqueá-lo. (WÆVER, 1995, p.55, grifo nosso, tradução nossa)[11]

[11] "What then is security? With the help of language theory, we can regard "security" as a *speech act*. In this usage, security is not of interest as a sign that refers to something more real; the utterance itself is the act. By saying it, something is done (as in betting, giving a promise, naming a ship). By uttering "security", a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it." (WÆVER, 1995, p.55, grifo nosso)

Devido a esse processo intersubjetivo, questões podem ser securitizadas em prol do próprio agente securitizador a fim de adquirir vantagens. Ao se tratar do Estado, o principal ator a ser analisado nessa pesquisa, o Ciberespaço pode ser utilizado na definição das estratégias na formulação de políticas adquirindo caráter militar, coercivo e sobre paz e resolução de conflitos (como apresentado mais acima), por exemplo.

2.3 O Ciberespaço a partir das características do Sistema Internacional

A transição da organização política europeia dos feudos para os Estados constitui, superficialmente, o que hoje denominamos como sistema de Estados. Desse modo, vale ressaltar que "o conceito de Estado não é um conceito universal, mas serve (...) para indicar e descrever uma forma de ordenamento político surgida na Europa a partir do século XIII até os fins do século XVIII ou inícios do XIX" (BOBBIO, 2004a, p. 425). Então, um sistema de Estados pode ser entendido como uma instituição histórica determinada pelos seres humanos resultando em uma organização social (JACKSON, SORENSEN, 2007). A partir da abordagem Realista, o principal ator do sistema internacional é o Estado, sendo ele dotado de características que permitem uma análise de seus comportamentos nacionais e internacionais.

Para além disso, outro elemento importante é o sistema internacional no qual o Estado está inserido, pois é a partir do conjunto de características desse sistema, somado ao comportamento e ordenamento de suas unidades, que torna possível um real entendimento das Relações Internacionais. Ademais, obtém sucesso do domínio político quem consegue manejar suas atuações nos níveis nacionais e internacionais mantendo a sobrevivência do Estado e sua soberania (HALLIDAY, 1999; BOBBIO, 2004b).

Tendo essas considerações como base e a concepção do Neorrealismo, o componente político que será analisado a partir das relações entre Estados no sistema internacional é o espaço cibernético, que possui uma relevante particularidade de se manifestar, ora como uma ferramenta (meio), ora como um ambiente (fim) (ACÁCIO, 2016). Portanto, como fora apresentado anteriormente, os meios de uso do espaço cibernético a partir da segurança, chega o momento de investigação desse ambiente no sistema internacional a partir da análise de suas semelhanças buscando atualizar a teoria para essa nova realidade.

2.3.1 A teoria Neorrealista e suas semelhanças com o Ciberespaço

Ainda que haja uma dificuldade na definição das fronteiras do Ciberespaço e sobre a atuação dos Estados nesse ambiente, o comportamento dos países pode ser considerado semelhante ao das unidades do sistema internacional, mais precisamente com os ideais do Neorrealismo. Inaugurada uma nova vertente do realismo em 1979, o Realismo Estrutural ou Neorrealismo, foi proposto por Kenneth Waltz em sua obra "Teoria das Relações Internacionais". Com a finalidade de criar uma teoria que resolva as adversidades acerca do sistema internacional, Waltz apresenta críticas às teorias reducionistas e, como uma maneira de solucionar os problemas gerados pelo caráter descritivo dessas teorias, o autor constrói uma abordagem sobre a política internacional e adota uma postura explanatória inovadora no campo de pesquisa das relações internacionais na época (CORRÊA, 2016). Na sequência, Waltz discute os conceitos de sistema e estrutura para, posteriormente, apresentar o funcionamento do sistema internacional [12].

Sendo assim, a partir da necessidade de uma abordagem sistêmica, o Neorrealismo define sistema como um conjunto de unidades que interagem entre si e, detalhadamente, introduz o conceito:

> Num primeiro plano, um sistema consiste numa estrutura, sendo a estrutura o nível sistémico propriamente dito que torna possível pensar nas unidades como formando um conjunto, algo mais do que uma mera coleção. Noutro plano, o sistema consiste em unidades em interação. (WALTZ, 1979, p.62)

Desse modo, apenas é possível a existência de um sistema internacional a partir de uma estrutura internacional que é retroalimentada pela interação de suas unidades. Em vista disso, o autor afirma que para uma análise sistêmica da política internacional, a parte interna das unidades e o modo como elas interagem não importam em primeiro plano, mas sim a disposição dessas unidades no sistema (WALTZ,1979; BITTENCOURT, 2013; CORRÊA, 2016).

Com isso, por meio dessa organização estrutural, as sociedades estabelecem de forma natural normas de comportamento capazes de moldar as ações dos atores envolvidos no sistema. Uma das formas que as estruturas trabalham seus efeitos sob as unidades é por meio da

[12] A teoria neorrealista de Waltz foi uma das teorias das relações internacionais escolhidas pela autora para explicar o Ciberespaço por haver conceitos relacionados ao desenvolvimento dessa pesquisa. A escolha teórica da autora não excluí o uso de outras teorias para se abordar o Ciberespaço, podendo ser feitas novas análises com as demais teorias.

competição que “incita os actores a acomodarem-se às práticas socialmente mais aceitáveis e com mais êxito” (WALTZ, 1979, p.111). Portanto, essa competição é interpretada como uma “cooperação de unidades egoístas” (WALTZ, 1979, p.129), mantendo o sistema a partir do princípio de autoajuda e assegurando a sobrevivência do Estado. Assim, o sucesso e o fracasso desse Estado dependem exclusivamente de seu esforço, pois cada um tende a buscar sua sobrevivência e garantir a própria segurança no âmbito internacional.

Para aprofundar mais nessas questões, Waltz (1979) estabelece três camadas de análise para definir a estrutura dos sistemas internacionais: os princípios ordenadores, o caráter das unidades (funções e características), e a distribuição das capacidades. É a partir daí que suas semelhanças avançam em relação ao Espaço cibernético.

Para os princípios ordenadores, entende-se sobre a organização das partes de um sistema. O realismo estrutural considera que “os sistemas internacionais são descentralizados e anárquicos” (WALTZ, 1979, p.125). Ou seja, não existe um ator supranacional capaz de governar a relação entre os demais atores. Portanto, ao invés de se pensar na autoridade das unidades, passa-se a considerar a capacidade dos atores (um dos pontos utilizados pelo autor e que será aprofundado em sequência).

A partir desse princípio, é reforçada a relação de autoajuda das unidades e a cooperação egoísta para a busca da própria sobrevivência no sistema internacional. Em consonância com o Ciberespaço, também não é possível estabelecer um ator supranacional que o governe, garantindo a este ambiente as características de descentralizado e anárquico. Consequentemente, os atores com maiores capacidades (no caso, voltadas para as tecnologias da informação e comunicação – TIC) tendem a ganhar destaque e se encontrar menos vulneráveis no espaço cibernético.

Ademais, existem unidades políticas diferentes do Estado no sistema internacional e suas funções se diferenciam entre eles.

> Para Waltz é claro que os Estados não são os únicos atores do sistema internacional, contudo, a partir do momento em que se escolhe uma determinada realidade para se observar, é necessário que se escolham as unidades em cujos termos se comporá sua análise. No caso de Waltz, que examina a política internacional, as unidades que compõem sua análise são aquilo que chamamos de Estados (BITTENCOURT, 2013, p.13).

As unidades nomeadas durante a obra do autor fazem referência aos Estados que são considerados unidades soberanas, independentes umas das outras para tomar suas decisões e agir no âmbito internacional e interno.

Assim, “as estruturas são definidas não por todos os actores que florescem dentro delas mas pelos mais importantes” (WALTZ, 1979, p. 132). Logo, as potências estatais têm maior poder de influência sobre o regimento do sistema internacional e, por isso, são consideradas como atores principais dessa estrutura. Do mesmo modo, as potências possuem vantagens no Ciberespaço devido à capacidade de maior investimento em TIC. Além disso, benefícios são alcançados a partir da securitização desse meio, como já apresentado anteriormente (HANSEN, NISSEMBAUM, 2009), garantindo a efetividade da conquista dos próprios interesses desse Estado.

O terceiro tópico, já citado anteriormente, diz respeito à distribuição de capacidades entre as unidades políticas que integram e esculpem a estrutura de maneira espontânea (BITTENCOURT, 2013). Essas unidades são irreconhecíveis a partir de suas funcionalidades, portanto, Waltz (1979) esclarece que, para diferenciá-las, deve-se considerar suas maiores ou menores capacidades para desenvolver tarefas similares abstraindo as demais características do Estado. A partir disso, é possível diferenciar as relações de poder no sistema internacional.

Aprofundando sobre as capacidades, essas possuem uma distribuição material sob a anarquia, ou seja,

> Embora a estrutura do sistema internacional waltziano seja horizontal, porquanto anárquica, existe hierarquia decorrente da distribuição de capacidades materiais [*capabilities*] entre os Estados, que se lançam irremediavelmente no esforço para sobrepujarem uns aos outros. Ao cabo, essa hierarquia acaba limitando e constrangendo o exercício da soberania pelos Estados mais fracos. (LOPES, RAMOS, 2009, p. 5)

Considerando isso, há uma grande variação das capacidades dos Estados ao se considerar território, poder, riqueza etc. Portanto para pertencer a uma estrutura, estarão apenas os atores mais importantes. Ou seja, que possuam as capacidades requisitadas pela estrutura e que tenham valor substancial em relação de uns com os outros.

Ao se tratar do Ciberespaço, uma importante capacidade a se considerar é o investimento em tecnologias voltadas para informação e comunicação. Ademais, outros recursos relevantes são

as habilidades técnicas desenvolvidas pelos indivíduos, pois além dos meios para se acessar o espaço virtual, é necessário conhecimento específico sobre a temática. Portanto a aplicação em pesquisa e educação voltada para as ciências da comunicação podem ser revertidas em poder cibernético também.

Por fim, após o entendimento do sistema internacional por meio do Realismo Estrutural, Waltz (1979) afirma que “mesmo quando as estruturas não mudam, são dinâmicas, não estáticas, e nisto alteram o comportamento dos actores e afetam o resultado das suas interações” (1979, p. 101). Assim sendo, mudanças no sistema não implicam mudanças de sistema e o surgimento de um novo plano, o Ciberespaço, passa a integrar essa lógica a partir de seus ordenamentos já estabelecidos.

3. O CIBERESPAÇO E SUA PRESENÇA NO SISTEMA INTERNACIONAL

Para se entender a fundo sobre o conceito do Ciberespaço, é indispensável conhecer um pouco sobre a história das redes de comunicações, em especial, a Internet. O projeto da Arpanet surgiu por incentivo do governo dos Estados Unidos para as universidades, sem a promessa inicial de ser um projeto militar (LOPES, 2013, p.34-35). Portanto, Kleinrock (2011 apud LOPES, 2013), um dos estudiosos que desempenhou um importante papel no desenvolvimento da Arpanet, declarou, em uma entrevista, que o objetivo dos envolvidos nesse estudo era

> […] prover um projeto entre nossos muitos computadores de pesquisas. Com o forte apoio dos gestores da ARPA, nossos pesquisadores naturalmente promoveram um ambiente de abertura, confiança, partilha e criatividade. Nós não esperávamos que a ARPANET crescesse tão drasticamente como de fato ocorreu, mas conseguíamos ver seu enorme valor desde aqueles primeiros dias.

Sendo assim, a partir do desenvolvimento tecnológico das redes, o mundo ensaiava o advento da Revolução da Informação ou Terceira Revolução Industrial desde o início da década de 1950. Tais avanços tecnológicos transformaram as relações entre os atores internacionais de forma abrupta para o que se conhece hoje, sendo um mundo interconectado e sem fronteiras como a aldeia global de Marshall McLuhan[13]. Como efeito desse novo momento experimentado na segunda metade do século XX, suas consequências já podiam ser observadas devido ao rápido desenvolvimento tecnológico a impactos da internet no mundo. Esses impactos foram ocasionados junto a expansão da Internet frente ao globo terrestre e que serão aprofundados ao longo desse capítulo.

Por meio de todos esses feitos concebe-se o Ciberespaço (conceito que também será aprofundado ao longo do capítulo), como um novo local de atuação dos atores internacionais formado pela rede global da Internet, que assim como o sistema internacional, é naturalmente descentralizado, anárquico e em auto expansão (LOPES, 2011). Desse modo, será dado início a análise da atuação do Estado no Ciberespaço demonstrando a interferência desse espaço no jogo de poder do sistema internacional e na agenda de segurança das potências mundiais.

[13] Estudioso canadense que lavrou esse conceito em seu livro "Os meios de comunicação como extensões do homem" publicado em 1964.

3.1 A invenção da Internet

Com o passar dos séculos, o desenvolvimento das tecnologias cresceu em conjunto com a busca por conhecimento. Pode-se afirmar que a inteligência que mais avançou desde o século XX foi o setor da aquisição, do processamento e da distribuição de informações (TANEMBAUM e WETHERALL, 2011). A indústria da informática, apesar de jovem, foi marcada por um grande progresso em um curto período de tempo e a sua associação às Tecnologias da Informação e Comunicação (TICs) contribuíram para a aceleração desse processo de desenvolvimento e, consequentemente, afetou (e ainda afeta) as bases econômicas, socias e políticas da sociedade contemporânea (CASTELLS, 2014). Em meio a todas essas mudanças, as ciências da computação passaram por transformações naturais no que diz respeito à distribuição e acesso a essas tecnologias, substituindo seus sistemas computacionais centralizados em locais específicos por um sistema descentralizado de redes de computadores. Dessa forma, popularizam-se esses sistemas de redes de computadores em todo o mundo, sendo o exemplo mais conhecido: a Internet (TANEMBAUM e WETHERALL, 2011). Portanto, o sistema de computadores que se encontrava inteiro em uma única sala agora está presente na maioria do globo terrestre.

Em 1958 a *Advanced Research Projects Agency* (ARPA) foi formada pelo Departamento de Defesa dos Estados Unidos junto seu propósito inicial de "mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957" (CASTELLS, 2003, p.16). Em consequência disso, foi idealizado o programa originário da internet: a Arpanet (NAUGTHON, 2000).

Um dos departamentos da ARPA, o *Information Processing Techniques Office* (IPTO), dirigido por Joseph Licklider, em 1962, tinha como objetivo estimular a computação interativa e, despretensiosamente, aprofundaram no sistema de redes da Arpanet. Esse método que buscavam estimular visava "uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar on-line tempo de computação" (CASTELLS, 2003, p.16). Ou seja, o desenvolvimento desse sistema serviria para facilitar o compartilhamento de informações entre os cientistas, podendo conectar todos os centros de pesquisa dos Estados Unidos. Esses pesquisadores se encontravam nas universidades estadunidenses e, somente a partir desse compartilhamento de informações foi possível o rápido

desenvolvimento das TICs, em virtude disso traria uma contribuição para as demais tecnologias de outros ramos futuramente.

O diretor da ARPA de 1962 exerceu um papel de grande relevância no avanço dos estudos desse programa, sendo que

> estima-se que, nos anos que se seguiram à passagem de Licklider na Agência, 70 por cento de todo o financiamento para ciência da computação a pesquisa nos Estados Unidos veio do ARPA, e grande parte dela seguiu o caminho traçado por ele em 1962 (NAUGHTON, 2000, p.81).

