UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Bruna Maria dos Santos

A influência da configuração geopolítica das relações internacionais para ação dos atores não estatais no ciberespaço a partir de 2015

Florianópolis

2024

Bruna Maria dos Santos

A influência da configuração geopolítica das relações internacionais para ação dos atores não estatais no ciberespaço a partir de 2015

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina, como requisito parcial para a obtenção do título de Mestre em Relações Internacionais.

Orientadora: Profa. Dra. Danielle Jacon Ayres Pinto

Florianópolis

2024

Santos, Bruna Maria dos
A influência da configuração geopolítica das relações internacionais para ação dos atores não estatais no ciberespaço a partir de 2015 / Bruna Maria dos Santos ; orientadora, Danielle Jacon Ayres Pinto, 2024.
94 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Relações Internacionais, Florianópolis, 2024.

Inclui referências.

1. Relações Internacionais. 2. Segurança Cibernética. 3. Hackers. 4. Geopolítica. I. Ayres Pinto, Danielle Jacon. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Bruna Maria dos Santos

A influência da configuração geopolítica das relações internacionais para ação dos atores não estatais no ciberespaço a partir de 2015

O presente trabalho em nível de mestrado foi avaliado e aprovado, em 14 de março de 2024, pela banca examinadora composta pelos seguintes membros:

Profa. Dra. Graciela de Conti Pagliari
Universidade Federal de Santa Catarina

Profa. Dra. Jéssica Maria Grassi

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para a obtenção do título de Mestre em Relações Internacionais.

ICP-Edu
Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 16/07/2024 16:13:33-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

ICP-Edu
Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 16/07/2024 16:14:08-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

Profa. Dra. Danielle Ayres Jacon Pinto

Florianópolis, 2024

Dedico este trabalho à minha família.

AGRADECIMENTOS

A conclusão desta dissertação expressa o fim de um trabalho em um momento desafiador em diferentes espaços da minha vida. Agradeço a todas as pessoas que estiveram e dedicaram tempo fortalecendo meu empenho nas atividades do mestrado.

Este mestrado foi, em parte, minha companhia durante os longos dias da pandemia de COVID-19, junto a ele minhas maiores parceiras e meus maiores agradecimentos são à minha irmã Lara e à minha namorada Laísa que me fizeram companhia em todos os momentos e torceram todos os dias para que os meus planos e caminhos tivesse o rumo que escolhi seguir. Obrigada por ter feito o meu esforço um trabalho diário de resistência às diferentes dificuldades que passamos junto. Agradeço a resiliência e paciência que nos trouxe até aqui.

À minha mãe Marta, meu pai Ridailton e à minha avó Maria agradeço o incentivo a seguir os meus desejos, sonhos e ambições. Com certeza esse apoio foi o que abriu cada vez mais caminhos nos espaços que ocupei até aqui.

Agradeço também às minhas amigas e companheiras de mestrado que estiveram comigo em atividades e seminários acadêmicos que tornaram os dias de trabalho mais leves, compartilharam comigo os sentimentos e emoções de estar em um programa de pós-graduação. Em especial, agradeço a Yasmin, amiga que levo dessa fase para a vida.

À minha orientadora, Professora Doutora Danielle Ayres, seu trabalho foi fundamental para a entrega dessa dissertação. Agradeço por me guiar compartilhando seu conhecimento e ensinamentos ao longo deste processo.

Quero agradecer a todos os professores do Programa de Pós-Graduação em Relações Internacionais de Santa Catarina que possibilitaram essa formação e de tantos(as) outros(as) estudantes desse programa. O trabalho de todos(as) vocês transformam vidas.

RESUMO

A partir das discussões da pré-candidatura de elegíveis a presidente dos Estados Unidos em 2015 e a repercussão do papel dos hackers e da disseminação de informações falsas pela internet esta pesquisa busca compreender a influência da geopolítica sobre o comportamento e a atuação de atores não estatais no ciberespaço. Para isso, foi realizado um levantamento bibliográfico para elucidar os principais conceitos sobre o espaço cibernético, assim como das duas teorias utilizadas para analisar o texto e a prática geopolítica no espaço em discussão na dissertação. O poder e a identidade são conceitos essenciais para o entendimento da maneira como diferentes atores utilizam da esfera virtual para tornar-se proeminente e por isso são elementos centrais da teoria construtivista e da teoria realista para analisar a construção da política internacional e as relações entre interação e interesses dos Estados em termos de poder. A ação dos Estados nos últimos dez anos pressiona a sociedade de maneira geral, incluindo a interação dos atores não estatais. Assim, como resultado do comportamento estatal, há movimentações conflituosas em termos geopolítico, e as ações dos atores não estatais passam a se moldar de acordo com os acontecimentos que estão ligados aos seus objetivos e lutas. No caso dos hackers, patrocinados ou não por atores estatais, o Estado continua sendo o centro de suas ações e, por esse motivo, a teoria realista expõe um ponto de vista melhor sobre o ciberespaço e a segurança cibernética.

Palavras-chave: segurança cibernética; hackers; geopolítica.

ABSTRACT

This research seeks to understand the influence of geopolitics on the behavior and actions of non-state actors in cyberspace, based on discussions of the pre-candidacy of eligible candidates for president of the United States in 2015 and the repercussions of the role of hackers and the dissemination of false information on the internet. To this end, a bibliographical survey was carried out to elucidate the main concepts about cyberspace, as well as the two theories used to analyze the geopolitical text and practice in the space under discussion in the dissertation. Power and identity are essential concepts for understanding how different actors use the virtual sphere to become prominent and are therefore central elements of constructivist theory and realist theory for analyzing the construction of international politics and the relationship between the interaction and interests of states in terms of power. State action over the last ten years has put pressure on society in general, including the interaction of non-state actors. Thus, because of state behavior, there are conflicting movements in geopolitical terms, and the actions of non-state actors begin to shape themselves according to events that are linked to their objectives and struggles. In the case of hackers, whether they are sponsored by state actors, the state remains at the center of their actions, and, for this reason, realist theory provides a better view of cyberspace and cybersecurity.

Keywords: cybersecurity; hackers; geopolitics.

Somos apenas micropontinhos, não significamos quase nada na imensidão do universo.

(Elliot Page, 2023)

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CSIRT	Equipes de Resposta a Incidentes de Segurança em Sistemas Computacionais
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECS	Enhanced Cybersecurity Services
EUA	Estados Unidos da América
HTML	Linguagem de Marcação do Hipertexto
HTTP	Protocolo de Transferência de Hipertexto
IoT	Internet of Things
IP	Protocol
ITU	International Telecomunication Union
LAN	Local Area Network
NCPS	National Cibersecurity Protection System
NSFNET	National Science Foundation Network
ODS	Objetivos para o Desenvolvimento Sustentável
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PIB	Produto Interno Bruto
RBN	Russian Business Network
TCP	Transmission Control Protocol
TICs	Tecnologias da Informação e Comunicação
UE	União Europeia
WANs	Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

1.1 APRESENTAÇÃO DO TEMA

A partir das discussões iniciais sobre as pré-candidaturas de elegíveis a presidentes dos Estados Unidos (EUA) em 2015, temas relacionados aos processos e procedimentos do período eleitoral tornaram-se foco do país, e, com o aumento exponencial no uso de sistemas conectados a rede um dos objetos observados tanto pelos EUA quanto por outros países, foi o espaço cibernético. Este trabalho pretende demonstrar através do esforço da realização de levantamento bibliográfico, compreensão de dados estatísticos e análises realizadas a partir de relatórios estatais como o ciberespaço foi tratado a partir da ótica da geopolítica a partir de 2015. Esse marco temporal expressa acontecimentos que direcionou olhares para política internacional, pois foi durante a corrida eleitoral de 2016 que a disseminação de informações falsas pela internet tomou proporções que modificaram, nos anos seguintes, o cenário e a disputa eleitora de outros países.

Com base nisso, diferentes atores da sociedade civil como movimentos sociais organizados, grupos políticos e até mesmo hackers começaram a agir em prol de seus objetivos perante as eleições que aconteceriam em 2016. Por isso, presente analise se justifica pela influência da ação de atores não estatais na configuração do ciberespaço passa pela lógica conflituosa dessa esfera a partir de 2015. Alguns acontecimentos foram marcantes nos períodos que antecedem 2015, mas a partir do ano citado ficou ainda mais evidente a importância de discussões que incluem o ciberespaço na política internacional. Após 2015 os países do globo passaram por crises econômicas, sanitárias, a ascensão da extrema-direita e guerras tornaram a relação entre os países cada vez mais frágil. Os Estados ampliaram a segurança dos recursos vulneráveis a ataques cibernéticos, o que foi intensificado após a corrida eleitoral estadunidense de 2016, ano em que as eleições ficaram marcadas pela atuação de hackers nas mídias sociais que levaram a manipulação da opinião pública da população dos Estados Unidos. Essa série de fatos e o conjunto de conceitos explicativos se aplicam à realidade após 2015, com episódios de tomadas de decisão marcados pela postura unilateral e centralizada, tem sido desenvolvida como estratégia política de governantes de diferentes nações. Gerado por uma tendência

estruturada ao longo de acontecimentos que modificou as relações internacionais, esse tipo de comportamento gera sensação de ameaça e um direcionamento para um mundo conflituoso, inicialmente, no discurso, mas que se aplica ao campo cinético e cibernético gradualmente.

O uso das redes conectadas a internet tomou espaço nas discussões e estudos das relações internacionais. Os atores não estatais e o papel que eles desempenham baseadas em seus objetivos e interesses afetam as ações dos Estados assim como eles são atingidos. As ações deles no ciberespaço, em sua maioria, repercutem em no poder dos Estados que atribuem a responsabilidade a outros Estados, a partir de um viés de pensamento realista, em que as relações estatais, são colocados no centro. Isso acontece mesmo em uma dinâmica em que outros atores, nesse caso, atores não estatais, por sua vez hackers atuam no ciberespaço atingindo as ações e preocupações dos Estados mesmo quando não ocupam um território físico ou possuem identidades de acordo com o esperado mediante aos elementos mais marcantes de um Estado, ou seja, território, fronteiras, capacidades e domínio.

Com o intuito de se fechar para si próprio, são prejudiciais ao mundo que vivemos hoje, visto que a sociedade está interconectada por blocos, organizações, pela comunicação e pela interdependência criada pelo advento da globalização. A globalização foi um acontecimento planejado e que permitiu que os Estados pudessem manter relações através de redes sem que cada tomada de decisão precisasse ser tomada em instâncias estatais a todo tempo. Além da comunicação entre Estados facilitada ou intermediada, foi criada uma rede em que todos estivessem conectados de alguma forma. Isso se intensificou com o surgimento e a popularização da internet e aparelhos eletrônicos, há ainda mais conexão e as pessoas podem estabelecer contato de maneira muito mais rápida do que anos atrás.

Nos últimos anos, observamos um aumento exponencial no uso de sistemas conectados à rede. Essa constatação será apresentada no primeiro capítulo deste trabalho. À medida que Estados incorporam essas conexões em suas atividades cotidianas, tornam-se suscetíveis a vulnerabilidades sistêmicas. Alguns casos de ataques e invasões cibernéticas, como Stuxnet – resultado de uma ação empreendida por hackers que causou danos a centrífugas de enriquecimento de urânio no Irã em 2010 – e o caso WannaCry – ataque cibernético que atingiu milhares de organizações com ações de criptografia que bloqueou usuários de computadores e os hackers

responsáveis pela manobra cobrava diferentes valores para devolver dados das pessoas atingidas. Além disso, a disseminação de fake news durante a corrida eleitoral dos Estados Unidos em 2016, evidenciam o avanço das redes e a exposição das estruturas dependentes do ciberespaço a interferências externas (Dunn Cavelty; Wenger, 2020). Para analisar esse cenário, será adotada a teoria realista, que concebe os Estados como protagonistas centrais nas relações internacionais. Esta teoria reconhece a necessidade de adaptação por parte dos Estados ao novo contexto em que estão inseridos, identificando as principais fontes de insegurança no sistema internacional. Isso é fundamental para garantir que os aparatos estatais permaneçam protegidos e capazes de responder aos desafios emergentes no ciberespaço.

Os estudos teóricos tradicionais das relações internacionais se concentram na centralidade do Estado, colocando-o como ator principal do sistema internacional. No entanto, em pesquisas e correntes teóricas que fogem ao *mainstream* da área, outros atores – sociedade civil, organizações não governamentais, instituições privadas, grupos terroristas, hackers – são colocados em pauta. O debate das relações internacionais se divide em subáreas e o presente trabalho é fruto do esforço de analisar a construção e o papel atribuído ao Estado no ciberespaço a partir de duas abordagens teóricas, o construtivismo e o realismo. Essa pesquisa tem o intuito de apresentar e testar a hipótese de que os atores estatais, impactados pelas inovações tecnológicas e acontecimentos que modificaram interações no cenário internacional, são parte dos moldes atuais do ciberespaço. Assim, a geopolítica teria impactado diretamente a forma construtivista em que o espaço cibernético foi construído – por meio das relações sociais – visando a melhoria e conexão de redes em prol da comunicação e interconexão global para um espaço securitizado e realista.

A teoria construtivista, uma das correntes teóricas presentes no trabalho, é inserida na análise com base no argumento de que os Estados são uma construção social (Wendt, 1994). Essa perspectiva sustenta que a construção da identidade dos Estados, como proposto por Wendt (2003), é constituída pelas relações sociais em diferentes níveis, tanto nacional quanto internacionalmente. Dentro desse subtópico da pesquisa, argumenta-se que, ao posicionar-se internacionalmente, um Estado traz consigo um conjunto de elementos que compõem sua identidade nacional. Externamente, esse Estado desenvolve uma identidade coletiva, formada pelas interações e interesses provenientes de cada ente estatal, convergindo para um

espaço comum. Assim, quando o ciberespaço, principal objeto de estudo do trabalho, é lido pelo construtivismo, questiona-se a forma como as relações que foram construídas coletivamente se movem para a esfera securitária. Isso acontece quando os Estados são colocados como os principais atores do sistema e assumem que, do mesmo modo em que espaços geográficos com divisões fronteiriças e interesses políticos e econômicos foi constituído, o ciberespaço também é um espaço que está envolto por elementos que geram insegurança interna e externa aos Estados, potencializando problemas securitários.

Para a teoria realista, os Estados estão nos centros das interações. Com a necessidade de manutenção da sobrevivência das unidades nacionais no sistema internacional, os Estados almejam a proteção. Para isso, diferentes estratégias de segurança são utilizadas. O realismo possui uma visão securitária das relações internacionais e explica a geopolítica como um dos fatores essenciais para a manutenção do Estado. Segundo essa teoria, é pela lógica e dimensão do conflito que as relações são desenvolvidas e conduzidas. Essa teoria será utilizada para apresentar e analisar o conflito e o cenário geopolítico conforme as interações entre os Estados e a disputa pelo poder.

O enfraquecimento nas tratativas estatais no cenário internacional gera constrangimento nas relações. Assim, através de um comportamento nacionalista e protecionista, os Estados agem na tentativa de restringir relações em prol de segurança e defesa contra ameaças externas. Estas ameaças não se limitam a atores estatais, mas também envolvem atores não-estatais que interferem nas atividades dos Estados, comprometendo a opinião pública, interrompendo a ordem, provocando medo ou sabotando infraestruturas críticas, espionando alvos em prol de seus objetivos particulares ou políticos; qualquer opção supracitada é capaz de provocar sensação de insegurança aos Estados e a sociedade civil. Por essa razão, pensando na dinâmica do ciberespaço, é possível observar novos cenários no campo da segurança internacional.

Ações que acontecem e envolvem o ciberespaço e principalmente a internet colocam diferentes campos de estudos das relações em debate. A segurança internacional é um deles, e, neste trabalho a teoria realista explica como a dinâmica da geopolítica, a partir de acontecimentos nas relações internacionais, incorporou discussões sobre ciberespaço a sua análise. Mediante a uma pesquisa bibliográfica e

os levantamentos realizados para essa pesquisa, as discussões sobre esse eixo temático aumentou nos últimos anos proporcionalmente aos impactos dos acontecimentos econômicos e políticos dos últimos anos que se intensificaram com a pandemia de Covid-19, que teve início em 2020 e a Guerra da Ucrânia. Esses dois acontecimentos recentes geraram grande pressão sobre a interação dos países no sistema e o tratamento dos temas de política internacional em óticas securitárias aumentou por se tratar de um momento de gestão de crise e por essa ocasião a bandeira de agir com base na defesa nacional foi veementemente erguida.