Além do sucesso na direção do programa, a maneira como foram determinadas as diretrizes e o financiamento para as pesquisas voltadas a área da informática e comunicações passaram a ser adotadas a partir do sucesso nos estudos da ARPA com a Arpanet. Portanto, o programa de pesquisa da ARPA já se mostrava inovador antes mesmo de concluir suas descobertas, além de ser apenas um ponto de partida para essas invenções do governo dos Estados Unidos.

Nessa época ainda não se sabia da magnitude que essa pesquisa poderia gerar, mas os Estados Unidos possuíam, de antemão, grandes pretensões acerca de seus objetivos ao desenvolverem uma tecnologia revolucionária. A base para o projeto da Arpanet já se encontrava bem construída devido a um outro trabalho desenvolvido por Paul Baran na *Rand Corporation*[14] que tinha como finalidade construir um sistema militar de comunicação capaz de sobreviver a um ataque nuclear (CASTELLS, 2003; TANEMBAUM e WETHERALL, 2011). Assim, os Estados Unidos se protegeram da ameaça da Guerra Fria e se beneficiaram da ideia do progresso a partir do desenvolvimento associado à guerra na história da inovação tecnológica. Portanto, Castells (2003, p.26) ainda afirma que "o esforço científico e de engenharia feito em torno da Segunda Guerra Mundial constituiu a matriz para as tecnologias da revolução da microeletrônica, e a corrida armamentista durante a Guerra Fria facilitou seu desenvolvimento."

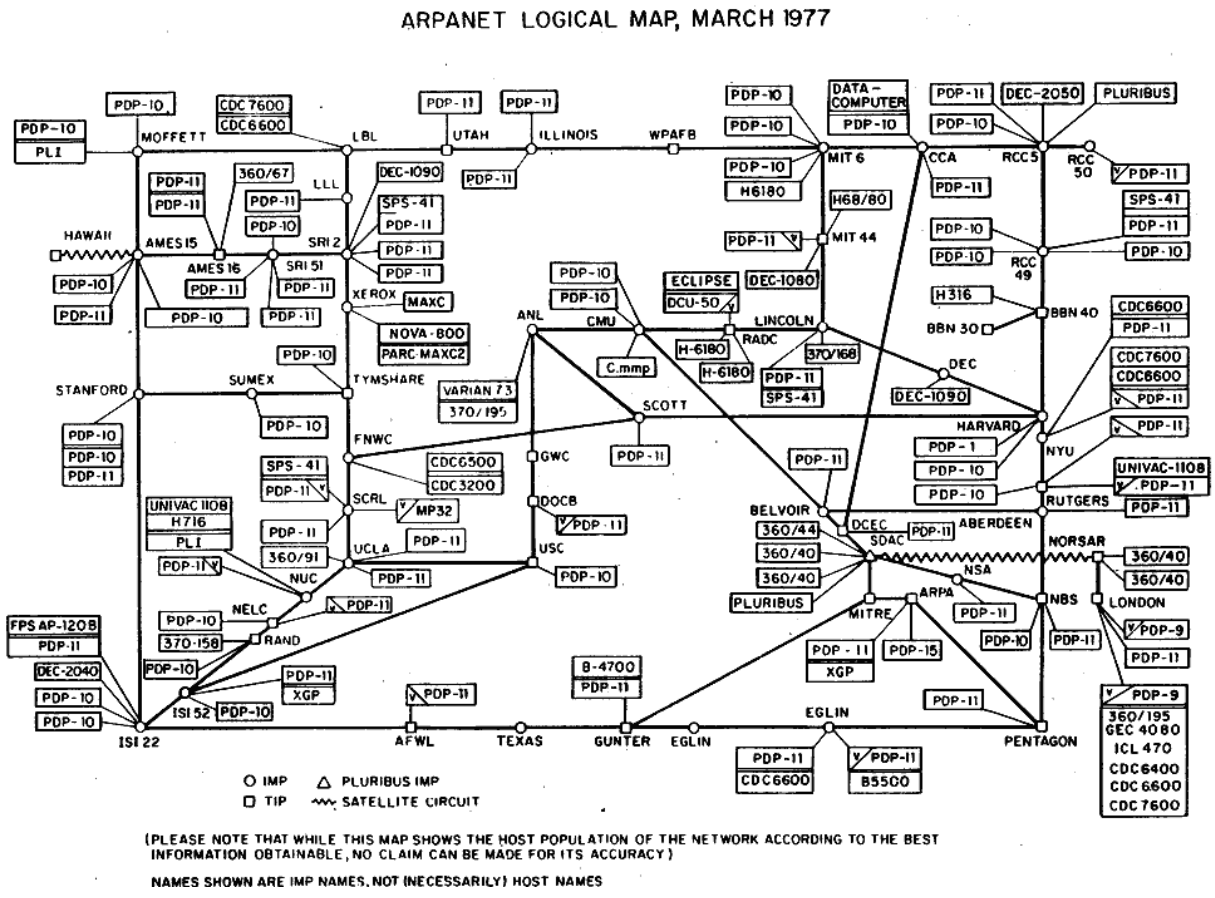
[14]O nome *Rand* advém da contração das palavras *Research* ("pesquisa" em português) e *Development* ("desenvolvimento" em português). Ela é uma organização sem fins lucrativos que atua desde a Segunda Guerra Mundial de maneira independente, reunindo grandes pesquisadores com o propósito de a promover e promover fins científicos, educacionais e de caridade para o bem-estar público e a segurança dos Estados Unidos (RAND CORPORATION, 2022). Portanto, mesmo que independente sempre atuou com incentivo do governo estadunidense compartilhando conhecimento com seus serviços de inteligência.
.

Em meio a essa facilidade, o esforço e incentivo científico se expandia nos EUA.

> Os primeiros nós da rede em 1969 estavam na Universidade da Califórnia em Los Angeles, no SRI (*Stanford Research Institute*), na Universidade da Califórnia em Santa Barbara e na Universidade de Utah. Em 1971, havia 15 nós, a maioria em centros universitários de pesquisa (CASTELLS, 2003, p.16).

Foi a partir da expansão dessa rede no meio acadêmico estadunidense que se percebe a aceitação dos indivíduos presentes ao avanço dessa nova tecnologia. A seguir, a figura 2 ilustra a complexidade da rede da ARPANET em 1977. Tal complexidade facilitou a propagação das informações, sendo possível, também, perceber um fenômeno de "bola de neve" acerca do desenvolvimento das TIC's, pois ao se aprofundar no objeto de estudo, cada vez mais o processo de compartilhamento foi facilitado pelos próprios cientistas na época.

Figura 2 – Mapa da Rede ARPANET em 1977



Fonte: ARPANET, 1977

Em meio ao seguimento das pesquisas, o projeto da Arpanet foi implementado por uma rede integrada de professores do MIT, Harvard e a firma de engenharia acústica *Bolt, Beranek and Newman* (BBN) fundada pelos próprios professores (CASTELLS, 2003). Foi Robert Elliot Kahn, um dos estudiosos da BBN e responsável pelas pesquisas acerca da Arpanet, quem organizou a primeira Conferência Internacional de Computadores e Comunicação em Washington, no ano de 1972 (DENNIS, 2021). Tal conferência possibilitou a apresentação do Projeto da Arpanet para o mundo.

Os estudos continuaram a ser elaborados e, em 1973, Robert Kahm e Vint Cerf, da Universidade de Stanford, publicaram um artigo delineando a arquitetura básica da Internet (CASTELLS, 2003). Tal estudo foi de suma importância para que o projeto da Arpanet pudesse ser utilizado para o desenvolvimento de outros tipos de sistemas, sendo a Arpanet transferida para um novo departamento, a *Defense Communication Agency* (DCA) (CASTELLS, 2003). Feito isso, um dos sistemas criados foi a *Defense Data Network* que, posteriormente, viria a ser a MILNET, uma rede independente para uso militar específico dos estadunidenses (CASTELLS, 2003). Vale ressaltar que ainda nessa época, o domínio da internet estava limitado inteiramente ao governo estadunidense, sendo os EUA patrono de toda essa nova inteligência. Ademais, percebe-se a intenção de aplicação da Internet como um instrumento de defesa militar por estar intimamente ligado à essa esfera do governo dos Estados Unidos.

Tendo em vista o uso promissor dessa tecnologia nos meios governamentais, em meados da década de 1980, o serviço de inteligência, *National Science Foundation* (NSF), começa a se interessar pelas tecnologias de rede, e inicia o *CS-net Project, Computer-Science Network project* (CERF, 2007, p. 15). Por meio desse projeto, a NSF montou sua própria rede de comunicações entre computadores nessa mesma década. Porém seu controle sobre a Net não durou muito tempo e a NSF decidiu privatizar a Internet afim de regulamentar as telecomunicações plenamente (CASTELLS, 2003). A decisão do governo dos Estados Unidos de privatizar essa rede de comunicação leva à tona uma das principais questões da Internet: a dificuldade de se regular tal área e responsabilizar seus atores, logo há possiblidade de agir na rede em anonimato. Além disso, o avanço na área da informática fomentava a possibilidade de introduzir na sociedade a utilização dessa nova rede, criando um novo mercado consumidor que se demonstrava cada vez mais promissor.

Considerando isso, a criação dos computadores pessoais determinou um importante fator para a popularização da Internet e, em 1976, o engenheiro da empresa HP, Steve Wozniak, construiu o *Apple-1*. Posteriormente, junto a Steve Jobs e Ronald G. Wayne, a empresa mundialmente famosa hoje viria a ser fundada, a *Apple Computer* (APPLE-1 REGISTRY, 2022). Desse modo, o primeiro computador de uso pessoal fora lançado marcando o começo de sua popularização e, enquanto isso, outras empresas demonstraram interesse neste novo mercado, aperfeiçoando essa tecnologia e tornando-a mais acessível. Então, foi em 1981 que a empresa de tecnologia *International Business Machines Corporation* (IBM) lança seu *Personal Computer* (PC) com um gerenciador de interface inovador da empresa *Microsoft*[15] tornando-se um sucesso de vendas (GADELHA, [s.d.]). Assim, há uma sucessão de aprimoramentos tecnológicos dos PC que fomentam a sua chegada no cotidiano das pessoas, tais como: o uso de ícones e mouse pelo *Macintosh* em 1984 (GADELHA, [s.d]); o sistema operacional *Windows* da *Microsoft* em 1981 (SILVEIRA, 2007); a junção do fax, modem, secretária eletrônica, scanner, acesso à Internet e drive para CD-ROM nos PC; o lançamento do DVD em 1996 (GADELHA, [s.d]); os computadores portáteis (*laptops* e *palmtops*) (GADELHA, [s.d]), dentre outros. Considerando essa série de atualizações, os PC's passam a estar mais presentes na vida das pessoas a partir da década de 1990 e, consequentemente, a internet também.

Com as bases de mercado sendo pré-estabelecidas pela chegada dos PC's e a tecnologia da Internet em domínio público, muitos provedores de serviços da Internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais no início da década de 1990. A partir de então, foi possível o crescimento da Internet em uma escala de rede global de computadores. Outro fator que contribuiu para sua popularização foi a criação de um projeto de hipertexto global, a *World Wide Web* (WWW) por Tim Berners-Lee em 1989-1990 (KENSY e GRANDO, 2016); (CASTELLS, 2003)[16]. Berners-Lee "definiu e implementou o software que permitia obter e acrescentar informação de e para qualquer computador conectado através da Internet: HTTP, MTML e URI (mais tarde chamado URL)" (CASTELLS, 2003, p.21). Esse sistema é responsável pela maneira como acessamos e enxergamos a Internet, por meio de

[15] Dá-se o nome de gerenciador de interface, pois "o Windows só começa a ser tecnicamente considerado como um SO a partir da versão Windows NT, lançada em agosto de 1993" (SILVEIRA, 2007).
[16] O primeiro site da World Wide Web criado por Tim Berners-Lee ainda pode ser acessado no seguinte link: https://www.w3.org/People/Berners-Lee/ (W3, 2022).

navegadores com endereços (*sites*) que acessam janelas (LOPES, 2013). Após isso, o *design* foi aperfeiçoado com o tempo, resultando na modelagem que conhecemos atualmente.

Em virtude dos aspectos abordados, tem-se o avanço das TIC's no século XX ocasionando o início da era da Internet na década de 90 e sua continuidade/popularização no início do século XXI. Assim, os conhecimentos foram descentralizados a partir de uma rede de computadores que permitiu e facilitou o intercâmbio de ideias e pesquisas científicas. Os Estados Unidos como pioneiro dessa tecnologia se beneficiaram do cenário internacional da Guerra Fria e investiram em recursos para pesquisas militares voltadas a guerra, dando um importante papel às universidades. As pesquisas financiadas pelo governo nas universidades permitiram a aceleração do desenvolvimento na área das TIC's e, também, geraram interesses de empresas privadas ao perceberem o mercado promissor em volta dessas invenções. Esse interesse do setor privado e a dificuldade de regulamentação do governo estadunidense abriu portas para a mudança de aplicação da internet como instrumento puramente militar para uma tecnologia de domínio público e que seria capaz de gerar impactos no mundo.

3.1.1 Os efeitos da internet na sociedade internacional

Após se aprofundar na história das TIC's e, principalmente, na gênese da Internet é possível perceber a grandiosidade dessas invenções e pressupor que haja impactos na utilização delas no cotidiano das pessoas e, até mesmo, dos Estados no sistema internacional. Sendo assim, neste tópico busca-se compreender os efeitos das redes de computadores no sistema internacional, priorizando a Internet, partindo do indivíduo (em escala micro) até abranger a sociedade internacional (em escala macro). Para isso, leva-se em consideração que as aplicações das redes de computadores podem ser empregadas em esferas distintas da sociedade contemporânea, abrangendo finalidades comerciais e domésticas (TANEMBAUM e WETHERALL, 2011). Para além disso e como finalidade da seguinte pesquisa, agrega-se a esta análise o emprego no fator político, também, ao perceber a influência dessas tecnologias no setor político.

Antes de tudo, é importante salientar que tecnologia é cultura material,

> produzida em um processo social em um determinado ambiente institucional com base nas ideias, valores, interesses e conhecimentos de seus produtores, tanto de seus primeiros produtores quanto de seus produtores posteriores. (CASTELLS, 2013, p.9, tradução nossa,)[17].

Tendo isso em consideração, pode-se afirmar que toda tecnologia já produzida no mundo é fruto das ideias, valores, interesses e conhecimentos de quem as produz, sendo seus usuários responsáveis por se apropriarem e adaptarem a tecnologia criando um ciclo perpétuo que se retroalimenta de novas informações e produz novos conhecimentos (GRIMALDI e MIRANDA, 2015), assim como o efeito "bola de neve" citado anteriormente. Esse novo ciclo influenciou o momento presente dos indivíduos na criação do saber científico, o que permitiu as TIC's o resultado de uma nova estrutura social, a "sociedade global em rede", implicando no aumento da velocidade de propagação de informações no mundo e fortalecimento do processo de globalização. Esse momento é caracterizado também pelo surgimento da cultura da autonomia (CASTELLS, 2013).

O fomento da cultura da autonomia a partir do avanço das tecnologias pode parecer contraditório ao processo de globalização propagado no século XXI, mas é por meio da liberdade conquistada pelas TIC's que ocorreu/vem ocorrendo o ganho dessa autonomia pelo processo de individuação (CASTELLS, 2013). Esse processo é um fator importante de análise dessa pesquisa pois, dentro do campo das RI, nos permite refletir sobre a natureza dos atores no sistema internacional e Ciberespaço. Afinal, a partir dessa mudança, qual seria o ator principal a operar no Ciberespaço e sistema internacional? Desde a conquista dessa liberdade por meio do Ciberespaço, os indivíduos se tornariam atores relevantes o suficiente para gerarem mudanças sistêmicas? Respectivamente, como apresentado no primeiro capítulo, o Ciberespaço possui quase os mesmos fundamentos de poderes e relações que o sistema internacional, logo, seu ator principal tende a ser o Estado e os indivíduos encontram dificuldades ao atuarem isolados no sistema a ponto de criarem alterações sistêmicas. Porém, mesmo que o ator principal seja o Estado, é preciso destacar o aumento da capacidade do indivíduo de participar mais ativamente no sistema internacional por causa das redes de computadores.

[17] "It is produced in a social process in a given institutional environment on the basis of the ideas, values, interests, and knowledge of their producers, both their early producers and their subsequent producers."

Embora o indivíduo não seja a peça principal no funcionamento do Ciberespaço e sistema internacional, ele não deixa de estar presente e teve sua participação aumentada nas esferas sociais, econômicas e políticas do mundo com o advento da Internet (CASTELLS, 2013). Um caso que exemplifica o poder de atuação dos demais atores não estatais é o *Wikileaks*. A organização fundada por Julian Assange em 2006 foi responsável pela divulgação de dados confidenciais dos EUA, gerando repercussão mundial ao compartilhar nas redes inúmeros documentos que expunham crimes de guerra e espionagem por meio de documentos diplomáticos, além do vazamento do vídeo sobre o ataque aéreo de Bagdá de autoria do mesmo país em 12 de julho de 2007(Figura 3) (ENTENDA, 2019).

Figura 3 – Cortes do vídeo vazado pelo *Wikileaks* sobre o ataque aéreo em Bagdá

Fonte: WIKILEAKS, 2010

Portanto, a autonomia conquistada pelos atores sociais pode acarretar num modo de democratização das informações e política também, já que passa a se permitir uma maior participação das pessoas no acesso, debate e construção de ideias em assuntos diversos por meio da Internet (DE MIRANDA; DE FRAGA, 2017). Com isso, verifica-se uma maior interferência dos usuários das redes nas questões políticas definindo seus projetos específicos em interação, sem a submissão das instituições da sociedade (CASTELLS, 2013). Retomando o caso de Assange, o indivíduo perde poder ao se retirar do Ciberespaço pois não possui condições de concorrer com um ator como o Estado, muito menos uma potência do sistema internacional como os EUA. Embora tenha sido exposto diversas contravenções que ferem diretos internacionais, Assange foi perseguido desde o início do vazamento dos documentos em 2007, ficando 7 anos em asilo político na embaixada do Equador em Londres para depois ser detido em 11 de abril de 2019 pela polícia britânica (WESEL, 2022; ENTENDA, 2019).

O principal local do Ciberespaço responsável pela conexão entre os usuários da Internet são as redes sociais, porque elas se tornaram plataformas escolhidas para todo o tipo de atividades, como: amizades pessoais, *marketing*, *e-commerce*, educação, cultura, criatividade, mídia e distribuição de entretenimento, aplicações de saúde e ativismo sociopolítico (CASTELLS, 2013). Atualmente, o número de usuários das redes sociais no mundo são 4.62 bilhões de pessoas, ou 58,4% da população mundial e 93,4% de usuários da Internet (WE ARE SOCIAL e HOOT SUITE, 2022), e é por meio do uso desse local do Ciberespaço que se percebe "os meios de comunicação de massa (...) [como] ferramentas chave para mediar a comunicação e afirmar o poder (...)" (CASTELLS, 2013, p.17, tradução nossa)[18]. Decorrente desse uso, o espaço virtual se tornou uma importante ferramenta eficaz na legitimação de poder dos Estados, porque funciona como mais um meio de comunicação entre governo-sociedade, além das relações indivíduo-indivíduo. E isso demonstra que, cada vez mais, essas relações são moldadas e decididas no campo da comunicação.

O potencial do Ciberespaço como instrumento político está relacionado com o aumento da abordagem de temáticas sobre Ciência e Tecnologia (C&T) no próprio meio político. Esse desdobramento ocorre devido à grande adesão de assuntos sobre C&T nas agendas políticas de países desenvolvidos, se tornando imediata a associação desse tópico com o grau de

[18] "(…) the mass media have been key tools of mediating communication and asserting power (…)"

desenvolvimento de um país (GRIMALDI e MIRANDA, 2015). Por causa disso, constata-se a dependência do mundo, e consequentemente do sistema internacional, a produção de conhecimentos científicos e tecnológicos, principalmente advindos das TIC's, já que passaram a ser peças fundamentais das relações e ações internas e externas dos Estados.

A internet como uma grande invenção correlata ao Ciberespaço se comprovou apta em alterar o comportamento da sociedade global. O fenômeno da globalização conectou toda uma estrutura complexa pautada em diferentes aspectos e com divisões econômicas, sociais, políticas, culturais, religiosas e também jurídicas, confirmando seu fortalecimento (SANTOS, 2011 apud DE MIRANDA; DE FRAGA, 2017). A conexão nesse grau de profundidade não seria possível sem o desenvolvimento das TIC's que aumentaram a velocidade de propagação de informações e permitiram mais facilidade nas relações entre Estado-Estado, Estado-não Estado, não Estado-não Estado.

3.2 O que é o Ciberespaço?

Frente à transformação do mundo físico para o virtual surge uma nova realidade. O que antes era concreto e tátil, se modificou para algo sensorial e digital. Essa virtualidade traz ao mundo uma certa noção de infinito, um mundo sem barreiras, de conexão entre seus usuários e aumento na velocidade da troca de informações. A partir disso, percebe-se a alteração no modo de se relacionar das pessoas e o sentido da mensagem não é mais produzido apenas pelos seus autores, mas sim pela interatividade de todos os sujeitos também (RAMAL, 2002). Em consequência disso e com o desenvolvimento das TIC's, apresenta-se um novo momento da cultura na sociedade da informação, criando uma nova maneira de lidar com a leitura, escrita entre outras artes denominadas como cultura pós-moderna ou cibercultura (MONTEIRO, 2007 apud RAMAL,2002). Portanto, o que difere a cultura da cibercultura é justamente a estrutura na qual ela está inserida, o que demonstra a importância da definição desse meio, o Ciberespaço, para se entender os desdobramentos dessa nova era.

Como resultado do desenvolvimento das TIC's, o Ciberespaço manifesta-se como um ambiente para além do mundo físico e, apesar de ainda não ter um conceito consensual, está presente nas Relações Internacionais e possui seu próprio campo de estudo a ser desenvolvido (LOPES, 2013). Em prol dessa presença nas RI, neste tópico serão apresentados alguns dos

principais conceitos para o Ciberespaço e suas dificuldades epistemológicas que, de certa maneira são obstáculos encontrados na utilização do espaço cibernético pelos atores internacionais também.

Dessa maneira, o termo Ciberespaço foi utilizado pela primeira vez no conto *Burning Chrome* do autor estadunidense Willian Gibson em 1982 (KELLNER, 2001 apud MONTEIRO, 2007, AZEVEDO; MONTEIRO, 2010). Contudo, é comum encontrar na literatura que o termo Ciberespaço foi cunhado por Gibson em seu livro "*Neuromancer*" publicado em 1984 (MONTEIRO, 2007) devido sua popularidade. É baseado nessa obra literária que os primeiros conceitos sobre esse espaço virtual foram suscitados e saíram apenas do campo da ficção. Em vista disso, Pierre Lévy, filósofo pesquisador das tecnologias de inteligência e investigador das interações entre informação e sociedade, define o Ciberespaço nomeado na obra de Willian Gibson como:

> o universo das redes digitais como lugar de encontros e de aventuras, terreno de conflitos mundiais, nova fronteira econômica e cultural. […] O ciberespaço designa menos o suporte de informação do que os modos originais de criação, de navegação no conhecimento e de relação social por eles propiciados. (LÉVY, 1998, p.104 apud MONTEIRO, 2007)

Ainda que de maneira simplória, entende-se o que Gibson inaugurou ao utilizar o termo Ciberespaço em suas obras. A partir da compreensão de Lévy, a intenção do autor da obra de ficção científica é de enxergar o espaço virtual como um ambiente a ser explorado suscetível a descobertas e enfrentamentos, além de estar apto a impactar no mundo real e ocasionar mudanças econômicas e culturais.

Afim de dar início à exploração desse ambiente, conceitos sobre o espaço virtual foram desenvolvidos no mundo científico, apresentando diferentes abordagens que se complementam e debatem entre si na busca pelo seu entendimento. Dando continuidade ao pensamento do autor citado anteriormente, Pierre Lévy, o Ciberespaço é "o espaço da comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores" (1999, p. 92). Partindo dessa concepção, o Ciberespaço adquire como característica um ambiente puramente virtual habilitado à troca livre de informações e que possibilita a comunicação por meio das redes de computadores, sendo este um plano a parte da realidade. Desse modo, leva-se em consideração

que esse ambiente digital não está sujeito aos limites físicos no qual as pessoas estão acostumadas a lidar no dia-a-dia, como por exemplo a distância.

Entretanto, em oposição à ideia anterior de virtualidade completa desse espaço, Koepsell enfatiza o aspecto físico do Ciberespaço como fundamental e o define como:

> um meio composto de chips de silício, fios de cobre, fitas e discos magnéticos, cabos de fibra ótica e de todos os outros componentes de computadores, meios de armazenamento e redes que armazenam, transmitem e manipulam bits. [...] O software existe no ciberespaço como o texto existe no papel ou como uma estátua existe em uma pedra. (2004, p. 125).

Essa abordagem trata o espaço virtual cibernético como um resultado dos componentes físicos citados pelo autor e ainda acrescenta que o espaço cibernético se manifesta da rede de computadores em expansão, a Internet (KOEPSELL, 2004; MONTEIRO, 2007; RABAÇA e BARBOSA, 2001). Ainda em conformidade à mescla desses conceitos, o ambiente virtual com a Internet, Santos e Ribeiro definem o Ciberespaço como "um conjunto de computadores e serviços que constituem a Internet" (2003 apud MONTEIRO, 2007, [s.p.]) também. Esse pensamento pode acarretar em alguns prejuízos ao se aprofundar na compreensão do mundo virtual, pois ao se considerar a Internet como o meio único e exclusivo desse espaço todo o restante de seus componentes é ignorado.

Então, afirmar que a constituição do Ciberespaço advém da Internet, pode-se considerar uma falácia que incita ao erro no momento de se buscar tal definição[19]. A falácia é formada quando se sustenta que: a Internet é um componente do Ciberespaço, logo todo o Ciberespaço é Internet. Sendo assim, torna-se necessário diferenciar o espaço cibernético e a Internet. Para isso, considera-se que a Internet está em sua totalidade inserida no ambiente cibernético e é um elemento desse local, mas esse ambiente cibernético é formado por outros elementos para além da Internet e não está conectado a ela integralmente (CLARKE e KNAKE, 2012). Portanto, Clarke e Knake (2012 apud PORTELA, 2016, p. 92) ainda conceituam "o espaço cibernético como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou

[19] A falácia é um raciocínio que parece lógico e verdadeiro, porém existe alguma falha que o faz ser falso (FONTES, [s.d]).

submetidas aos seus controles". Ademais, um fator que distingue essa relação de igualdade entre os conceitos do Ciberespaço e Internet é que ele não precisa dela para existir (PORTELA, 2016).

Retomando às considerações a respeito dos aspectos físicos e virtuais para construir o conceito de Ciberespaço, tem-se que ambos os aspectos são importantes na constituição desse meio digital, como um complexo híbrido que é integrado por propriedades virtuais e físicas (NYE, 2010). Desse modo, Daniel T. Kuehl realiza essa junção em sua definição, considerando-o um:

> [...] domínio global dentro do ambiente da informação [...] moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar e explorar informação através das redes interdependentes e interconectadas utilizando tecnologias de informação e comunicação (2009 apud KENSY e GRANDO, 2016, p56-57).

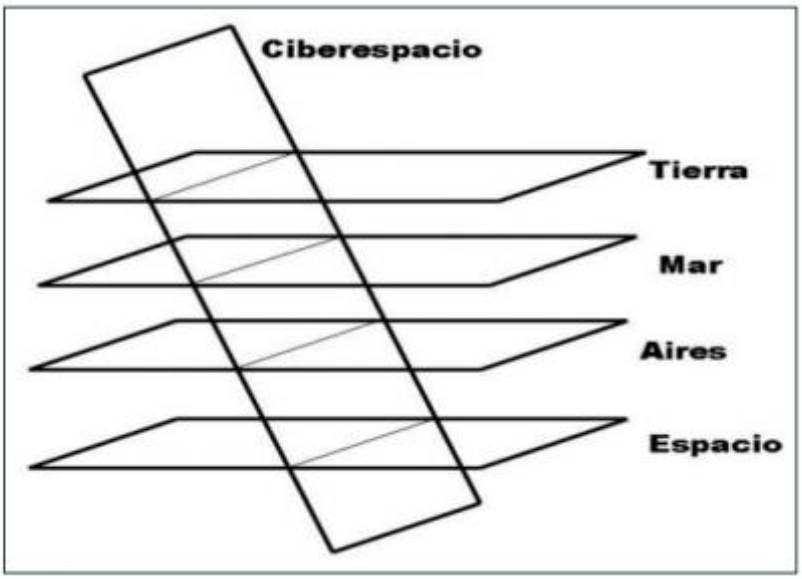
Em vista disso, ao se abordar matérias da eletrônica e do eletromagnetismo é possível fazer referência à adesão do meio físico ao virtual devido ao desdobramento dessas matérias em questão que beneficiam a criação de novas tecnologias, além de serem compostas por elementos físicos (placas eletrônicas, bobinas, fios, entre outros) que contribuem para a criação do meio virtual (lógicas de programação, algoritmos, entre outros).

Além dos quesitos estruturais já apresentados, a definição demonstrada por Daniel Ventre (2011) agrega a figura dos usuários do Ciberespaço a esse ordenamento. Para Ventre, deve-se considerar três aspectos ao se tratar do Ciberespaço: o *hardware*, o *software* e o *peopleware*. Sendo que os aspectos tratam, respectivamente, do conjunto de equipamentos físicos; a dimensão virtual com sistemas, programas, aplicativos e conteúdo de dados e informações; e a camada cognitiva dos usuários. Abordagens como essa destacam o fato de o espaço cibernético não ser um ambiente puramente virtual, pois ele possui, também, parte no mundo físico, como a infraestrutura para armazenamento de dados e as pessoas que utilizam os computadores e outros dispositivos que estão conectados ao Ciberespaço (SINGER e FRIEDMAN, 2014). Com esse seguimento, ratifica-se a perspectiva da presença do Ciberespaço no cotidiano social das pessoas e a dependência desta tecnologia na sociedade contemporânea (KENSY e GRANDO, 2016).