O objetivo geral desta dissertação é investigar como a geopolítica intensificou as mudanças nas interações entre Estados e atores não estatais, com foco nos casos de atuação de hackers para ilustrar o papel desses atores no ciberespaço. Dessa forma, o levantamento bibliográfico realizado na pesquisa desempenhará o papel de atender aos seguintes objetivos específicos: 1) Conduzir um debate entre a teoria construtivista e a teoria realista, explorando os elementos que possibilitam a compreensão das motivações políticas estabelecidas ao longo do tempo, levando alguns Estados a fortalecerem sua segurança e defesa a partir de 2015; 2) Definir os conceitos de atores não estatais e ciberespaço, contextualizando como esses conceitos ascenderam nas Relações Internacionais e relacionando as atribuições dos atores não estatais no ciberespaço; 3) Analisar as mudanças geopolíticas mundiais a partir de 2015 e verificar como impactaram as interações que resultaram em alterações significativas nos anos subsequentes a 2020 no cenário global, provocando reações no espaço cibernético e nas relações entre atores presentes no mesmo.

Esta dissertação está organizada em três capítulos, cada um correspondendo aos objetivos específicos delineados no trabalho. O primeiro capítulo introduz o tema que será analisado ao longo do trabalho, fornecendo definições e conceitos relacionados à internet. Além disso, será abordada a influência de instituições responsáveis pelos avanços históricos na rede de computadores e telecomunicações, ou seja, o ciberespaço. O capítulo também incluirá dados estatísticos referenciados por organizações internacionais para justificar a necessidade de contribuições na área. Este trecho, intitulado "A influência da internet para o desenvolvimento global", visa elucidar e explicar como a internet evoluiu ao longo da história, suas implicações e o momento em que os Estados começaram a incorporá-la em suas considerações de política internacional.

O segundo capítulo será uma extensão do primeiro fragmento da dissertação em termos conceituais. Nele, ocorrerá o aprofundamento das teorias construtivistas e realistas para esclarecer como o espaço cibernético pode ser considerado como um objeto de estudo dentro dessas teorias. Essa ampliação envolverá a incorporação dos principais conceitos das duas abordagens teóricas, que são lentes frequentemente utilizadas por estudiosos da área de relações internacionais para analisar a dinâmica política do cenário internacional. No contexto deste trabalho, essas teorias serão aplicadas para compreender o comportamento tanto de atores estatais quanto não estatais no ciberespaço. Consequentemente, para cumprir o objetivo desta pesquisa, o aporte teórico, constituído pelos elementos mencionados, estabelecerá uma conexão entre a evolução e dissolução dos eventos no ciberespaço. Isso será realizado por meio de análises que empregarão a perspectiva proporcionada por essas teorias para interpretar os acontecimentos nesse ambiente específico.

O terceiro capítulo será dedicado à compreensão das atividades de atores não estatais, com foco especial no papel dos hackers no ciberespaço. Esses indivíduos serão os atores centrais para o desenvolvimento da análise que culminará no fechamento do trabalho. O capítulo visará elucidar como os atores não estatais reagem ao cenário geopolítico na prática. Para atingir esse objetivo, serão apresentados casos de ataques e interferências perpetrados por hackers russos. Esses exemplos serão explorados para demonstrar como a política e a economia globais influenciam esses grupos, motivando suas reações e interações no ciberespaço. O capítulo buscará evidenciar como esses atores não estatais, notadamente os hackers, criam suas próprias dinâmicas e narrativas em resposta ao contexto geopolítico em constante evolução.

A conclusão cumprirá a função de fornecer uma resposta à pergunta de pesquisa “Qual a influência da geopolítica na ação dos atores não estatais no espaço cibernético a partir de 2015?”, contrastando-a com a hipótese formulada a partir do objetivo geral do trabalho. Este capítulo representará uma síntese das análises conduzidas com base nos casos apresentados de atuação dos atores não estatais, neste caso, os hackers, destacando os interesses e comportamentos dos Estados em face da dinâmica geopolítica no cenário internacional. Para desenvolver as considerações finais, serão estabelecidas conexões a partir da importância tanto dos atores estatais quanto dos não estatais para as relações internacionais. A conclusão

proporcionará uma visão abrangente e integrada das descobertas obtidas ao longo da dissertação, consolidando as contribuições para a compreensão das relações entre geopolítica e atores não estatais no ciberespaço, conforme delineado pelos objetivos específicos.

Conforme será evidenciado ao longo da argumentação desenvolvida neste trabalho, os conhecimentos sobre o ciberespaço estão em constante movimento e evolução. Por esse motivo, o texto que encerrará este trabalho de conclusão de mestrado é uma tentativa de elaborar uma análise concentrada no panorama atual da geopolítica e do ciberespaço, proporcionando um fechamento reflexivo à dissertação.

2 A INFLUÊNCIA DA INTERNET PARA O DESENVOLVIMENTO GLOBAL

2.1 A RELEVÂNCIA DA INTERNET PARA A CONSTRUÇÃO SOCIAL MODERNA

A internet tem se desenvolvido por diversos fatores. Um desses ocorre no contexto internacional por meio do sistema de acesso à rede global de computadores. A rede global de computadores teve início no período da Guerra Fria nos Estados Unidos e Europa Ocidental no projeto de pesquisa militar *Advanced Research Projects Agency*[1] (ARPA). O projeto ARPA consistia na transmissão de dados sigilosos entre militares auxiliando-os no período da guerra. Apesar de ter sido iniciado com os militares na Guerra Fria, o conhecimento técnico sobre a transmissão de dados não se restringiu, no entanto, a essas pessoas. A *National Science Foundation* (Fundação Nacional da Ciência dos Estados Unidos) expandiu as pesquisas sobre o funcionamento desses setores, publicizando-os. A partir de então, houve uma difusão de acesso à rede, o que tornou possível a integração entre pessoas de diferentes localidades do mundo (Glowniak, 1998; Kurbalija, 2016).

Uma das razões para o surgimento da internet foi a necessidade de transmitir informações. A demanda por comunicação de maneira rápida e eficiente motivou que aparelhos de informática fossem conectados à internet. A ARPA foi a primeira rede de computadores funcional existente e conectou sistemas que transmitiam dados confidenciais por todo território estadunidense entre os anos 1960 e 1970. Assim, a ARPA impulsionou o funcionamento das redes militares através de um padrão que gerasse contato entre computadores localizados em lugares distintos capazes de assegurar a manutenção das operações das agências de segurança norte americanas (Glowniak, 1998; Dias, 1999; Oliveira, 2014).

Nos primeiros anos de internet, o crescimento de conexões foi um processo vagaroso. O projeto experimental da ARPA interligou quatro centro de pesquisas dos EUA. Foram conectadas as Universidade da Califórnia em Santa Bárbara, Universidade da Califórnia em Los Angeles, Stanford e a Universidade de Utah. Nas primeiras fases do projeto, a complexidade envolvida nos processos exigia um alto nível de instrução dos pesquisadores deste setor. Por isso, inicialmente, a área foi desenvolvida de maneira lenta, prova disso é que apenas um computador era

[1] Rede de Agências de Pesquisa em Projetos Avançados.

conectado à internet a cada duas ou três semanas. Assim, a fase inicial do uso da rede foi limitada e restrita até que, nos anos 1990, novas pesquisas foram desenvolvidas, ampliando a conexão de uma ampla gama de usuários com os sistemas e provedores de internet (Glowniak, 1998; Dias, 1999; Oliveira, 2014).

Progressivamente, o uso de máquinas conectadas à rede cresceu. Nos anos 1980, os *Transmission Control Protocol* (TCP) e *Internet Protocol* (IP)[2] permitiram que qualquer computador, independente das suas configurações de hardware e sistema operacional, se conectasse a internet. Em 1981, aproximadamente 200 computadores acessavam à rede. Neste momento, os aparelhos eletrônicos estabeleciam conexão com uma rede local chamada de *Local Area Network* [3] (LAN) que por sua vez se conectava com a ARPA por meio de um roteador[4]. Em outros casos, um número maior de LANs ligava-se a *Wide Area Network* (WANs)[5] que posteriormente estabelecia conexão com a *Advanced Research Projects Agency Network* (ARPANET). Esses padrões de protocolos foram massivamente disponibilizados para que o uso da rede crescesse (Glowniak, 1998).