Outro fator importante ao se discutir sobre o espaço cibernético é recordar de que ele não é um espaço natural, como por exemplo, os espaços terrestre e aéreo. Esse novo espaço em questão foi criado pelo próprio homem (KENSY e GRANDO, 2016) e, em virtude disso, se

difere dos demais sobre o aspecto da interconectividade (PORTELA, 2016). Desse modo, Ventre (2011) determina que o Ciberespaço permeia todos os demais espaços geográficos, como mostrado na figura a seguir:

Figura 4 - Relação de interconectividade do Ciberespaço com os demais espaços geográficos



FONTE: Ventre (2012, p.55 apud PORTELA, 2016, p.94)

Considerando a ideia apresentada, entende-se que por meio do Ciberespaço é possível a interação com os demais espaços geográficos e que nos espaços geográficos existem pontos de acesso ao próprio espaço cibernético (VENTRE, 2011). Por meio dessa, as ações no meio virtual podem gerar consequências nos meios físicos. Um exemplo clássico para isso é o *Stuxnet*, um *worm* que infectou o *software* de uma usina nuclear no Irã e comprometeu seu funcionamento se tornando uma ameaça ao governo iraniano em 2010 (KUSHNER, 2013).

Agora que já foi apresentado importantes aspectos na compreensão do espaço cibernético como: a diferenciação de Ciberespaço e Internet; virtualidade *versus* materialismo; os usuários como parte do Ciberespaço; e a interconectividade do espaço virtual com os demais espaços geográficos; cabe definir se o Ciberespaço se trata de um instrumento ou se pode realmente ser considerado um ambiente. Portanto, adiantando os resultados desse questionamento, o espaço cibernético pode ser considerado e utilizado, ora como ferramenta (meio), ora como ambiente (fim) (ACÁCIO, 2016). Esse argumento pode ser justificado com o auxílio de uma reflexão

geográfica, afim de apresentar mais uma questão acerca das características do Ciberespaço, sendo essa versatilidade um importante fator da sua utilização pelos Estados em suas agendas de segurança e defesa nacional.

Portanto, por se tratar de um ambiente artificial é indissociável a questão da técnica para a construção desse espaço. Com isso, Milton Santos compreende as técnicas como "um conjunto de meios instrumentais e sociais, com os quais o homem realiza sua vida, produz e, ao mesmo tempo, cria espaço" (2002, p.29 apud AZEVEDO e MONTEIRO, 2010, p.140). Sendo assim, a técnica é um intermediário entre o homem e o meio (neste caso, a técnica é a ferramenta). Com o passar dos anos e a aceleração tecnológica do século passado até os dias atuais, houve uma alteração na concepção materialista do espaço, no qual ocorre a diminuição do espaço e a intensificação do tempo.

Figura 5 – A compreensão do espaço e do tempo

Fonte: HARVEY, 1992, p.220 apud AZEVEDO e MONTEIRO, 2010, p.140

Essa mudança de concepção é entendida como a “revolução da técnica”, onde nota-se que com o aumento da presença das TIC’s ao longo dos anos, esse fenômeno assume um grau de autonomia em que “não apenas se soma ao meio comprimindo o espaço, [mas] também gera um outro espaço, artificial e dotado de características peculiares, o ciberespaço.” (AZEVEDO e MONTEIRO, 2010, p. 141). Posto isso, a figura 5 ilustra a diminuição do espaço em relação ao tempo a partir da intensificação do desenvolvimento das técnicas no mundo a ponto de conceber o espaço virtual, podendo considerá-lo num momento como instrumento, outro momento como ambiente. Ainda seguindo a lógica utilizada por Harvey na figura anterior, houve a intensificação do desenvolvimento das tecnologias voltadas para a comunicação e informação a partir da década de 1960, no qual aumenta-se tanto a velocidade de propagação de dados a ponto de criar um outro ordenamento dentro do sistema internacional.

Portanto, um fator impactante no mundo material desde a inauguração do Ciberespaço é a maneira como ele é utilizado pelos Estados e como eles se comportam nesse ambiente. Entender sobre as questões técnicas desse ambiente se tornou fundamental para as relações do Estados atualmente devido à inserção de atores diversos nesse universo permitindo identificar ameaças ou apenas exercer sua expansão de influência naquele local. A busca pelo desenvolvimento C&T ocorre por questões políticas, sociais, econômicas e de segurança e, assim como qualquer tecnologia, não produz efeitos por si só.

4. PANORAMA DO MODO DE ATUAÇÃO DO ESTADO NO CIBERESPAÇO

Em vista de todos os pontos abordados na pesquisa até aqui é perceptível a interferência do Ciberespaço no ordenamento do sistema internacional, principalmente no comportamento de seus atores. Neste capítulo será introduzido como acontece a participação dos demais atores no Ciberespaço e essa análise será aprofundada no Estado em específico. A partir da presença do Estado no espaço virtual, percebe-se uma série de adaptações políticas acerca do fenômeno da globalização e ascensão da cibercultura. Essas adequações podem ser percebidas por meio de alterações nos tópicos das agendas de segurança dos países e na maneira de administrar o poder internamente e em suas RI. Em meio a isso, os parâmetros considerados para averiguar a diferença de poder cibernético entre os Estados e a utilização eficiente do Ciberespaço são as capacidades e as vulnerabilidades desses atores, assim busca-se compreender a relação entre elas.

Por fim, após a apresentação de tais conceitos, será possível relacioná-los à busca por compreender as capacidades e vulnerabilidades cibernéticas do Estado. O conceito desses parâmetros nas RI pode indicar a maneira como o Estado lida com essas questões e conduz suas ações atualmente. Portanto, será realizada uma breve revisão teórica sobre esses conceitos.

4.1 Os atores no Ciberespaço

Antes de tudo, a abordagem considerada para a definição dos atores internacionais neste estudo será a de Castro, a qual determina que os atores internacionais são

> [...] os entes que exercem, influenciam ou moldam, direta ou indiretamente, o cenário internacional por meio da interação de inputs e outputs. [Atores internacionais] exprimem o exercício de titularidade, de representatividade e de capacidade de influência, de mando e de alteração dos atos e fatos internacionais (2012, p.428).

Esse perfil se aplica também aos atores no espaço virtual, pois a maneira de agir no Ciberespaço está vinculada à estrutura sistêmica internacional também, o que expõem esse ambiente aos mesmos confrontos e desafios, como já apresentado no capítulo 1, apesar de suas particularidades. Outro ponto a se considerar são que as unidades existentes no mundo físico são as mesmas para o Ciberespaço para este estudo e com faculdades de influência diferentes entre

eles podendo haver alterações substanciais em seus papéis e capacidades (no sentido de haver recursos).

Então, ao se tratar de segurança cibernética os demais atores não estatais possuem importância considerável apesar da abordagem tradicional de se pensar o conflito entre dois Estados (FERNANDES, 2012). Isso ocorre devido ao ganho de autonomia dos atores não estatais que por meio dessa liberdade se tornam elementos mais ativos no sistema internacional e, por isso, os Estados encontram dificuldades de controlar o Ciberespaço da mesma maneira em que controlam os demais ambientes aéreo, marítimo e terrestre (RATTRAY, 2009 apud MESQUITA, 2019). Entretanto, existem diferentes potencialidades entres os dois elementos, sendo o Estado uma unidade mais complexa e preparada para manejar o espaço virtual. Essa diferença potencial pode ser vista por meio da observação nas concepções de autonomia e capacidade tecnológica (recursos) desses atores. Segue a tabela com as diferenças:

Tabela 2 – Diferenças de potencialidade entre os atores Estatais e Não-estatais

Tipo de ator / **Conceitos**	**Não estatal**	**Estado**
Autonomia	Mais Liberdade de expressão/participação	Plena (inerente) à estrutura do Estado
Capacidade tecnológica	Tecnologia simples e acessível	Tecnologia complexa, de maior valor agregado e estratégica

FONTE: Elaborado pela autora

Através dessa diferenciação percebe-se a complexidade da estrutura utilizada pelo Estado para o Ciberespaço devido à adoção de tecnologias de alto nível que permitem a ele manter sua soberania e autonomia nas RI. Em contrapartida, os atores não estatais adquirem certa liberdade de expressão e participação por meio de tecnologias simplórias e que podem ser facilmente conseguidas por civis (como por exemplo, um Computador). Porém, mesmo que haja um maior

ganho potencial pelos atores não estatais, o Estado continua possuindo vantagens prevalecentes em termos de poder cibernético.

Como citado no capítulo anterior, esse ganho de liberdade ou "democratização" dos demais atores é fundamental na conquista pela autonomia. Assim, esses atores adquirem um maior ganho de potencial ao poderem articular de maneira mais eficiente sobre as informações e em questões políticas abordadas no Ciberespaço, como por exemplo em movimentos sociais (DE MIRANDA; DE FRAGA, 2017). Porém, mesmo que notável, tal ganho não é o suficiente para ultrapassar as vantagens do Estado com todo seus sistemas de rede multifacetados.

Dessa maneira, as mudanças do cenário atual ocorrem devido a maior pluralidade de atores no sistema internacional que possuem capacidade de influência também (MARIANO, PIGATTO e ALMEIDA, 2018). Em vista disso, Nye (2012 apud MESQUITA, 2019) categoriza os atores no espaço cibernético em três grupos: (i) governos, (ii) organizações com redes altamente estruturadas e (iii) indivíduos e redes fracamente estruturados. O autor, também, dispõe de quadros em sua obra que expõem resumidamente esses atores com suas potencialidades e vulnerabilidades (NYE, 2012, p.174 apud MESQUITA, 2019, p.10).

Quadro 1- Governo como ator no Ciberespaço

Principais governos
[Recursos/potencialidades:] 1. Desenvolvimento e apoio de infraestrutura, educação e propriedade intelectual. 2. Coerção legal e física de indivíduos e intermediários localizados dentro das fronteiras. 3. Tamanho do mercado e controle do acesso – por exemplo, União Europeia, China, Estados Unidos. 4. Recursos para ataque e defesa cibernéticos: burocracia, orçamentos, agência de inteligência. 5. Provisão de bens públicos, como as regulações necessárias para o comércio. 6. Reputação para a legitimidade, benignidade e competência que produzem poder brando. **Principais vulnerabilidades:** alta dependência de sistemas complexos facilmente danificáveis, instabilidade política, possível perda de reputação.

Fonte: NYE, 2012, p. 174 apud MESQUITA, 2019

Quadro 2 – Organizações e redes altamente estruturadas como atores no Ciberespaço

Organizações e redes altamente estruturadas
[Vantagens/potencialidades:] 1. Grandes orçamentos e recursos humanos, economias de escala. 2. Flexibilidade transnacional. 3. Controle de desenvolvimento de código e produto, geração de aplicativos. 4. Marcas e reputação. **Principais vulnerabilidades:** perseguição legal, roubo de propriedade intelectual, danos a sistemas, possível perda de reputação (denúncias).

Fonte: NYE, 2012, p. 174 apud MESQUITA, 2019

Quadro 3 – Indivíduos e redes fracamente estruturadas como atores do Ciberespaço

Indivíduos e redes fracamente estruturadas
[Vantagens/potencialidades:] 1. Baixo custo de investimento para a entrada. 2. Virtual anonimato e facilidade de saída. 3. Vulnerabilidade assimétrica em comparação aos governos e às grandes organizações. **Principais vulnerabilidades:** coerção legal e ilegal por parte dos governos e das organizações, caso sejam apanhados

Fonte: NYE, 2012, p. 174 apud MESQUITA, 2019

Sendo assim, ao categorizar cada um dos atores, percebe-se pontos que acentuam a participação deles no Ciberespaço, demonstrando o ganho de maior participação dos atores não estatais no sistema internacional apresentando organizações e redes altamente estruturadas para além da atuação dos simples indivíduos.

Embora haja a possibilidade de maior presença, ainda existe a disparidade do Estado e o desenvolvimento de tecnologias com relação aos demais atores. Essa diferença esclarece que as interações baseadas no meio cibernético não dispensam as maneiras tradicionais de articulação de interesses e agregação, nacional ou internacionalmente, servindo como uma maneira de desafiar a ordem estabelecida (CHOUCRI, 2012). Um exemplo para isso foi a Primavera Árabe em 2011,

um acontecimendo que foi impulsionado pelo Ciberespaço e acarretou em agitações nos Estados envolvidos, alterando o ordenamento existente[20].

Ademais, Nye (2010) também apresenta a não existência de uma governança global única que se encarregue do Ciberespaço, mas sim uma série de instituições autônomas, configurando mais um ator que se encaixa neste intermédio de potencial. Choucri (2012), ainda acrescenta que ocorre o

> [...] crescimento e poder sem precedentes das instituições para gerenciamento cibernético, em grande parte entidades privadas criadas especificamente para permitir e gerenciar interações cibernéticas (como a Corporação da Internet para Atribuição de Nomes e Números – ICANN, em inglês), ou para ajudar dar suporte à segurança cibernética (como o Consórcio para Soluções de Tecnologia de Confiabilidade Elétrica – CERTS, em inglês) (CHOUCRI, 2012, p.9, tradução nossa[21]).

Por fim, percebe-se a importância dos demais atores não estatais que com o advento do Ciberespaço ganharam significante potencial por meio da capacidade de influência e já geram interferências no Estado Vestfaliano e seu sistema internacional (CHOUCRI, 2012). Esse último ator citado será aprofundado em seguida.

4.2 O Estado e o Ciberespaço

Para compreender o comportamento dos Estados no Ciberespaço, David Betz, em sua obra "*Cyberspace and the State: Toward a Strategy for Cyber-Power*", afirma que:

> Os Estados são obviamente atores importantes e continuarão a sê-lo, mas sua presença online compete por influência com uma ampla gama de entidades que abraçam as oportunidades do ciberespaço para seus próprios propósitos. Estes variam de cidadãos individuais a organizações da sociedade civil e empresas comerciais, desde terroristas e insurgentes a ramos do poder estatal (militares, agências de inteligência, etc.) a instituições globais multilaterais e conglomerados de mídia, de nós individuais a todas as redes e não humanos na forma de hardware e software também. Cada um procura usar o

[20] A autora Nazli Choucri utiliza o exemplo do Wikileaks. Neste evento "o estado não é propenso a aceitar, ou mesmo acomodar, a tais tendências" (CHOUCRI, 2012, p.10, tradução nossa).

[21] "Unprecedented growth and power of *institutions for cyber management*, largely private entities created specifically to enable and manage cyber interactions (such as Internet Corporation for Assigned Names and Numbers and Internet Engineering Task Force), or to help support cyber security (such as Consortium for Electric Reliability Technology Solutions)".

> ciberespaço para buscar seus próprios fins, sejam estes individualmente ou em conjunto com outros. (2011, p. 38, tradução nossa[22])

Por meio do exposto, o Estado no Ciberespaço é considerado um ator de relevância, porém não são os únicos a se beneficiarem desse meio. Assim como na lógica de funcionamento do sistema internacional exposto pela escola neorrealista (e abordado no capítulo 1), os atores agirão em busca dos próprios interesses, influência e expansão de poder (CHOUCRI, 2012; BETZ, 2011). Não obstante, o Estado adota essa lógica de atuação também. Sendo assim, o uso do Ciberespaço como ferramenta para buscar esses interesses suscita a aparição do conceito de "poder cibernético".

Ao se tratar o Ciberespaço como um espaço operacional, no qual os humanos e suas organizações utilizam das tecnologias necessárias para agir e criar efeitos, esse ambiente é como qualquer um dos outros quatro domínios físicos (terra, mar, ar e espaço sideral) nos quais os atores da comunidade internacional já operam (KUEHL, 2009). Logo, se estabelece o poder cibernético para colocar o Ciberespaço dentro dos domínios operacionais e elementos de poder dirigidos pela comunidade de segurança internacional.

A partir disso, o Ciberespaço passa a integrar a agenda de segurança do Estado na qual deve se preparar para as situações de risco não apenas como políticas de governo, mas sim como questões de Estado (CRUZ, 2013). Então, acerca da temática de segurança cibernética, um dos pontos a ser esclarecido é o conceito de c*yberpower* (em inglês), ou poder cibernético, afim de analisar a ampliação de influência do poder pelas vias do Ciberespaço.

A fim de somar aos conceitos de *hardpower* e *softpower*, Joseph Nye (2011) se aprofunda no conceito de c*yberpower* a partir da análise do sufixo *power*, em português, poder. Para o autor, o poder possui três faces: 1) a de interferir nas decisões do outro em relação à atuação; 2) a de interferir nas decisões a ponto de influenciar nas configurações da agenda e discussões de assuntos do outro (questões políticas); e, 3) de exercer poder nos interesses dos outros. Posterior a

[22] "States are obviously important actors and will continue to be so, but their online presence competes for influence with a wide range of entities who embrace the opportunities of cyberspace for their own purposes. These range from individual citizens to civil society organizations and commercial enterprises, from terrorists and insurgents to branches of state power (militaries, intelligence agencies, etc.) to multilateral global institutions and media conglomerates, from individual nodes to whole networks, and non-humans in the form of hardware and software too. Each seeks to use cyberspace to pursue its own ends, whether these be individually or in concert with others."

isso, o autor agrega o prefixo *cyber* por estar relacionado a atividades eletrônicas e de informática devido o contexto a qual a relação de poder viria a ser aprofundada. Então o autor conceitua *Cyberpower* (ou poder cibernético):

> Definido comportamentalmente, o poder cibernético é a capacidade de obter resultados preferenciais através do uso dos recursos de informação interconectados eletronicamente do domínio cibernético. Em uma definição amplamente usada, poder cibernético é "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e entre os instrumentos de poder" (NYE, 2010, p. 3-4).

Portanto, o poder cibernético nada mais seria que o uso do Ciberespaço para exercer o poder. Esse poder pode ser experimentado por qualquer um dos seus atores, afinal eles estão presentes no Ciberespaço, porém ao ser utilizado pelo Estado adquire a questão da militarização (MESQUITA, 2019). Ao definir o poder cibernético militar (em inglês, *military cyberpower*), Zimet e Barry (2009) afirmam que esse poder ocorre a partir da aplicação dos recursos cibernéticos para atingir objetivos militares, incluindo missões de assistência humanitária, de estabilização, de transição e reconstrução e, principalmente, de combate bélico efetivo. Atualmente, se percebe as operações militares por meio de outros domínios (terra, mar, ar e espaço exterior) cada vez mais dependentes da eficiência do Ciberespaço. Isso demonstra a importância e influência do poder cibernético nas questões de defesa do Estado.

Essa utilização do Ciberespaço para vias militares é denominada como a militarização do Ciberespaço e ela ocorre devido à necessidade do Estado de se posicionar quanto aos assuntos cibernéticos. A busca pelo preparo de defesa às ameaças e ataque aos inimigos gera hoje uma espécie de "corrida armamentista", assim como na guerra fria, para o desenvolvimento de tecnologias voltadas ao Ciberespaço (SINGER e FRIEDMAN, 2014). A evolução de conhecimento nas áreas de informações e dados obtiveram grande avanço em um pequeno período de tempo levando em consideração a alta velocidade e a grande quantidade de informação propagada de uma década atrás até hoje.

O uso dessas tecnologias pode gerar relações conflituosas entre os elementos do Ciberespaço também, seja ele entre atores não estatais, entre Estados, e entre atores não estatais e Estados. Ao mesmo tempo que um Estado soberano procura exercer influência e estender o poder e controle sobre o domínio cibernético, ele procura reproduzir a ecologia tradicional e familiar, e sua demografia e sistemas de autoridade associados (CHOUCRI, 2012, p.4). Por isso, o

Ciberespaço é uma importante ferramenta para manter a soberania do Estado atualmente, porque por meio dela podem ocorrer conflitos que geram ataques e defesas, instaurando a Ciberguerra (em inglês, *Cyberwar*).

4.2.1 Ciberguerra e o que os Estados fazem dela

Um dos primeiros conceitos de Ciberguerra foi lavrado em 1993, por John Arquilla e David Ronfeldt. Para os autores, "a ciberguerra refere-se à condução e preparação para conduzir operações militares de acordo com os princípios relacionados à informação" (ARQUILLA; RONFELDT, 1993, p.146, tradução nossa[23]). Por causa disso, os autores tratam esse fenômeno como Guerra de Informação, porque o espaço cibernético é utilizado com o intuito de causar desordem por meio dos sistemas de informação e comunicação mesmo sem causar destruições reais no conflito, como por exemplo, a destruição de um local ou cidade.

Ainda neste estudo da década de 1990, os autores identificam o caráter militar intrínseco à Ciberguerra por meio do uso dos recursos das TIC's para "(...) questões amplas de organização militar e doutrina, bem como estratégia, tática e design de armas" (ARQUILLA; RONFELDT, 1993, p.146, tradução nossa[24]). Seu uso nas operações militares está relacionado à administração das informações para adquirir vantagens conhecendo a si próprio e ao inimigo, podendo distinguir a parte vitoriosa da guerra como a que melhor compreende as informações. Tal pensamento se aplica em conflitos de baixa e alta intensidade, em ambientes convencionais e não convencionais, além de ser útil para fins defensivos ou ofensivos (ARQUILLA; RONFELDT, 1993).

Outro ponto interessante levantado por Arquilla e Ronfeldt (1993 apud ASSUNÇÃO, 2022) é de que a Ciberguerra seria capaz de resultar na transformação da natureza da guerra. A validação dessa transformação ocorre pela comparação dos autores sobre a modernização adquirida com a captação de informações com a tática de guerra *Blitzkrieg*[25] na Segunda Guerra

[23] "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles"
[24] "In sum, cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design."
[25] Foi uma tática de guerra muito utilizada pelo exército alemão, também é Conhecida como "Guerra-relâmpago".

Mundial (LOBATO; KENKEL, 2015). Portanto, ainda que um texto do final do século XX e anterior a grande expansão sobre os assuntos cibernéticos pós-11 de setembro, os autores obtiveram resultados além do seu tempo, pois suas considerações vão de encontro aos estudos atuais.

Entretanto, enquanto os autores citados anteriormente anunciavam a chegada dessa nova modalidade da Guerra[26], alguns estudiosos se opõem a sua existência. O raciocínio utilizado pelos opositores retoma Clausewitz em sua afirmação de que a violência é um elemento essencial da guerra (ASSUNÇÃO, 2022), logo se não há o uso da violência letal, não se configura Guerra (RID, 2011). Isto posto, Rid (2011) trata as demais abordagens como um grande exagero[27], argumentando que a Ciberguerra não é precisamente uma guerra e não irá substituir a maneira tradicional da guerra como conhecemos desde os primórdios da história mundial, mas sim agregar ao conflito por meio do uso das TIC's.

Agora que foi apresentado as questões constituintes da Ciberguerra em diferentes pontos de vista, questiona-se: A Ciberguerra é de fato guerra? Afim de buscar explicações, a resposta para essa pergunta foi debatida por meio dos estudos desenvolvidos por Clausewitz sobre a natureza da guerra, buscando aplicar a variação do seu conceito em uma teoria tradicional de guerra (ASSUNÇÃO, 2022). O resultado atingido foi de que a Ciberguerra é apenas mais um elemento da Guerra e que ao afirmar a existência de uma não anula os outros meios de fazê-la (ASSUNÇÃO, 2022). Então, entende-se que a Ciberguerra faz parte das políticas de estratégia e defesa do Estado como uma alternativa, por meio dos atributos específicos da guerra cibernética, para alcançar seus interesses.

Portanto, após a exposição do debate envolto ao conceito da Guerra é possível delinear as principais características desse fenômeno pautadas na análise acadêmica de Alcântara e Da Silva (2018, p.139-140), as propriedades são:

> 1) a presença mandatória de Estados, 2) o uso de poderes assimétricos, 3) a existência de um elemento surpresa e 4) o uso de trapaça no decorrer do conflito, 5) implicações com envolvimento de IC e/ou sistemas de redes governamentais, 6) ações com motivação político-militar por detrás, 7) ações via ciberespaço, com invasão de redes

[26] O nome do artigo publicado por Arquilla e Ronfeldt é "A Ciberguerra está chegando" (tradução nossa).
[27] O autor se refere a comparações de demais atores sobre ataques cibernéticos com a magnitude de eventos como o 11 de setembro, ataque a base de Pearl Harbor em dezembro de 1941 e a bomba de Hiroshima em agosto de 1945.

> alheias, 8) envolvimento de hard e soft power, traduzido aqui enquanto forças físicas e virtuais, e 9) o alcance de impactos multidimensional.

Os atores ainda desenvolveram a seguinte tabela a fim de ilustrar as características mais facilmente.

Tabela 3 – Características da Guerra Cibernética para Acadêmicos

Áreas	Característica
Domínio Prioritário	Cibernético
Intensidade	Alta
Atores	Estatais (direta ou indiretamente)
Equilíbrio de Poder	Tendenciosamente assimétrico
Forças Empregadas	Virtual e Física
Instrumentos	Elemento surpresa + trapaça + rompimento e destruição de redes
Alvos	IC e Sistemas de Redes Governamentais
Motivação	Político- Militar
Alcance de Impactos	Multidimensional (terra, água, ar, espaço)

FONTE: VENTRE, 2012; ARQUILLA e RONDFELDT, 1997; CLARKE e KNAKE, 2010; FERNANDES, 2012; SHAKARIAN, SHAKARIAN E RUEF, 2013; KLIMBURG, 2011; SAMPAIO, 2001; CROSSTON, 2011; LIBICKI, 2011; DUNN, 2010; GREATHOUSE, 2014; SINGER e FRIEDMAN, 2014; SENHORAS et. AL. 2015; SCHMITT, 2013; NYE, 2013; CROSSTON, 2011 apud ALCÂNTARA; DA SILVA, 2018, p.139)

Considerando essas características, é possível prever de modo geral o comportamento do Estado frente à Ciberguerra, principalmente pelo fato de a primeira característica ser a respeito do envolvimento obrigatório do Estado. Ademais, as outras características apresentadas acometem as questões das estratégias utilizadas pelas partes envolvidas na Ciberguerra buscando o interesse próprio e explorando as fraquezas do inimigo com suas vulnerabilidades.

4.2.2 Ciberataques e suas particularidades

A princípio quando pensamos sobre “armas” e “Ciberespaço” naturalmente nos vem em mente as armas cibernéticas, o que não está equivocado logicamente. Porém, essa ideia inicial

pode desviar a atenção do potencial presente em um ciberataque. Desse modo, busca-se esclarecer os conceitos de ciberataque e arma cibernética em seguida para depois demonstrar as suas aplicações pelo Estado.

Para estabelecer as características sobre o que é um ciberataque, parte-se da ideia de trazer as principais características que o distinguem de um ataque tradicional. Portanto, diferente das armas cinéticas (como bombas, armas, facas etc), os ciberataques usam computadores e os meio digitais para atingir seu alvo, assim não possuem fatores físicos limitadores como os ataques tradicionais (SINGER; FRIEDMAN, 2014). A vantagem da desterritorialidade no meio digital concede ao ataque alcance ilimitado e na velocidade da luz, podendo atingir inúmero alvos em diferentes locais de uma vez só. Essas viabilidades adquiridas a partir do Ciberespaço permitem aos atores estatais a aplicação de estratégias específicas, podendo adotar tanto posturas dinâmica defensiva e resilientes, quanto ofensivas (PINTO; GRASSI, 2020).

Dando continuidade ao estudo, o Ciberataque também se difere em relação ao alvo. O resultado do ataque cibernético não será diretamente o dano físico, pois sempre o primeiro alvo a ser atingido será um outro computador (SINGER; FRIEDMAN, 2014). Mesmo assim, não quer dizer que um ciberataque não possa ter fins de causar danos matérias, mas seu primeiro resultado sempre será fruto de um incidente digital independente da repercussão final.

Além disso, Singer e Friedman (2014) ainda afirmam que, de maneira geral, é mais difícil atribuir a autoria de um ciberataque a um determinado ator do que nos ataques tradicionais. No exemplo utilizado anteriormente nesta pesquisa sobre os ciberataques na Estônia, em 2008, mesmo após uma série de especulações, os culpados sobre o ocorrido não foram responsabilizados devido à dificuldade de se atribuir culpa aos atores que teriam executado tais ações (MCGUINNESS, 2017).

Outra diferença fundamental entre as partes está no orçamento e recursos para a realização dos ataques. Os custos para realizar um ataque tradicional são realizados na compra de armas reais e materiais (bélicos ou de existência da guerra), enquanto nos ataques cibernéticos os custos são voltados para a pesquisa e desenvolvimento (SINGER; FRIEDMAN, 2014). Com isso, por serem realizados a partir de computadores, os ciberataques reduzem os custos da guerra por não haver necessidade de real deslocamento e munições.

Ademais, se tratando dos atores estatais, os ciberataques podem ser categorizados pelos objetivos no qual o outro Estado está sendo ameaçado. Os objetivos são: Disponibilidade, Confidencialidade e Integridade (SINGER; FRIEDMAN, 2014). Desse modo, os ataques de disponibilidade são aqueles que geram dificuldade de acesso à rede, impedindo ou sobrecarregando um servidor, página da web ou programa. Os ataques de confidencialidade têm como alvos dados e informações com o objetivo de forçar o acesso em outra rede de computador afim de extrair ou monitorar as informações. Por fim, os ataques à integridade se dão com a invasão de sistemas para alterar e manipular informações já existentes (SINGER; FRIEDMAN, 2014).

A partir do exposto, percebe-se que os ataques cibernéticos buscam sempre explorar as vulnerabilidades da esfera virtual afim de causar danos nos sistemas de informação nas quais as sociedades atualmente dependem (LOBATO, KENKEL, 2015), como por exemplo, as instituições do Estado e seus bancos de dados. Fazendo uso dessa modalidade de ataque, o Estado possui mais um meio para expandir seus interesses e exercer poder, porém, por outro lado, ele deve estar preparado para se defender de possíveis ameaças alimentando suas capacidades.