Foi necessária uma mudança de formato para viabilizar a expansão da internet. Em 1985, a *National Science Foundation Network* (NSFNET), idealizada pela *National Science Foundation,* tomou o lugar da ARPANET e conectou a internet às redes telefônicas. Isso possibilitou a conexão em alta velocidade, utilizando os serviços de distribuição de rede à longa distância das empresas de telecomunicações, por meio da tecnologia de fibra ótica nacional e internacional e dos Provedores de Serviços de

---

[2] "O nome TCP/IP refere-se a um conjunto de protocolos de comunicação de dados. O nome é enganoso porque TCP e IP são apenas duas de dezenas de protocolos que compõem a suíte. Seu nome vem de dois dos protocolos mais importantes da suíte: o Protocolo de Controle de Transmissão (TCP) e o Protocolo Internet (IP).

O TCP/IP teve origem na pesquisa investigativa sobre protocolos de rede que o Departamento de Defesa (DoD) iniciou em 1969. Em 1968, a Agência de Projetos de Pesquisa Avançada do DoD (ARPA) começou a pesquisar a tecnologia de rede que hoje é chamada de comutação de pacotes." (CISCO, 2023b)

[3] "Uma Rede Local (LAN) é um conjunto de dispositivos conectados em um único local físico, como um edifício, escritório ou casa. Uma LAN pode ser pequena ou grande, desde uma rede doméstica com um usuário até uma rede empresarial com milhares de usuários e dispositivos em um escritório ou escola" (CISCO, 2023c).

[4] "Os roteadores orientam e direcionam os dados da rede, usando pacotes que contêm vários tipos de dados, como arquivos e comunicações e transmissões simples, como interações na Web.

Os pacotes de dados têm várias camadas ou seções, uma das quais contém informações de identificação, como remetente, tipo de dados, tamanho e, o mais importante, o endereço IP de destino (protocolo de Internet). O roteador lê essa camada, prioriza os dados e escolhe a melhor rota a ser usada para cada transmissão" (CISCO, 2023a).

[5] "Uma Rede de Longa Distância (WAN) ou Rede de Área Metropolitana (MAN) cobre áreas geográficas maiores. Algumas WANs e MANs conectam muitas LANs juntas" (CISCO, 2023c).

Rede (NSPs). A conjuntura dos anos 1980 possibilitou a conexão em outros países e alavancou a quantidade de computadores com acesso à internet, o que ocorreu com o intuito de fomentar instituições de educação e pesquisa dos EUA. Assim, facilitou-se o uso de aparelhos de informática conectados à rede (Glowniak, 1998).

Na década de 1990, o uso da internet cresceu exponencialmente. Nesse período surgiu o HTML (Linguagem de Marcação do Hipertexto) e o protocolo de comunicação HTTP (Protocolo de Transferência de Hipertexto), que permitiu que documentos fossem enviados pela internet ampliando a comunicação na internet.

> A Internet continua a expandir em ritmo acelerado. Muitos novas pesquisas e tecnologias são continuamente testadas e implementadas. Dentro dos próximos anos, serão desenvolvidas novas capacidades que integrarão a Internet em muitas áreas da medicina, da ciência e da vida cotidiana. Uma das principais mudanças que ocorrem atualmente é a velocidade na qual os indivíduos podem acessar informações (Glowniak, 1998, p. 144).[6]

Este foi o momento em que outros atores, além dos acadêmicos, passaram a atuar na rede, fazendo com que o número de usuários escalasse (Dias, 1999; Oliveira, 2014).

Os avanços da internet até aquele momento fomentaram a ideia de que o modo de vida sofreria grandes alterações. O intercâmbio de informações de maneira mais rápida e em tempo real gerava mais oportunidades com o acesso à rede. Surgiu, neste período, o termo Internet das Coisas[7] (IoT). A *International Telecomunication Union* (ITU) define a IoT como "uma infraestrutura global para a sociedade da informação permitindo avançados por meio da conexão (física e virtual) de coisas baseadas em tecnologias da informação e comunicação interoperáveis existentes ou em evolução" (ITU, 2016, p. 10)[8], que está relacionada com a conectividade e a produção e transmissão de dados entre máquinas e pessoas e máquinas. Essas interações são importantes tanto por fornecer dados básicas para o dia a dia das pessoas, quanto como banco de dados para pesquisas mais complexas. A IoT fornece, portanto, uma

---

[6] Traduzido de: "The Internet continues to expand at a rapid pace. Many new developments and technologies are being continually tested and implemented. Within the next few years, dramatic new capabilities will be developed that will integrate the Internet into many areas of medicine, science, and daily life. One of the major changes occurring at present is the speed at which individuals can access information."

[7] Traduzido de: "Internet of Things."

[8] Traduzido de: "[...] a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication Technologies."

evolução na dinâmica da transferência de dados que circulam pela rede (Zhou *et al.*, 2021; ITU, 2016; Ge; Bangui; Buhnova, 2018).

Houve mudanças significativas no uso da internet. A massificação do acesso a rede permitiu que cada vez mais atividades diárias fossem realizadas ou intermediadas pela internet. Segundo a ITU, isso aconteceu a partir do desenvolvimento da conexão wireless, das redes móveis, identificação via rádio frequência, sensores de coleta de dados e nanotecnologia. Além disso, "a redução do custo dos aparelhos de informática (incluindo sensores) e a evolução do Wi-Fi são fatores que impulsionam o crescimento em aplicações da IoT" (ITU, 2016, p. 15)[9]. Essas alterações são eficazes em diversos domínios. Elas implicam no desenvolvimento de pesquisa, avaliação e monitoramento em diversos setores como saúde, saneamento, políticas públicas, agricultura e gestão de recursos. Assim, com a perspectiva de obter melhores técnicas, processos e acessos, podem ser geradas novas oportunidades de avanços em variadas esferas do cotidiano da humanidade (ITU, 2016).

O avanço da internet esbarra em alguns desafios. A possibilidade de criar, armazenar e compartilhar dados, potencializada pelo avanço da IoT, gera riscos para os usuários. Essas adversidades estão relacionadas sobretudo a privacidade e a segurança. Em 2019, foi realizada uma pesquisa sobre a privacidade na rede. Nela, foi constatado que em média uma pessoa a cada quatro não confia na internet. "As preocupações têm intensificado nos últimos anos sobre como acesso à internet tem proliferado, tais como privacidade, segurança cibernética, conteúdo nocivo, e o poder de grandes empresas" (ITU, p. 9, 2022a). Essa desconfiança deriva de vazamento de dados pessoais, assédio, hackeamento, vírus, roubo de informações sigilosas, acesso de crianças à sites maliciosos e disseminação de *fake news* ou desinformação

> Além das notícias falsas, a desinformação é igualmente conceituada como uma forma de (contra)argumentação política em que os fatos aparecem seletivamente em narrativas alternativas relativas a contextos políticos e ideológicos, muitas vezes descontextualizados com intenções especulativas. A desinformação também é vista como propaganda externa que inclui fatos fabricados e fictícios disseminados e amplificados on-line com intenções de criar divisões. Considerando a transformação radical do trolling e dos mimos

[9] Traduzido de: "The reduction in the cost of computing (including sensors) and the growth of Wi-Fi are enabling factors driving growth in IoT applications."

> ao longo do tempo, nossa primeira pergunta de pesquisa visava conhecer a opinião dos hacktivistas sobre essa transformação no contexto das conceitualizações concorrentes entre os usuários comuns de mídia social (Sharevski; Kassell, 2023, p. 6)[10].

Por isso, diversas vulnerabilidades impedem que a conexão com a internet tenha riscos limitados ou nulos. A privacidade na internet ainda é um tema que precisa avançar, para isso é necessário que sejam realizados esforços conjuntos para a proteção de dados (ITU, 2016; ITU, 2022a).

Surgiram preocupações sobre o uso da rede. As principais dúvidas das pessoas conectadas à internet estão relacionadas à segurança de seus dados e dispositivos. Os usuários normalmente levantam questionamentos sobre quais são os métodos adequados para proteção e se os mecanismos utilizados são de fato eficazes. Chukwuere (2022) afirma que é necessário proteger os dispositivos, a segurança dos dados e a privacidade pessoal para um ciberespaço seguro. Alguns itens como a falta de atualização, protocolos de segurança, conscientização e monitoramento ativo dos usuários podem expor as vulnerabilidades dos sistemas (Chukwuere, 2022). Há uma preocupação em relação a esse tema que pode até, em casos específicos, levar à vigilância em larga escala "[...] transformando a sociedade da informação em sociedade da vigilância, pois sistemas de gestão de identidade podem melhorar sem enfatizar paralelamente o anonimato e a propriedade dos dados pessoais"[11] (ITU, p. 42, 2016). Assim, a segurança no ciberespaço se tornou pauta importante no debate sobre a internet e seu desenvolvimento.