4.3 A relação entre Capacidade e Vulnerabilidade cibernética

Os dois conceitos abordados neste momento possuem um papel importante na pesquisa pois, a partir dessa análise conceitual, será analisado se a busca por recursos cibernéticos é capaz de diminuir as vulnerabilidades cibernéticas do Estado afim de propiciar sua segurança. Além disso, aplica-se esses conceitos ao modo de atuação dos Estados, buscando entendimento acerca da militarização do Ciberespaço para lidar com tal a situação.

Com intuito de iniciar tal tópico, é de suma importância conceituar tecnologia porque por meio dessa definição será estabelecido o primeiro parâmetro necessário para se entender as capacidades e vulnerabilidades cibernéticas, além de permitir relacioná-las. Desse modo, tecnologia é “o método de fazer alguma coisa” e para utilizar esse método deve-se ter três elementos fundamentais: “informação sobre o método, o meio de empregá-lo e certa compreensão do mesmo” (DAHLMAN; WESTPHAL, 1983, p. 6). A tecnologia como recurso é de suma importância pois possui caráter de não esgotamento, configurando alto valor de

aquisição. Isso está intimamente relacionado à possibilidade desse método ser repassado por terceiros, podendo ser aprimorado.

Outro critério a ser mencionado e que está intimamente ligado à tecnologia (ROSENTHAL, 2010) é o desenvolvimento. Existe uma gama de definições sobre esse conceito, de modo geral e considerando os trabalhos sociológicos de Durkheim, o desenvolvimento é a expansão econômica adorando a si (DIAS CONDE, 2021). A analogia realizada pelo sociólogo advém dos estudos aprofundados na religião, na qual a religião é a sociedade adorando a si mesma, logo essa adoração permeia o sentimento de que algo está voltado para o caminho "correto" e seguindo um caminho trilhado para o progresso. Portanto, a "crença no desenvolvimento" permite compreender o desenvolvimento como um dos paradigmas que permeiam a modernidade (RIBEIRO, 2012; RIST, 2002 apud DIAS CONDE, 2021, p.196).

Dessa maneira, com o desenrolar da história mundial percebe-se que os conceitos apresentados acima sempre estiveram relacionados. Aliás, desde que se tem conhecimento da existência da raça humana, variadas técnicas foram desenvolvidas para resultar na complexa sociedade contemporânea e suas tecnologias. Compreendendo a busca pelo conhecimento como atividade exclusiva dos humanos, a arte rupestre foi uma forma primitiva de comunicação criada a partir de técnicas nos primórdios da sociedade e tem como grande importância para o entendimento nas formas de comunicação humana (GONDIM, 2012). Dando um salto no tempo, o desenvolvimento da comunicação humana atingiu um patamar altíssimo devido às técnicas criadas, ou melhor dizendo, às tecnologias da comunicação e informação.

Conforme apresentado sobre a relação entre os conceitos, Rosenthal (2010, p.7) conclui de modo geral que:

> na medida em que o *desenvolvimento* de um país envolve (e depende de) um processo intensivo de *elevação da produtividade social* ao longo do tempo, ele está necessariamente ligado à questão da *tecnologia*, entendida esta como um (ou *o*) *conjunto de conhecimentos aplicados à produção dos bens e serviços necessários à vida da sociedade*.

Desse modo, a produção de recursos tecnológicos complementa a ideia do desenvolvimento para o progresso do Estado. Essas tecnologias servem também para suprir as

lacunas do bem-estar e garantir a segurança para a população. Sendo assim, os seguintes tópicos irão tratar das capacidades para suprirem as vulnerabilidades.

4.3.1 Das capacidades

Ao pesquisar sobre a etimologia da palavra "capacidade" encontra-se parte de seu significado relacionado ao poder, seja ele para acomodar ou receber algo (CAPACIDADE, 2022). Não obstante, a capacidade de um país em realizar alguma coisa dependerá do poder atribuído a ele naquela questão e os conceitos intermediários para atingi-lo. Nesse sentido, os conceitos intermediários que servirão de parâmetro para definir a capacidade cibernética serão a tecnologia e o investimento de recursos aplicados a ela.

Tendo em vista o sistema econômico no qual os Estados estão inseridos, o capital é um importante recurso para se elaborar qualquer fim político. Seguindo esse raciocínio, os Estados que investem mais recursos em tecnologias terão maiores capacidades para se inserir em questões relacionadas a ela, como por exemplo o Ciberespaço. Então, para se obter maior capacidade tecnológica (ou cibernética) a sociedade fica condicionada a "(...) introduzir sistematicamente, em seus sistemas produtivos, novos e mais avançados conjuntos de tais conhecimentos – i.e., novas tecnologias" (ROSENTHAL, 2010, p. 7).

Cabe aqui mencionar que os termos "capacidade tecnológica" e "capacidade cibernética" não estão sendo utilizados como sinônimos, pois incitaria a redução de todo o viés cibernético e suas particularidades. Assim, o intuito da pesquisa não é definir esse conceito a fundo, mas sim relacioná-lo com o comportamento do Estado no Ciberespaço, podendo ser objeto de estudo em um outro momento. Portanto, considera-se a capacidade cibernética uma rama da capacidade tecnológica por estarem intimamente ligadas no viés da técnica e conhecimento sobre a área da informação e comunicação.

Sendo assim, sejam as capacidades tecnológicas ou cibernéticas, sempre estarão relacionadas aos recursos econômicos de um país. Esses recursos econômicos, se destinados para as questões como ciência e tecnologia voltados para informação e comunicação, irão servir aos assuntos cibernéticos desse Estado. Assim, o Estado cria maiores possibilidades de exercer e expandir poder no Ciberespaço para atingir seus interesses.

4.3.2 Das vulnerabilidades

Vulnerabilidade pode ser conceituada como

> [...] uma fragilidade presente ou associada a ativos que manipulam ou processam informações, que ao ser explorada por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação (GARCIA, 2020, p.14)

Considerando essa definição e se tratando do Estado, estar vulnerável não quer dizer que automaticamente o elemento se torne alvo e será atingido, mas sim que possui condições propícias para que seja atacado. A vulnerabilidade do Estado vai de encontro à exposição de alguma fraqueza que pode ser utilizada contra ele.

Essa fraqueza configura uma ameaça e ela "é um possível perigo que pode explorar uma vulnerabilidade" (SÊMOLA, 2003 apud GARCIA, 2020, p. 14). Identificar as ameaças para saber as vulnerabilidades são passos fundamentais no momento de determinar a segurança de algum sistema ou do próprio Estado. Ao se tratar dos sistemas de redes de computadores tem-se a vulnerabilidade cibernética. Esse elemento está presente nas questões de segurança de todos os atores. Para o Estado, essa presença ocorre devido à informatização das instituições do Estado e pelo uso massivo da Internet por sua população (como abordado no capítulo 2).

Contudo, a vulnerabilidade cibernética é um assunto no qual os Estados devem tratar por ter adquirido ao longo dos anos suma importância a partir do desenvolvimento das TIC's. Desse modo, esse conceito está intimamente ligado à segurança e identificação de falhas por meio de um levantamento minucioso no ambiente da tecnologia da informação, levando em consideração a questão estratégica do Ciberespaço.

4.3.3 A relação entre Capacidade e Vulnerabilidade

Uma questão de suma importância para se entender a maneira de atuação dos Estados com a presença do Ciberespaço no sistema internacional é a relação entre as capacidades tecnológicas (ou, de modo mais específico, cibernéticas) e vulnerabilidades cibernéticas. Por meio da impossibilidade de se dissociar a capacidade tecnológica de um país às questões econômicas do próprio país e do sistema internacional, percebe-se que a competitividade entre os atores é

mantida (ROSENTHAL, 2010). Então, dentro da lógica neorrealista, o Estado, para assegurar sua soberania e existência, se empenha na busca pelos recursos tecnológicos da informação e comunicação acirrando a competitividade entre eles neste setor (cibernético). Assim, com a presença efetiva no Ciberespaço por causa da tecnologia, o Estado utiliza desses recursos para diminuir suas vulnerabilidades cibernéticas e não se tornar vítima de novos ataques.

Em vista disso, experimenta-se a relação de dependência entre "capacidade" e "vulnerabilidade" considerando-a inversamente proporcional. Ou seja, quanto mais um Estado investir em recursos tecnológicos para o Ciberespaço, menos vulnerável ele será ou vice-versa. A partir dessa ideia, ao se pensar no Estado isoladamente, pode-se concluir que seja uma afirmação verdadeira, pois dentro da lógica estabelecida de que tecnologia resulta em desenvolvimento (apresentada anteriormente), compreende-se que tal ganho seria benéfico ao Estado em todas suas questões, até mesmo nas de segurança.

Porém, ao se analisar o Estado inserido no sistema internacional é de suma importância considerar outros quesitos que possam afetar a vulnerabilidade de um país, pois a vulnerabilidade como conceito sempre dependerá de algumas questões inerentes a ela. Sendo assim, a questão cibernética é apenas mais um dos quesitos a serem inseridos nessas condições próprias. Desse modo, ao se pensar em qualquer tipo de vulnerabilidade, os parâmetros considerados devem estar atrelados aos fatores geopolíticos também, como por exemplo: "a localização, a dimensão total, a topografia, a climatologia, o recorte (formato) territorial, a distribuição demográfica e o governo nacional" (CASTRO, 2012, p. 143).

Decorrido isso, Gomes (2020, p.46) conceitua vulnerabilidade cibernética como um "conjunto de um incidente indesejado, que resulta em risco para um sistema". Ou seja, a vulnerabilidade cibernética deve ser medida a partir de um incidente, não podendo mensurá-la apenas pela busca de capacidades. Considerando isso, um Estado terá dificuldade de saber sua real vulnerabilidade no Ciberespaço até que este sofra algum ataque.

Por conseguinte, o Estado ao adentrar o Ciberespaço foca seu modo de atuação de maneira a sanar (ou reduzir ao máximo) suas vulnerabilidades e diminuir as chances de ser atacado. Em meio a isso e na tentativa de abarcar os parâmetros corretos na intenção de apaziguar os efeitos de algum ataque cibernético, o Estado utiliza a militarização do Ciberespaço como

estratégia para interligar esses fatores afim de sanar suas vulnerabilidades, consequentemente, a cibernética também.

5. CONSIDERAÇÕES FINAIS

A disciplina de Relações Intencionais tem como caráter intrínseco o estudo do funcionamento do mundo a partir de variadas áreas do conhecimento. Desse modo, relacionar o eixo teórico dessa disciplina com temas emergentes se torna essencial no desenvolvimento de novos saberes, dentre eles o subcampo internacionalista de CiberRI. Provocar a junção de temáticas sobre informática e comunicação com fatores políticos motiva a compreensão do funcionamento do mundo contemporâneo, além de ser uma associação de estudo cada vez mais requisitada com o passar dos anos.

Essa demanda cresceu em conjunto ao desenvolvimento das TIC's que transformaram a maneira do mundo se relacionar e, também, passaram a estar presentes no dia a dia dos atores no sistema internacional. Sendo assim, a aparição do Ciberespaço evoca seu estudo a partir de elementos teóricos das RI colocando em voga o desenvolvimento do conhecimento ciberinternacionalista. Assim, se torna possível teorizar sobre o Ciberespaço para além das vias técnicas da ciência da computação, permitindo trazer proximidade do assunto com as RI.

Considerando isso, o primeiro capítulo da pesquisa buscou inserir o Ciberespaço nas questões de segurança e estratégia dos Estados, além de adicionar o espaço cibernético nos assuntos estruturais do sistema internacional a partir da teoria neorrealista. Em busca disso, foi introduzida a abordagem tradicional dos conceitos de Segurança e Estratégia voltada para a guerra para, posteriormente, atualizá-la à conjuntura de duas realidades: a física e a virtual, ora preponderante.

O aprimoramento desses conceitos vai ao encontro com os estudos desenvolvidos pela Escola de Copenhague, na qual consideram a necessidade de se abordar as questões de segurança a partir de novas estratégias para além das militares. Essa exigência diz respeito à emergência de novos problemas securitários cada vez mais comuns atualmente, como os ataques cibernéticos e a fragilidade dos sistemas de dados.

Desse modo, as estratégias possuem abordagens além das questões tradicionais, podendo ainda serem coercitivas e de paz e resolução de conflitos. O Ciberespaço pode auxiliar em qualquer uma das perspectivas, seja em ataques diretos ligado à guerra e uso da violência, por

meio de sanções limitando algum recurso e informação, ou permitindo maior comunicação entre as partes envolvida no conflito.

Os autores clássicos da Escola de Copenhague não aprofundaram nas questões de segurança cibernética, mas as considerações de Helen Nissenbaum e Lene Hansen (2009) foram fundamentais para a análise geopolítica internacional a partir do desenvolvimento das TIC's. A criação dessa tecnologia tem uma repercussão significante com as questões de segurança militar, pois, como apresentado no capítulo 2, houve uma trajetória de criação atrelada ao Estado estadunidense por meio de incentivos no campo de ciência e tecnologia.

Sendo a segurança cibernética um tema cada vez mais alarmante, as autoras ainda propuseram questionamentos para lidar com a hipersecuritização do espaço virtual. Como exposto, há a preocupação em manter o monopólio do uso da força sob tutela do Estado, diminuindo a concorrência do mesmo com os demais atores que terminaram por receber uma parcela de autonomia com o uso do Ciberespaço. Essa securitização do espaço cibernético é composta pela busca de protagonismo dos atores estatais com a constante criação de tecnologias de dados e redes, ocasionando a "corrida armamentista cibernética", como abordam Singer e Friedman (2014).

A partir disso, o Estado mantém seu protagonismo no sistema internacional a partir da lógica Neorrealista de busca pela sobrevivência no sistema anárquico. Dessa maneira, mede-se o poder dos Estados envolvidos na estrutura por meio das suas capacidades, sejam elas tamanho, riqueza, população etc. Não obstante, o Ciberespaço se adequa a essa lógica ao se considerar o protagonismo do Estado para o poder cibernético e sobre a vantagem adquirida de um determinado ator estatal ao investir em recursos tecnológicos.

Dando continuidade aos resultados, os avanços tecnológicos no campo das informações e comunicações transformaram rapidamente as relações dos atores internacionais para como conhecemos hoje. Como parte do processo de globalização, o mundo está interconectado devido à redução das barreiras físicas de troca de dados. Desse modo, o espaço virtual configura um novo local de atuação dos atores internacionais que, assim como o sistema internacional, é naturalmente descentralizado, anárquico e em auto expansão de poder.

Portanto, após revisão bibliográfica acerca do conceito de Ciberespaço, opta-se por adotar a definição de Kuehl (2009) devido à abordagem dos elementos físicos e virtuais acerca dos componentes formadores do espaço cibernético. Assim, o Ciberespaço pode ser entendido como um "(...) domínio global dentro do ambiente da informação".

Para além disso, outro aspecto relevante além do *hardware* e *software* são os usuários que compõem esse ambiente. Os atores presentes no espaço cibernético vão desde o mais simples (o indivíduo) aos mais complexos (o Estado, Organizações Internacionais, grupos Terroristas, dentre outros) e a partir da dependência da sociedade a essas tecnologias é possível entender sua relevância na sociedade contemporânea.