2.2 O USO DA INTERNET: AVANÇOS E LIMITES

Reconhecido pelos Objetivos para o Desenvolvimento Sustentável (ODS), a conectividade acelera e amplia o desenvolvimento. Isso se deve às vantagens que a

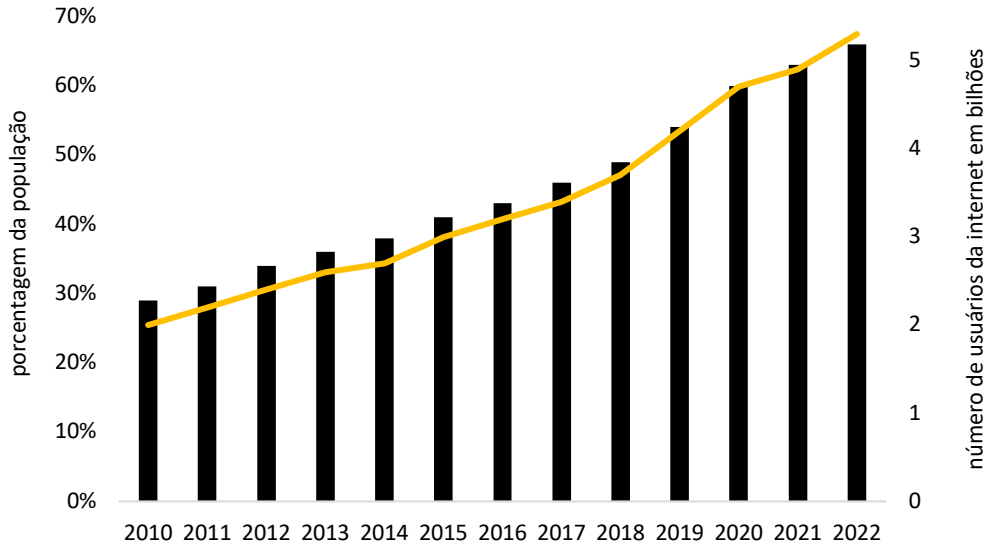
[10] Traduzido de: "Beyond just fake news, misinformation is equally conceptualized as form of political (counter)argumentation where facts do selectively appear in alternative narratives relative to political and ideological contexts, often taken out-of-context with speculative intentions. Misinformation is also seen as external propaganda that includes manufactured facts and factoids disseminated and amplified online with division-creating intentions. Given the radical transformation of the trolling and mimes over time, our first research question aimed to learn the hacktivists' take on this transformation in the context of the competing conceptualizations amongst ordinary social media users".

[11] Traduzido de: "[...] turn the 'Information Society' into the 'Surveillance Society', as identity management systems improve without parallel emphasis on anonymity and ownership of personal data".

internet oferece e ao seu potencial para ajudar as pessoas ao longo do tempo. Através da rede, as pessoas podem se comunicar, desfrutar de lazer, estabelecer sua identidade e se sentir parte de uma comunidade, além de terem acesso a serviços, recursos e oportunidades. Além disso, as Tecnologias da Informação e Comunicação (TICs) podem gerar dados em grande volume, contribuindo para o empreendimento de novas soluções e projetos. Isso significa que a conectividade faz parte e é um elemento favorável ao desenvolvimento (ITU, 2022a).

A pandemia de Covid-19 causou grandes impactos na vida humana. Isso aconteceu em decorrência das medidas de distanciamento social, restrição e bloqueios generalizados que levaram ao fechamento ou redução da capacidade de atendimento de estabelecimentos de serviços não essenciais. Nesse período, a internet se tornou indispensável. As empresas e instituições de ensino adotaram o modelo de trabalho remoto e educação à distância. Outros setores impactados foram os de serviços de saúde e atendimento ao público que, em muitos casos, passaram a ser oferecidos exclusivamente online. Dessa forma, a pandemia evidenciou a importância da internet como um recurso essencial para a vida humana. O cenário de crise manteve crescente o número de novos adeptos à rede, que passou de 4,1 bilhões de usuários em 2019 para 4,9 bilhões de pessoas em 2021 e 5,3 bilhões em 2022, um aumento de 6,1% em relação ao ano anterior (ITU, 2021; UN, 2021). No gráfico abaixo pode ser observado o crescimento no número de usuários da internet entre os anos 2010 e 2022.

Gráfico 1: Usuários da Internet (2010 - 2022)



Fonte: ITU, 2022b.

O acesso à internet ainda não está ao alcance de todos. Mesmo com o constante crescimento no número de usuários conectados, ainda há uma parcela da sociedade que não tem acesso à rede. Apesar da internet ter facilitado o acesso a recursos essenciais durante a pandemia, cerca de 2,9 bilhões de pessoas, 96% dessas residentes de países em desenvolvimento, continuam sem acesso à internet. A exclusão digital foi escancarada durante pandemia de Covid-19, houve um aumento da desigualdade social e, em um mundo em que 95% da população global tem possibilidade de se conectar a redes móveis, uma média de 390 milhões de pessoas não possui nenhuma chance de estar conectada pela falta de ferramentas básicas, como um smartphone. Portanto, as desigualdades presentes na sociedade se perpetuam para além das fronteiras físicas, estando presentes também na internet (ITU, 2021; ITU, 2022a).

Há ainda uma parcela da população mais excluída do que as demais. Mulheres e idosos enfrentam maiores dificuldades para acessar e se adaptar ao uso das redes. Grande parte da exclusão digital está relacionada a pobreza, analfabetismo, falta de energia elétrica, desconhecimento e conscientização digital, definindo então uma lacuna, muito presente no meio rural dos países em desenvolvimento. A divisão de gênero se localiza principalmente na África e países árabes, locais onde há limitações quanto ao acesso das mulheres à internet, impostas por regras políticas ou culturais, que esbarram tanto na liberdade de expressão quanto no imperativo da manutenção da desigualdade de gênero. Em relação à juventude, os usuários da internet representam 71% dos jovens de 15 a 24 anos, enquanto nas outras faixas etárias representam 57%. Em contrapartida, pessoas que vivem em cidades, homens e jovens são maioria quando se trata de usuários da internet. A exclusão digital é um obstáculo a mais na busca da igualdade social e econômica desses grupos (ITU, 2021; Tallmann, 2023).

A conectividade deve ser universal. Segundo o Relatório de Conectividade Digital da União Internacional de Telecomunicação, o objetivo para esta década é que exista uma conectividade para todos e em todos os lugares, de forma segura, eficiente, produtiva e acessível. Isso pode ser idealizado por meio da evolução da tecnologia, que possui capacidade de gerar benefícios a longo prazo no que diz respeito a remoção de barreiras e desigualdades digitais. Nesse sentido, a internet

seria capaz de avançar em termos de disseminação do acesso com o apoio de políticas e iniciativas que tenham como objetivo a conectividade (ITU, 2022a).

2.3 SEGURANÇA CIBERNÉTICA NO CONTEXTO ESTATAL

O ciberespaço mudou a dinâmica das Relações Internacionais. A segurança cibernética começou a ser discutida no início das décadas de 1970 e 1980. Nos anos 1990, as principais ideias sobre essa temática foram distribuídas pelo globo. Nos anos 2000, a cibersegurança tornou-se uma das preocupações centrais dos Estados. Isso está relacionado a crescente utilização das redes para troca e armazenamento de informações sigilosas e estratégicas. São cada vez mais comuns casos de espionagem e ataques cibernéticos divulgados com a autoria de diferentes atores, que buscam acessar essas informações com o objetivo de obter vantagens nas discussões e movimentos estratégicos dos Estados. Progressivamente, essas ações mostram-se perigosas, articuladas e difundidas em diversos países. Ou seja, elas representam ameaças para a segurança nacional (Institute for Strategic Studies, 2012)

A cibersegurança se tornou ponto de atenção dos Estados. Tornou-se mais difícil encontrar e identificar os oponentes, suas técnicas e motivações. Esse momento pode ser descrito por ter “condições geoestratégicas mais dinâmicas, áreas mais numerosas e preocupantes, e adversários menores, mais ágeis e mais diversificados” (Institute for Strategic Studies, 2012, p. 106)[12]. Com base nesse sentimento de vulnerabilidade, a militarização do espaço cibernético foi uma alternativa viável, encontrada como tentativa de conter possíveis conflitos (Institute for Strategic Studies, 2012).

O quadro a seguir apresenta os termos mais utilizados nos estudos sobre o espaço e segurança cibernética.

[12] Traduzido de: [...] more dynamic geostrategic conditions, more numerous areas and issues of concern, and smaller, more agile, and more diverse adversaries.

Quadro 1: Definições dos termos mais utilizados nos estudos sobre ciberespaço

Nome	Definições
Espaço Cibernético	É um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, computadores e processadores embutidos e controladores (Department of Defense, 2010, p. 58).[13] O espaço cibernético é um domínio caracterizado pelo uso da eletrônica e do espectro eletromagnético para armazenar, modificar e trocar informações via rede sistemas de informação e infraestruturas físicas (Webster, 2010, p. 5).[14]
Segurança Cibernética	Prevenção de danos, proteção e restauração de computadores, sistemas de comunicação eletrônica, serviços de comunicação eletrônica, fio comunicação, e comunicação eletrônica, incluindo as informações nela contidas, para assegurar sua disponibilidade, integridade, autenticação, confidencialidade e não-repúdio (Department of Defense, 2010, p. 57). [15]
Poder Cibernético	A capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todas as operações ambientes e através dos instrumentos do poder (KUEHL, 2009, p. 38).[16]
Ataque cibernético	Operações para interromper, negar, degradar ou destruir informações presentes em computadores e em redes de computadores, ou os próprios computadores e redes (WEBSTER, 2010, p. 16).[17]
Hackers	O termo Hacker é geralmente usado para descrever este indivíduo e pode ser definido como alguém que faz tentativas não autorizadas de acessar um banco de dados (computador) hospedeiro, geralmente a partir de um local remoto, frequentemente contornando os controles de acesso. O Hacker usará a imitação ou mascará como um usuário autorizado para obter acesso ao computador hospedeiro. Em alguns casos, o Hacker será, de fato, um usuário autorizado ao sistema e estar fazendo tentativas de acesso em áreas não autorizadas ou no computador (US DEPARTMENT OF JUSTICE, 1989, p. 70).[18]
Espionagem Cibernética	Acesso não autorizado a computadores e servidores com a finalidade de se testar a configuração e sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas (INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).[19]

[13] Traduzido de: A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Department of Defense, 2010, p. 58).

[14] Traduzido de: Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures (Webster, 2010, p. 5).

[15] Traduzido de: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (Department of Defense, 2010, p. 57).

[16] Traduzido de: The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power (KUEHL, 2009, p. 38).

[17] Traduzido de: Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (WEBSTER, 2010, p. 16).

[18] The term Hacker is most generally used to describe this individual and can be defined as someone who makes unauthorized attempts to access a host database (computer) most generally from a remote location, often by circumventing access controls. The Hacker will use impersonation or masquerading as an authorized user to gain access to the host computer. In some instances the Hacker will in fact be na authorized user to the system and be making access attempts into unauthorized areas o the computer US DEPARTMENT OF JUSTICE, 1989 p. 70).

[19] Traduzido de: The unauthorised probing to test a target computer's configuration or evaluate its system defenses, or the unauthorised viewing and copying of data files (INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).

Nome	Definições
Sabotagem Cibernética	Criação de empecilhos ao desenvolvimento de processos e rotinas de trabalho nos setores público e privado a partir de meios eletrônicos (INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).[20]
Guerra Cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação (INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).[21]

Fonte: Elaboração Própria

A internet oferece novos desafios aos Estados. No século XXI, as inovações tecnológicas propiciaram o surgimento de ameaças à segurança de indivíduos e Estados. Exemplos disso foram os ataques à Estônia em 2007, que atingiram sites de organizações públicas, bancos e empresas de comunicações. Nesse caso, o país assumiu a Rússia como culpada, mas a autoria dos ataques nunca foi comprovada. Há também o caso dos ataques cibernéticos acompanhados pela crise Russo-ucraniana, que tiveram como alvos os sites do governo ucraniano, empresas de telecomunicação e veículos de mídia importantes. Os atores responsáveis pelos ataques foram hackers patriotas russos. Esse tipo de acontecimento evidencia a complexidade das relações internacionais no século XXI e as nuances em relação à atores e suas ações (Choucri; Goldsmith, 2012; Institute for Strategic Studies, 2012).

A estrutura dos Estados está intrinsecamente ligada à tecnologia, tornando-nos cada vez mais dependentes do eficiente desempenho de sistemas informacionais. A crescente interdependência entre os países e os avanços tecnológicos resultaram em desafios significativos relacionados à segurança internacional. A partir disso, as infraestruturas críticas, responsáveis pela prestação de serviços essenciais à sociedade, tornam-se alvos de interesse para potenciais ataques. Isso motivou a elaboração de planos nacionais direcionados à segurança dessas infraestruturas. Esse tipo de ação é crucial, uma vez que essas infraestruturas são atingidas, podem causar consequências que afetam a vida de milhares de pessoas (Gallais; Filiol, 2017; Institute for Strategic Studies, 2012).

Os limites da atividade atividades online são pouco definidos quando é pensada a maneira como a comunicação realizada repercute na sociedade. Acredita-se que esse é um espaço sem regras, ou com regras limitadas, o que potencializa os riscos

[20] The deliberate disturbance of an economic or military process for achieving a particular (often political) goal with cyber means (INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).

[21] Traduzido de: The use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. The term is also used loosely for cyber incidents of a political nature(INSTITUTE FOR STRATEGIC STUDIES, 2012, p. 116).

inerentes a esfera virtual. Nesse sentido, estabelecer controle nas ações e no conteúdo difundido na internet é trabalhoso, os riscos e as consequências não são pré-estabelecidos ou perceptíveis à primeira vista, isso acontece tanto para os indivíduos quanto para as organizações. Por isso, são necessárias equipes especializadas para controlar o que pode ser difundido ou não por organizações e Estados em relação a informações sensíveis e confidenciais.

O debate em torno da regulação do espaço cibernético é constante. A discussão sobre soberania no ciberespaço tem aumentado e a evolução para um regime baseado em normas internacionais permanece lenta. Esse cenário é influenciado pelos interesses estratégicos dos Estados em manterem um espaço em que as suas ações possam ocorrer com uma mínima interferência das barreiras tradicionais impostas pelas fronteiras, especialmente dada a velocidade com que as informações são disseminadas. A questão, permeada por desafios políticos, divide-se "entre os países que insistem na soberania do Estado no ciberespaço e aquelas que interpretam tais chamadas como forma de assegurar o controle do Estado através da Internet" (Pawlak, 2017, p. 3).[22] Como outras discussões multilaterais, esse debate se tornou politizado e é utilizado para a manutenção de interesses nacionais (Martins, 2012; Pawlak, 2017).

O tema da regulação do ciberespaço é monitorado por organizações multilaterais, e esforços têm sido feitos na ONU para a elaboração de tratados que estabeleçam uma base jurídica internacional para tal regulação. No entanto, essa empreitada é desafiadora. Vários tratados propostos não foram ratificados, e a perspectiva de sucesso para novas tentativas permanece incerta. A resistência à aceitação de normas pela comunidade internacional é atribuída ao fato de que alguns Estados podem se beneficiar com a ausência de regulamentações. Além disso, as organizações e empresas desempenham um papel limitado nessas negociações, dada a centralidade dos Estados na discussão. Essa abordagem protagonizada pelos Estados abre brechas para que eles exerçam um controle mais amplo sobre a Internet, transformando um espaço originalmente aberto e de livre circulação em um ambiente centralizado no poder estatal. Independentemente dessas dificuldades, ações

[22] Traduzido de: between the countries which insist on state sovereignty in cyberspace and those which interpret such calls as way to ensure state control over the internet.

conjuntas, seja por meio de acordos bilaterais ou multilaterais, continuarão sendo implementadas para garantir a segurança no ciberespaço (Pawlak, 2017).

A interconexão entre o local e o global foi estabelecida através da transformação na distribuição de informações e do avanço do poder tecnológico. Esse fenômeno foi impulsionado pelo uso crescente da internet, o que, por sua vez, ampliou o processo de interdependência. A expansão do uso de ferramentas tecnológicas também provocou uma reconfiguração nos conceitos de segurança, tanto em nível nacional quanto internacional. Esse fenômeno decorre da presença diversificada de atores na rede. Em outras palavras, o sentimento de insegurança é fomentado pelas inúmeras oportunidades que as tecnologias sofisticadas proporcionam para que atores ameacem a segurança uns dos outros (Zendelovski; Cvetkovski, 2021).