Desde a criação da Internet com a ARPA, percebe-se os Estados Unidos como principal interessado no desenvolvimento da pesquisa na época. Por meio de investimento financeiro, e como pioneiro dessa tecnologia, ele se beneficiou do cenário internacional da Guerra Fria e investiu em recursos para pesquisas militares voltadas à guerra, dando um importante papel às universidades. Por conta das oportunidades de mercado vistas nesta nova tecnologia e as dificuldades de regulá-la, o governo estadunidense ampliou o uso da Internet para domínio público além do militar. Porém, desde a criação do que viria a ser o espaço cibernético, o Estado age dentro da lógica das unidades egoístas neorrealistas e militariza o Ciberespaço. Essa conduta é adotada pelos atores estatais com a finalidade de sobreviver ao sistema internacional e atingir seus interesses.

Sendo assim, com a disseminação das TIC's no mundo e a inserção de diversos atores nesse universo, é fundamental ao Estado estar atento às ameaças existentes no Ciberespaço. Para isso, o empenho do Estado em mobilizar recursos de pesquisa serve para diminuir as chances de um possível ataque cibernético ou de estar preparado para potencializar seu ataque frente a algum conflito.

Desse modo, o poder cibernético se torna uma peça chave no modo de conduta do Estado, pois ele deve se preocupar com as questões de segurança cibernética e desenvolver estratégias para garantir sua sobrevivência e interesses frente ao sistema internacional. Logo, se estabelece o poder cibernético para colocar o Ciberespaço dentro dos domínios operacionais e elementos de poder dirigidos pela comunidade de segurança internacional.

Outra questão relevante ao se considerar o Ciberespaço como parte da matéria de segurança do Estado está na relação de interconectividade com os demais espaços geográficos. Essa característica expõem uma vantagem de se utilizar o espaço virtual para acessar os demais espaços (terra, mar, ar e espaço sideral), reduzindo o tempo hábil da troca de dados, e consequentemente, das distâncias no mundo físico.

Sendo assim, o uso do Ciberespaço para exercer poder configura o poder cibernético. Tal controle é exercido pelo Estado por meio da questão da militarização ao se aplicar os recursos cibernéticos para atingir objetivos militares. Por causa da eficiência das TIC's nas operações militares, percebe-se, assim como da sociedade global, cada vez mais dependência em relação ao uso das inteligências ligadas a ele.

Um dos meios de utilização do espaço virtual pelo Estado ao militarizá-lo é a Ciberguerra. Essa modalidade de fazer guerra não anula o conceito real do que é uma guerra, mas faz parte das políticas de estratégia e defesa do Estado como uma alternativa ao conflito ou um método de se iniciar o conflito (isso depende do interesse de quem utilizar essa estratégia). Portanto, o essencial para se configurar a Ciberguerra está na presença do Estado como envolvido no combate e no uso de armas cibernéticas. As armas cibernéticas podem ser usadas isoladamente ou combinadas com armas cinéticas, e adquirem a vantagens ao serem utilizadas, como a desterritorialidade, alcance ilimitado, velocidade da luz e maior número de alvos em diferentes locais.

Considerando a conduta dos Estados pra o Ciberespaço buscou-se entender a relação entre as capacidades e vulnerabilidades. Em primeiro momento, a proporção estabelecida sobre quanto mais recursos cibernéticos desenvolvidos, menos vulnerável um Estado se encontra, parecia atraente ao se tratar do Estado isoladamente no sistema internacional. Porém, ao se analisar o conjunto dos Estados a partir de uma estrutura complexa, percebe-se diferentes fatores que devem ser considerados, como por exemplo os geopólíticos. Assim, a vulnerabilidade cibernética de um ator é medida para além da quantidade de recursos aplicados ao Ciberespaço.

Portanto, confirmando em parte a hipótese apresentada, a maneira de atuação dos Estados, no sistema internacional, se repete no Ciberespaço no qual os Estados buscam agir em contraponto com suas três principais características para lidar com os desafios de Defesa e Segurança, (1) a desterritorialidade; (2) multiplicidade de atores; e (3) incerteza (MEDEIROS,

2019). Essa maneira de atuação ocorre com a finalidade de regulamentar e tornar esse espaço cada vez mais previsível. Para isso, os países buscariam se capacitar e desenvolver estratégias específicas voltadas para a militarização do Ciberespaço para sanar suas vulnerabilidades neste meio, ambicionando evitar as ameaças e exercer poder. Porém, apenas a militarização não se demonstra capaz de sanar as vulnerabilidades cibernéticas dos Estados por se tratar de conceitos que consideram além do desenvolvimento das capacidades e aplicação de recursos.

REFERÊNCIAS

ACÁCIO, I. D. P. Segurança Internacional no século XXI: O que as teorias de relações internacionais têm a dizer sobre o ciberespaço? In: OLIVEIRA, Marcos Aurélio Guedes de. NETO, Ricardo Borges Gama. LOPES, Gills Vilar (org.). Relações Internacionais Cibernéticas (CiberRI): Oportunidade e desafios para os estudos estratégicos e de segurança internacional. Recife: Ed.UFPE, 2016. p. 35-58 (**Defesa e Fronteiras Virtuais**).

ALCÂNTARA, Bruna; DA SILVA, Igor. Guerra Cibernética: Uma análise conceitual sobre o termo. *In*: Danielle Ayres; Ana Luiza Vedovato; Daniela Lunkes; Elany de Souza; Juliano Bravo. (Org.). **Política Internacional Contemporânea**. 1ed.Rio de Janeiro: Autografia, p. 132-166, 2018. Disponível em: <https://www.academia.edu/50821913/Guerra_Cibern%C3%A9tica_Uma_an%C3%A1lise_conceitual_sobre_o_termo>. Acesso em: 30 nov. 2022.

AMARAL, Arthur. **A Guerra ao Terror e a Tríplice Fronteira na agenda de segurança dos Estados Unidos**. Tese (Mestrado em Relações Internacionais) – Programa de Pós-graduação em Relações Internacionais, Pontifícia Católica do Rio de Janeiro. Rio de Janeiro. 2008. Disponível em: <https://www2.dbd.puc-rio.br/pergamum/biblioteca/php/mostrateses.php?open=1&arqtese=0610356_08_Indice.html>. Acesso em: 1 nov. 2022.

APPLE-1 REGISTRY. Apple-1 Registry, 2022. The Apple-1. Disponível em: < https://www.apple1registry.com/en/theapple1.html>. Acesso em: 15 jun. 2022.

ARPANET. ARPANET logical map circa 1977. The Computer History Museum. 1977. Disponível em: <https://en.wikipedia.org/wiki/File:Arpnet-map-march-1977.png>. Acesso em: 13 dez 2022.

ARQUILLA, John; RONFELDT, David. "Cyberwar is Coming!". **Comparative Strategy**, v.12, n.2, RAND, p. 141–165, 1993. Disponível: < https://www.tandfonline.com/doi/abs/10.1080/01495939308402915>. Acesso em: 30 nov 2022.

ASSUNÇÃO, Juliana. A ciberguerra é guerra? **Rev. Hoplos**, Niterói, v.6, n10, p.9-23, 2022. Disponível em: < https://periodicos.uff.br/hoplos/article/view/52506>. Acesso em: 30 nov. 2022.

AZEVEDO, H. L.; MONTEIRO, H. P. F. O ciberespaço em uma reflexão geográfica. **Revista Vértices**, [S. l.], v. 12, n. 3, p. 139–148, 2010. DOI: 10.5935/1809-2667.20100026. Disponível em: https://essentiaeditora.iff.edu.br/index.php/vertices/article/view/1809-2667.20100026. Acesso em: 29 nov. 2022.

BETZ, David. **Cyberspace and the State**: Toward a Strategy for Cyber-Power. Londres: Ed.The International Institute for Strategic Studies (IISS), 2011. Disponível < https://www.researchgate.net/publication/345705816_Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-power >. Acesso em 10 jul. 2022.

BITTENCOURT, Paulo. **Kenneth n. Waltz:** uma análise da perspectiva de sua teoria das relações internacionais através das obras "theory of international politics" e"man, the state, and war". In: SEMANA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA, I., 2013, São Carlos. Anais eletrônico... São Carlos: [s.n.], 2013. n.p. Disponível em: < http://www.semacip.ufscar.br/wp-content/uploads/2014/12/Kenneth-N.-Waltz-uma-an%C3%A1lise-da-perspectiva-de-sua-teoria-das-rela%C3%A7%C3%B5es-internacionais-atrav%C3%A9s-das-obras-%E2%80%9CTheory-of-International-Relations%E2%80%9D-e-%E2%80%9CMan-the-State-and-War%E2%80%9D..pdf>. Acesso em: 18 ago. 2021

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. Estado Moderno. *In*: _____. **Dicionário de Política**. São Paulo: Editora UNB, 2004a p. 425-431.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. Relações Internacionais. *In*: _____. **Dicionário de Política**. São Paulo: Editora UNB, 2004b p. 1089-1099.

BUZAN, Barry; HANSEN, Lene. **A Evolução dos Estudos de Segurança Internacional**. São Paulo: Editora Unesp, 2012. ISBN 978-85-393-0266-6.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. **Security:** a new framework for analysis. Boulder: Lynne Rienner, 1998.

CAPACIDADE. *In*: DICIONÁRIO da língua portuguesa. São Paulo: **Michaelis**, 2022. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/capacidade>. Acesso em: 30 nov. 2022.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Ed. 1. Rio de Janeiro: Zahar, 2003. Disponível em: < https://www.academia.edu/41717035/A_Galaxia_da_Internet_Manuel_Castells. Acesso em: 09 jan. 2022.

CASTELLS, Manuel. The Impact of the Internet on Society: A Global Perspective. **MIT Technology Review**, 2013. Disponível em: < https://www.technologyreview.com/2014/09/08/171458/the-impact-of-the-internet-on-society-a-global-perspective/>. Acesso em: 09 jan. 2022.

CASTRO, Thales. **Teoria das Relações Internacionais.** Brasília: FUNAG, 2012. Disponível em: <https://funag.gov.br/loja/download/931-Teoria_das_Relacoes_Internacionais.pdf>. Acesso: 08 jul. 2022

CEPIK, Marcos; CANABARRO, Diego; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. *In*: SOUZA, André; NASSER, Reginaldo; MORAES, Rodrigo. **Do 11 de Setembro de 2001 à Guerra ao Terror:** reflexões sobre o terrorismo no século XXI. 1ª Ed. Brasília: IPEA, 2014. p. 161-186. Disponível em: <https://professor.ufrgs.br/marcocepik/files/cepik_canabarro_borne_-_2014_-_securitizacao_ciberespaco.pdf>. Acesso em: 15 nov. 2022.

CERF, Vinton. Oral History of Vinton (Vint) Cerf. [Entrevista concedida a] Donald Nielson. **Computer History Museum**, Mountain View, California, p. 1-49, 2007.

CHOUCRI, Nazli. Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences. **MIT Political Science**. Montreal: MIT Press, 2012. Disponível em: < https://hdl.handle.net/1721.1/141686>. Acesso em: 10 jul. 2022.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war**: the next threat to national security and what to do about it. Ed 2. New York: HarperCollins, 2012.

CORRÊA, Fernanda. A balança de poder sob a ótica de Kenneth Waltz: uma discussão da teoria sistêmica**. Revista InterAção** [online], v. 11, n. 11, jul/dez 2016. Disponível em: <https://doi.org/10.5902/2357797529398 > ISSN 2357-7975. Acesso em: 18 ago. 2021.

CRUZ, Samuel César da Jr. **A segurança e defesa cibernética no brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Brasília: Rio de Janeiro: Instituto de Pesquisa Econômica Aplicada (IPEA), 2013. (Texto para Discussão). Disponível em: < https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=19183 >. Acesso em: 10 jul. 2012.

CURLEY, Robert. **Stuxnet**. Encyclopedia Britannica, 23 nov. 2016, Disponível em: <https://www.britannica.com/technology/Stuxnet>. Acesso em: 16 set. 2021.

DAVID, Charles Philippe. Estratégia e Segurança no Limiar do Século XXI. In: _____. **A Guerra e a Paz:** abordagens contemporâneas da segurança e da estratégia. Lisboa: Instituto Piaget, 2000. p. 19-44. ISBN 972-771-410-2.

DE MIRANDA, J. A. A.; DE FRAGA, M. N. Sociedade Global e Movimentos Sociais em Rede: Expansão da Democracia?. **Prim Facie**, [S. l.], v. 16, n. 31, p. 01–27, 2017. DOI: 10.22478/ufpb.1678-2593.2017v16n31.34017. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/34017. Acesso em: 29 nov. 2022.

DENNIS, Michael. Robert Kahn. **Encyclopedia Britannica**, 2021. Disponível em: < https://www.britannica.com/biography/Robert-Elliot-Kahn#ref1068993>. Acesso em: 09 jan. 2022.

DIAS CONDE, L. C. Do conceito de desenvolvimento à cooperação internacional como uma agenda de política externa: considerações teóricas e conceituais. **Missões: Revista de Ciências Humanas e Sociais**, v. 7, n. 2, p. 193-212, 25 out. 2021. Disponível em: < https://periodicos.unipampa.edu.br/index.php/Missoes/article/view/104581>. Acesso em: 30 nov. 2022.

DONALD, L. A Critical Evaluation of the Estonian Cyber Incident. **Journal of Advanced Forensic Sciences**, Cybersecurity and Policy Department, Morgan State University, Baltimore, Maryland, v.1, n.2, p.7-14, Nov, 2020. Disponível em: < https://openaccesspub.org/jafs/article/1489>. Acesso em: 13 set. 2022.

DYKSTRA, Josiah. INGLIS, Chris. WALCOTT, Thomas. Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat. **National Defense University Press**, 19, nov. 2020. News. Disponível em: < https://ndupress.ndu.edu/Media/News/News-Article-

View/Article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/>. Acesso em: 15 nov. 2022.

ENTENDA o caso Assange e Wikileaks fato a fato. **Carta Capital**, [S.I], 11, abril, 2019. Mundo. Disponível em: <https://www.cartacapital.com.br/mundo/entenda-o-caso-assange-e-wikileaks-fato-a-fato/>. Acesso em: 12 dez. 2022.

FONTES, Carlos. Navegando na Filosofia, [s.d]. Falácias e Paradoxos. Disponível em: <http://www.filorbis.pt/filosofia/11.falacia.htm.> Acesso em: 30 jun. 2022.

GADELHA, Júlia. A evolução dos computadores. **Instituto de Computação – UFF**, [s.d]. Disponível em: <http://www.ic.uff.br/~aconci/evolucao.html>. Acesso em: 15 jun. 2022.

GARCIA, Fábio Luiz. **Defesa cibernética brasileira: panorama atual e evolução das ameaças e vulnerabilidades existentes no Ciberespaço**. Tese (Especialização em Ciências Militares) - Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais, Ciências Militares, Escola de Formação Complementar do Exército e Colégio Militar de Salvador. Salvador, 2020. Disponível em: <http://bdex.eb.mil.br/jspui/handle/123456789/7983>. Acesso em: 30 nov. 2022.

GOMES, Nilton**. Vulnerabilidade cibernética e as estratégias de segurança cibernética internacional do estado brasileiro**. Tese (Bacharel em Relações Internacionais) – Instituto de Humanidade e Letras dos Malês, Universidade da Integração Internacional da Lusofonia Afro-Brasileira. São Francisco do Conde, 2020. Disponível em: < repositorio.unilab.edu.br/jspui/handle/123456789/1913>. Acesso em: 30 nov. 2022.