Nesse sentido, a internet consolidou-se como um espaço de atenção para a segurança internacional. Existem questionamentos sobre o ciberespaço que ainda não foram solucionados, relacionados principalmente a rapidez e a dinâmica desse espaço, que afetam substancialmente a segurança dos Estados e da ordem internacional. Diante desse cenário, encontrar políticas para a segurança que consigam suprir o atraso existente em relação ao avanço das ameaças cibernéticas é, neste momento, uma forma de gerir suas complexidades (Zendelovski; Cvetkovski, 2021; Choucri; Goldsmith, 2012).

No chamado “futuro” digital, existe a expectativa de que ferramentas conectadas a rede sejam o principal instrumento de poder dos Estados, organizações e pessoas. Hoje, isso já é observado quando se trata de fake news, como ocorreu nos ataques cibernéticos realizados por hackers russos à Ucrânia em 2013, em que uma das façanhas utilizadas por esses atores foi a disseminação de informações falsas. Esse tipo de ação mina a confiança da população gerando uma série de consequências para a sociedade. Hoje, o aumento no número de aparelhos e equipamentos conectados à internet e as mudanças na sociedade advindas do contato com as inovações tecnológicas, abrem espaço para um grande poder de influência dos atores, o que contribui para um número crescente de ataques cibernéticos (Pernik, 2018; Zendelovski; Cvetkovski, 2021).

Quando se trata da vertente política, acredita-se que os novos meios e oportunidades de engajar nessa frente têm chamado atenção de muitos atores. O uso da rede abrange diversas demandas, a vida política é uma delas e vem causando

grandes alterações no padrão de comportamento das pessoas no que diz respeito ao uso da internet como meio de interagir e participar de processos com fins políticos. O espaço virtual abriu caminhos para que os mais diferentes atores demonstrem suas posições perante a regimes e governos por todo o mundo, mudando e oferecendo a possibilidade de formação de opinião e identidade (Kim, 2006).

Nesse espaço também foi alterado o comportamento político dos Estados. “[...] ciberespaço ficou entendido como um local em que a autoridade, os limites e a geografia eram fracas ou não se aplicavam” (Mainwaring, 2020, p. 1).[23] O que significa, na leitura de Mainwaring (2020), que os Estados utilizam o espaço cibernético para obter vantagens estratégicas, como usariam um espaço em que se poderia munir de armamentos para garantir em alguma instância vantagens políticas e alterar o status quo de acordo com as capacidades e poder dos Estados atuantes em um dado contexto. Esse espaço em questão se tornaria, portanto, um local onde seriam tomadas medidas ofensivas com base em suas possibilidades em ameaças. Esse entendimento pode ser visto na prática quando se observa o contexto em que a internet foi criada e têm sido moldadas, o meio militar (Mainwaring, 2020).

Com essa alteração no pensamento dos mais diferentes atores, tornou-se necessário que os Estados adotassem políticas que garantissem a proteção à soberania nacional e às suas infraestruturas críticas. Para que as nações conseguissem estabelecer suas operações em infraestruturas críticas, foi necessário que elaborassem conceitos para suprir os sistemas a serem atendidos. A primeira definição de infraestrutura crítica é datada de 2001, pelo Congresso Nacional dos Estados Unidos (GALLAIS; FILIOL, 2017). Em uma versão atualizada de 2019 do U.S. Department of Homeland Security, define-se que:

> a infraestrutura crítica inclui os ativos, sistemas, instalações, redes e outros elementos dos quais a sociedade depende para manter a segurança nacional, a vitalidade econômica e a saúde e segurança públicas. Conhecemos a infraestrutura crítica como a energia usada nas casas, a água que bebemos, o transporte que nos movimenta, as lojas onde fazemos compras e a Internet e as comunicações em que confiamos para manter nosso contato com amigos, família e colegas. Nos Estados Unidos, esta infraestrutura física e cibernética é tipicamente de propriedade e operada pelo setor privado, embora algumas sejam de propriedade de governos federais, estaduais ou locais. Nem toda infraestrutura dentro de um setor industrial é crítica para uma nação ou região. É necessário identificar qual infraestrutura é tanto crítica para manter serviços ou funções contínuas quanto vulnerável

[23] Traduzido de: [...] cyberspace became understood as a place in which authority, boundaries, and geography were weak or even did not apply (Mainwaring, 2020, p. 1).

> a algum tipo de ameaça ou perigo. Priorizando a alocação de recursos disponíveis para que um subconjunto de infraestrutura pode melhorar a segurança, aumentar a resiliência e reduzir os riscos (U.S. Department of Homeland Security, 2019, p. 4).[24]

Esse tipo de ação existe em quase todos os países do globo, tanto nas grandes potências quanto nas pequenas economias, o que aponta o quão importante a segurança cibernética se tornou na atualidade (Gallais; Filiol, 2017).

Cada país é responsável por definir os setores críticos de sua sociedade. Em 2007, a OTAN (Organização do Tratado do Atlântico Norte), reconheceu que não existe um conceito amplamente aceito pelas nações e que isso depende daquilo que é mais relevante para cada uma delas. Brevemente, dentro disso, há dois outros conceitos, o de infraestrutura crítica e de infraestrutura básica, que se diferenciam pelo dano, transtorno e destruição causados quando são atingidos. Além disso, alguns setores são mais úteis e importantes para a vida da sociedade do que outros, e trazem mais riscos a vida caso sejam atingidos, caso do setor elétrico. Quando são atingidos, os danos causados são identificados mais rapidamente do que as consequências de transtornos gerados a infraestruturas básicas (Gallais; Filiol, 2017).

Uma das maneiras de causar danos a infraestruturas críticas através da internet é por meio de ataques Denial of Service (DoS),

> Uma Denial of Service (DoS) é uma tentativa intencional por parte de usuários/atacantes maliciosos de interromper ou degradar completamente (comprometer) a disponibilidade de serviço/recursos para usuários legítimos/autorizados [...] Os ataques DoS exploram fraquezas nos protocolos de internet, aplicações, sistemas operacionais e implementação de protótipos em sistemas operacionais. Os ataques de Distributed Denial of Service (DDoS) degradam ou interrompem completamente os serviços para usuários legítimos, gastando comunicação e/ou recursos computacionais do alvo (Sachdeva *et al.*, 2010, p. 14).[25]

---

[24] Traduzido de: Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. We know critical infrastructure as the power used in homes, the water we drink, the transportation that moves us, the stores where we shop, and the Internet and communications we rely on to maintain our contact with friends, family, and colleagues. In the U.S., this physical and cyber infrastructure is typically owned and operated by the private sector, though some is owned by federal, state, or local governments. Not all infrastructure within an industry sector is critical to a nation or region. It is necessary to identify which infrastructure is both critical to maintain continued services or functions and vulnerable to some type of threat or hazard. Prioritizing the allocation of available resources to that subset of infrastructure can enhance a nation's security, increase resiliency, and reduce risk (U.S. Department of Homeland Security, 2019, p. 4).

[25] Traduzido de: A Denial os Service (DoS) is such an intentional attempt by maliciious users/attackers to completely disrupt or degrade (compromise) availability of service/resource to legitimate/authorized users [...] DoS attacks exploit weaknesses in internet protocols, applications, operating systems, and protocl implementation in operating systems (Sachdeva *et al.*, 2010, p. 14).

Para contê-los, medidas preventivas devem ser tomadas. Essas ações são onerosas e não podem ser deixadas de lado por parte dos Estados, pois os problemas gerados por ataques do tipo podem afetar setores estratégicos e causar grande desgaste político. Assim, devem ser considerados quais são os custos para a implantação de sistemas de segurança cibernética; quais são as medidas cabíveis perante os potenciais ameaças; e como reagir a ocorrência de um ataque cibernético. Isso mostra que, para além da dimensão militar do ciberespaço, há outros domínios que devem ser levados em consideração nas tratativas dessa temática para que todos os processos não fiquem restritos a um setor, quando na verdade ele está relacionado a todo o aparelho estatal (Górka, 2021).

Os ataques DoS[26] são conhecidos desde os anos 1980 e são responsáveis por causar quedas em sites devido ao alto tráfego gerado. À medida que a internet se torna o principal meio de conduzir a vida, os negócios e a economia, os avanços tecnológicos resultam em um aumento exponencial no uso da rede. Nesse contexto, os ataques DoS podem prejudicar significativamente o uso da internet. Embora não sejam capazes de destruir completamente os dados de usuários, empresas ou organizações, esses ataques podem ser onerosos em termos de tempo e dinheiro. O avanço da proteção contra os ataques DoS permitiu que esses ataques também progredissem. Em outras palavras, os ataques DoS envolvem uma ação coordenada contra um ou mais alvos, utilizando abordagens sofisticadas para sobrecarregá-los com um volume considerável de tráfego, ameaçando a estabilidade da rede. Embora seja comumente associado a hackers, esse tipo de ataque também pode ser realizado por outros atores, visando objetivos políticos ou financeiros. Portanto, grandes empresas e governos fazem altos investimentos na área de tecnologia da informação (TI), pois um único ataque DoS pode resultar em prejuízos devastadores, superando os custos de implementar medidas de defesa contra eles (Sachdeva *et al*., 2010; Gordon, 2017).