GONDIM, Caline. Pinturas rupestres: a representação da imaginação do homem primitivo. **Revista Temática**, v.8, n.4, s.p., 2012. Disponível em: < https://periodicos.ufpb.br/ojs/index.php/tematica/article/view/23751>. Acesso em: 30 nov. 2022.

GRIMALDI, Stphanie; MIRANDA, Májory. Ciência e Tecnologia: um patrimônio cultural ameaçado. *In*: CONFERÊNCIA SOBRE TECNOLOGIA, CULTURA E MEMÓRIA, 2015, Recife. Anais eletrônicos [...] Recife: Liber UFPE, 2015. [s.p.]. Disponível em: < http://www.liber.ufpe.br/home/wp-content/uploads/2016/09/11-Ciencia-e-tecnologia_grimaldi-Miranda.pdf>. Acesso em: 30 jun. 2022.

HALLIDAY, Fred. **Repensando as Relações Internacionais**. Porto Alegre: Editora UFRGS, 1999.

HANSEN, Lene. NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School**. International Studies Quarterly**. Vol 53, No. 4, p.1155- 1175, 2009. Disponível em: <http://www.jstor.org/stable/27735139>. Acesso em: 17 set. 2021.

HOFF, Natali. George W. Bush e a Securitização do Terrorismo após os Atentados de 11 de Setembro de 2001. **Conjuntura Global,** Curitiba, v. 6 n. 2, mai./ago, 2017, p. 246-266. Disponível em: <https://revistas.ufpr.br/conjgloblal/article/download/54615/33154>. Acesso em: 16 nov. 2022.

JACKSON, Robert; SORENSEN, Georg. **Introdução às Relações Internacionais**. Rio de Janeiro: Jorge Zahar Ed., 2007.

KASPERSKY. Kaspersky, 2021a. O que são vírus de computador e *worm* de computador? Disponível em: < https://www.kaspersky.com.br/resource-center/threats/computer-viruses-vs-worms>. Acesso em: 21 set 2021a.

KASPERSKY. Kaspersky, 2021b. Aprenda sobre *malware* e como proteger todos seus dispositivos contra eles. Disponível em: < https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>. Acesso em: 21 set 2021.

KOEPSELL, David R. **A ontologia do ciberespaço**: a Filosofia, a lei e o futuro da propriedade intelectual. São Paulo: Madras, 2004.

KENSY, Ângela. GRANDO, Paulo. Ciberespaço: um estudo introdutório sobre a atuação dos atores das Relações Internacionais neste âmbito espacial. **Relações Internacionais Contemporâneas**: teorias, olhares e interpretações sobre a complexidade do mundo, Itajaí, p. 54-106. 2016. Disponível em: https://www.univali.br/vida-no-campus/editora-univali/e-books/Documents/ecjs/E-book%202016%20RELA%C3%87%C3%95ES%20INTERNACIONAIS%20CONTEMPOR%C3%82NEAS%20TEORIAS,%20OLHARES%20E%20INTERPRETA%C3%87%C3%95ES%20SOBRE%20A%20COMPLEXIDADE%20DO%20MUNDO.pdf. Acesso em: 8 ago. 2021.

KUEHL, D. T. From Cyberspace to Cyberpower: defining the problem. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 2. Disponível em: <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210>. Acesso em: 10 jul. 2022.

LANGNER, Ralph. **Norderstedt:** Langner Group, c2000-1. Disponível em: <http://www.cancer-pain.org/>. Acesso em: 9 jul. 2002.

LEHMANN, Kai E. Unfinished transformation: The three phases of complexity's emergence into international relations and foreign policy. **Cooperation and Conflict**, São Paulo, Vol. 47, No. 3, p-p 404-413. 2012. Disponível em: https://journals.sagepub.com/doi/10.1177/0010836712454274. Acesso em: 17 set. 2021.

LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LOBATO, Luisa. KENKEL, Kai. A Ciberguerra é Moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, Rio de Janeiro. v.37, n.2, mai/agosto, p. 629-660. 2015. Disponível: < https://doi.org/10.1590/S0102-85292015000200010>. Acesso em: 30 nov 2022.

LOPES, Dawisson Belém. RAMOS, Leonardo César Souza. Existe uma ordem econômica internacional? A problematização de uma premissa. **Revista de Economia Política**, vol. 29, nº 2 (114), abril-junho/2009. Disponível em <http://www.rep.org.br/PDF/114-6.PDF >. Acesso em: 12 dez 2022.

LOPES, Gills. Da ciberguerra: idiossincrasias do século XXI e as instituições militares de defesa cibernética de Brasil, Estados Unidos, OTAN e União Europeia. In: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 5., 2011, Fortaleza. **Anais do V ENABED**, 2011d, Fortaleza. Disponível em: < https://www.abedef.org/conteudo/view?ID_CONTEUDO=70 >. Acesso em: 21 jan. 2022

LOPES, Gills. *Reflexos da digitalização da guerra na política internacional do século XXI***:** uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. 133 f. Dissertação (Mestrado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2013.

LOPES, Gills**. Relações Internacionais Cibernéticas (CiberRI):** Uma defesa acadêmica a partir dos estudos de segurança internacional. 2016. Tese (Doutourado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2016.

MARIANO, Marcelo Passini; PIGATTO, Jaqueline Trevisan; ALMEIDA, Rafael Augusto Ribeiro. Atores internacionais e poder cibernético: o papel das Transnacionais de tecnologia na era digital. **Monções**, Dourados, v.7, n.13, jan./jul. 2018. Disponível em: <https://ojs.ufgd.edu.br/index.php/moncoes/issue/view/326>. Acesso em: 10 jul. 2022.

MCGUINNESS, Damien. How a cyber attack transformed Estonia. **BBC News**, Tallinn, 27 abr. 2017. Disponível em: https://www.bbc.com/news/39655415. Acesso em: 13 set. 2022

MEDEIROS, Breno Pauli. **Ciberespaço e Relações Internacionais**: Rumo a construção de um novo paradigma?. Tese (Mestrado em Ciências Militares) – Programa de Pós-graduação em Ciências Militares, Instituto Meira Mattos. Rio de Janeiro, 2019. Disponível em: <> Acesso em: 08 set 2022.

MESQUITA, Felipe Sousa**. Segurança cibernética e a política internacional contemporânea**: novos desafios e oportunidades. 2019. [38] f., il. Trabalho de Conclusão de Curso (Especialização em Relações Internacionais) —Universidade de Brasília, Brasília, 2019. Disponível em: <https://bdm.unb.br/handle/10483/25026>. Acesso em: 10 jul. 2022.

MISLEH, Soraya. Nas Olimpíadas, a indústria da morte israelense e o *sportwashing*. **Monitor do Oriente Médio**. Tóquio, 2021. Disponível em: https://www.monitordooriente.com/20210729-nas-olimpiadas-a-industria-da-morte-israelense-e-o-sportwashing/. Acesso em: 15. nov 2022.

MONTEIRO, Silvana Drumond. O Ciberespaço: o termo, a definição e o conceito. **Data Grama Zero – Revista de Ciência da Informação,** João Pessoa, v.8, n.3, [s.p], jun, 2007. Disponível em: <https://brapci.inf.br/index.php/res/download/45007>. Acesso em: 30 jun. 2022.

NAUGHTON, John. **A brief history of the future**: the origins of the internet. Ed. 3. Londres: Phoenix, 2000.

NYE JR, J. S. **Cyber Power**. Havard Kennedy School – Belfer Center for Science and InternationalAffairs, mai. 2010. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acesso em: 10 jul. 2022.

OLIMPÍADAS SEM APARTHEID. ***Olympics without apartheid*** **- Olimpíadas sem apartheid**. [S.l], 2015. Facebook: *Olympics* without apartheid - Olimpíadas sem apartheid. Disponível em: < https://www.facebook.com/profile.php?id=100069136908676>. Acesso em: 15 nov. 2022.

OTTIS, Rain. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. In: EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY, 7., 2008, Plymouth. **Proceedings** [...] Plymouth: Academic Publishing Limited, 2008. P. 163-168. Disponível em: < https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/>. Acesso em: 13 set 2022.

PINTO, Danielle.; GRASSI, Jéssica. M. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, [S. l.], v. 7, n. 2, 2021. DOI: 10.26792/rbed.v7n2.2020.75178. Disponível em: https://rbed.abedef.org/rbed/article/view/75178. Acesso em: 30 nov. 2022.

PORTELA, Lucas Soares. Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais. **Rev. Bra. Est. Def**, Niterói, v.5, n.1, p. 91- 113. jan/jun, 2016. Disponível em: < https://rbed.abedef.org/rbed/article/view/62071 >. Acesso em: 30 jun. 2022.

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

RAMAL, A.C. Educação na cibercultura: hipertexto, leitura, escrita e aprendizagem. Porto Alegre: Artmed, 2002. Resenha de: SANTOS, G.B. Educação na cibercultura: hipertexto, leitura, escrita e aprendizagem. Revista da FACED, n.6, p. 179-183, 2002. Disponível em: < https://periodicos.ufba.br/index.php/entreideias/article/view/2784/1962>. Acesso em: 30 jun. 2022.

RAND CORPORATION. Rand Corporation, 2022. **A Brief History of RAND**. Disponível em: <https://www.rand.org/about/history.html>. Acesso em: 20 nov 2022.

RID, Thomas. Cyberwar and Peace. London: Oxford University Press. **Council on Foreign Relations**, 2013. Disponível em: <https://www.foreignaffairs.com/articles/2013-11-01/cyberwar-and-peace>. Acesso em: 26 jun 2021.

RID, Thomas. Cyberwar will not take place. **Journal of Strategic Studies**. v.35, n.1, 2011. Disponível em < http://dx.doi.org/10.1080/01402390.2011.608939 >. Acesso em 30 nov. 2022.

ROSENTHAL, David. **Capacidade tecnológica e desenvolvimento em tempos de globalização: idéias para o Mercosul**. Núcleo de Estudos para América Latina, Universidade Católica de Pernambuco. 2010. Disponível em: < http://www.unicap.br/neal/artigos/ >. Acesso em: 30 nov. 2022.

RUDZIT, Gunther; NOGAMI, Otto. Segurança e Defesa Nacionais: conceitos básicos para uma análise. **Revista Brasileira de Política Internacional**. São Paulo: Universidade Federal de São Paulo. V. 53, No.1, 2010. Disponível em: <https://www.scielo.br/j/rbpi/a/VxLnyTqsYNHYnrZ3fxTjwRg/?format=pdf&lang=pt>. Acesso em: 21 set 2021.

SENRA, Ricardo; KAWAGUTTI, Luis. Por dentro da estratégia do Estado Islâmico em redes sociais no Brasil. **BCC Brasil**, São Paulo, 22, jul, 2016. Disponível em: <https://www.bbc.com/portuguese/brasil-36839598>. Acesso em: 16 nov. 2022.

SILVA, Caroline; PEREIRA, Alexsandro. A Teoria da Securitização e a sua aplicação em artigos publicados em periódicos científicos. **Revista de Sociologia e Política**, Curitiba, v. 27, n.69, ed.7. 2019. Disponível em: < https://doi.org/10.1590/1678987319276907>. Acesso em: 15 nov. 2022.

SILVEIRA, Denise; CÓRDOVA, Fernanda. Unidade 2- A pesquisa científica. *In:* GERHARDT, Tatiana; SILVEIRA, Denise (org.). **Métodos de Pesquisa**. 1. ed. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2009. p. 33-44. Disponível em: http://hdl.handle.net/10183/213838. Acesso em: 10 nov. 2022.

SILVEIRA, Richard Batista. História do Microsoft ® Windows ®. **Centro de Informática – UFPE**, 2007. Disponível em: <https://www.cin.ufpe.br/~bfp/Arquivos/3196_Sistemas%20Operacionais.pdf>. Acesso em: 15 jun. 2022

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar:** What Everyone Needs to Know. New York: Oxford University Press, 2014.

STONE, Marianne. Security According to Buzan: A Comprehensive Security Analysis. **Security Discussion Papers**. No 1, 2009. Disponível em: < http://geest.msh-paris.fr/IMG/pdf/Security_for_Buzan.mp3.pdf>. Acesso em: 17 set. 2021.

TANENBAUM, Andrew S.; WETHERALL, David. **Rede de Computadores**. Ed. 5. Londres: Pearson, 2011.

THUDIUM, Guilherme. et. al. **Os Estudos de Segurança Internacional em Perspectiva Histórica: evolução teórica, regionalismo e a expansão da agenda securitária**. Porto Alegre, 2020. Disponível: < https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xiv_cadn?b_start:int=40>. Acesso em: 15 nov. 2022.

VALENÇA, Marcelo Mello. **Novas Guerras, Estudo para a Paz e Escola de Copenhague: uma contribuição para o resgate da violência pela segurança**. 2010. Tese (Doutorado em Relações Internacionais) - Programa de Pós-Graduação em Relações Internacionais, Pontifícia Universidade Católica, Rio de Janeiro, 2010. Disponível em: < https://www.maxwell.vrac.puc-rio.br/16533/16533_1.PDF>. Acesso em: 03 nov. 2022.

VILAR-LOPES, Gills. Relações internacionais cibernéticas (CiberRI): o impacto dos estudos estratégicos sobre o ciberespaço nas relações internacionais. In: CONGRESSO LATINO-AMERICANO DE CIÊNCIA POLÍTICA, 9., 2017, Montevidéu. **Anais eletrônicos**... Montevidéu. 2017. [online]. Disponível em <http://www.congresoalacip2017.org/arquivo/downloadpublic2?q=YToyOntzOjY6InBhcmFtcyI7czozNToiYToxOntzOjEwOiJJRF9BUlFVSVZPIjtzOjQ6IjMyMzAiO30iO3M6MToiaCI7czozMjoiMjlmYmNkMDViYjk2NTFiNWRjMzI2OTRiMmUwZTVlNzciO30%3D >. Acesso em: 18 ago. 2021.

WÆVER, O. **Securitization and Desecuritization**. In: LIPSCHUTZ, R (Ed.) On Security. Nova York: Columbia University Press, 1995, p. 26-86.

WALTZ, Kenneth. **Theory of international politics**. New York: McGraham Hill, 1979.

WE ARE SOCIAL; HOOT SUITE. Digital 2022 Global Overview Report: The essential guide to the world's connected behaviours. **We are social**, 2002. Disponível em: < https://wearesocial.com/uk/blog/2022/01/digital-2022/>. Acesso em: 15 jun. 2022.

ZIMET, E.; BARRY, C, L. Military Service Overview. In: KRAMER, F. D.; STARR, S. H.;

WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 12. Disponível em: < https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-12.pdf?ver=2017-06-16-115053-710 >. Acesso em: 10 jul. 2022

WESEL, Barbara. Legal Options running out for Julian Assange. **Deustche Welle**, United Kingdom, 08 out. 2022. Law and Justice. Disponível em: <https://www.dw.com/en/will-julian-assange-be-extradited-to-the-us/a-62761569>. Acesso em: 12 dez. 2022.