Em uma outra perspectiva, pode se dizer que, assim como o espaço físico e geográfico possuem limitações, quando se trata de um contexto de conflito, o espaço

[26] Distribute Denial of Service (DDoS) attacks degrade or completely disrupt services to legitimate users by expending communication and/or computational resources of target.

cibernético esbarra em alguns obstáculos, dado as múltiplas possibilidades oferecidas pelo ciberespaço quando se calcula:

Quadro 2: Cálculo do resultado de operações no espaço cibernético

Quantidade de pessoas atingidas por uma informação x Tempo

Fonte: Shallcross, 2017; Elaboração Própria

O tempo, que é o principal recurso, pode ser limitado para determinada operação, assim como uma determinada quantidade de armamento pode não ser suficiente para uma batalha. Diante disso, a coordenação de movimentações em conflitos deve se concentrar em pontos decisivos para atacar o adversário, reforçar as próprias vulnerabilidades e ter a possibilidade de contra-atacar caso seja descoberto (Shallcross, 2017).

Uma das estratégias para atingir pessoas na internet é por meio das mídias ou redes sociais. O que muitas vezes não é levado em consideração é que os riscos à segurança aumentam devido ao próprio ciclo das informações difundidas nos websites; ou seja, quando alguém compartilha um dado, isso gera vulnerabilidades. Por essa razão, quando se trata de informações estratégicas da segurança cibernética, as redes sociais devem ser incluídas no planejamento operacional de qualquer estratégia de comunicação. Isso implica que, ao movimentar-se no ciberespaço com informações sensíveis, é necessário prevenir-se quanto ao risco de ataque. Dessa forma, é essencial que os governos utilizem seu poder nacional para mobilizar recursos contra adversários, desenvolvendo uma estratégia cibernética relevante para o país (Shallcross, 2017).

A partir disso, torna-se evidente que os conflitos políticos e militares agora incluem perspectivas cibernéticas. Mesmo que seja apenas por meio de campanhas políticas e propaganda, sempre haverá algum aspecto relacionado ao ciberespaço. A globalização tem sido uma peça-chave nesse cenário, e a internet auxilia nos sistemas de comunicação, financiamento, relações públicas, coleta de dados e privacidade, influenciados pelas tecnologias que afetam até mesmo os serviços de inteligência. Nesse contexto, Estados, governos e algumas empresas da iniciativa privada desempenham papéis e têm responsabilidades específicas na proteção das infraestruturas ligadas à informação. Essas funções são essenciais para garantir a

manutenção e integração dos sistemas, além do desenvolvimento, pesquisa, produção e comércio de produtos relacionados à rede. Portanto, considerando o envolvimento de diferentes atores, é crucial que os atores estatais compreendam a dimensão política do ciberespaço e os processos que podem conduzi-los a alcançar objetivos políticos ou sociais (Geers, 2009; Tsakanyan, 2017).

Nos EUA, a Tecnologia da Informação e Comunicação (TIC) é a referência dos sistemas baseados em rede do país. As operações cibernéticas do Departamento de Defesa se relacionam com as TICs que reúnem todas as tecnologias referentes a telecomunicações, mídias, sistemas de gerenciamento, processamento, transmissão, controle e monitoramento de dados. Isso fornece insumo suficiente para as ações militares do país, que agem atualmente com base em informações e comunicação. Por essa razão, as pesquisas devem focar nos conceitos aplicados nos estudos de ciências política, segurança e inteligência para realizar análises eficazes sobre o setor relativo aos serviços de segurança e inteligência (Crowther, 2017; Górka, 2021).

Enquanto isso, estudos críticos afirmam que, apesar do papel político e midiático do ciberespaço, o pensamento sobre segurança cibernética ainda está em estágio inicial. Os estudos sobre esse ambiente estão relacionados à teoria da securitização, estabelecendo uma conexão entre segurança cibernética e segurança nacional, o que coloca em destaque atores predominantemente nacionais, apesar da ampla variedade de outros envolvidos no ciberespaço. Devido às divergências e concordâncias dentro desse campo, assim como em outros, é imperativo que continue sendo objeto de estudos, pois há muitos avanços a serem explorados (Liebetrau; Christensen, 2020).

No campo prático, os Estados têm utilizado cada vez mais recursos do espaço cibernético, tanto para interesses políticos quanto para a área da segurança. Assim, o contexto cibernético proporciona novos recursos e capacidades para os Estados. Além das atuações diplomáticas, políticas, militares e outras responsabilidades estatais e governamentais, as nações agora estão presentes em outro domínio: o ciberespaço. Diante desse cenário e da diversidade entre atores e objetivos que operam nesse espaço, o combate às ameaças envolve uma série de agentes públicos e privados, assim como toda a sociedade. Essa conjuntura destaca a segurança cibernética como um aspecto essencial na política e nas relações internacionais do século XXI (Whyte, 2020; Tsakanyan, 2017).

O conceito de poder é compreendido de diferentes formas, e a interpretação do termo varia dependendo da vertente seguida. No construtivismo, um ponto comum na abordagem dos autores é que o poder é uma construção, ou seja, é constituído e atribuído a recursos, sejam militares, econômicos ou políticos, que influenciam na diplomacia, proporcionando maior poder de barganha. Nesse contexto, o poder é superior para o Estado que consegue criar uma identidade e moldar seus interesses da melhor forma diante das condições fornecidas pelo sistema internacional. Isso significa que o poder existe na construção social e na estrutura existente, e o Estado tem domínio sobre o contexto presente (Santos, 2017).

A percepção do outro no sistema internacional desempenha um papel determinante. As interações entre atores dependem da maneira como observam o comportamento uns dos outros. Para que uma interação conduza a uma nova relação ou aliança, são necessários processos e a expectativa de determinados comportamentos. O reconhecimento de um ator como amigo, inimigo, rival ou irrelevante colabora para a construção de interesses. Sob a perspectiva construtivista, a constituição de relações depende do discurso, da persuasão e da identidade. Em resumo, é crucial que os Estados compreendam os rumos políticos de suas interações; portanto, medidas de observação, estudo e acompanhamento dos atores de interesse são relevantes (Green; Bogard, 2012).

O poder cibernético é definido a partir de múltiplos elementos. A presença da tecnologia eleva a complexidade da definição do poder; e a capacidade de uso de ferramentas de informática também faz parte da construção do poder neste espaço.

> O comportamento do poder cibernético se baseia em uma série de recursos relacionados como a criação, o controle e a comunicação dos eletrônicos e computadores baseados na informação, infraestrutura, redes, softwares e habilidades humanas [...]. Definido comportamentalmente, poder cibernético é a habilidade de se obter melhores resultados através do uso de recursos de informação eletronicamente interconectados do domínio ciber. (Nye Jr., 2010, p. 2-3, tradução própria).

Com base nisso, o comportamento dos atores é resultado de um conjunto de elementos que integram o contexto em que eles estão submetidos (Nye Jr, 2010).

O poder cibernético, como instrumento de poder, cria vantagens e influência movimentos no ciberespaço. É essencial considerar não apenas o conceito de poder cibernético, mas também outras formas de poder e suas interações com a estrutura estatais. O construtivismo é uma das teorias capazes de fazer análises que aglutinam

o debate entre o poder cibernético e as relações poder entre os Estados. Compreender a dinâmica do poder cibernético requer uma compreensão de como a concepção de poder surgiu e foi disseminada pelos atores do sistema internacional. Portanto, é importante investigar os processos e as circunstâncias nas quais o Estado, o principal objeto deste estudo, se posiciona na construção social (Kuehl, 2009).

Geograficamente, o ciberespaço ultrapassa os limites das fronteiras. As conexões estabelecidas pelas redes e sistemas de informação são instituições próprias que podem ocupar o espaço físico e virtual. Diferentes indivíduos, com diversos objetivos, utilizam ferramentas tecnológicas para realizar suas atividades. A conectividade, nesse cenário, depende das plataformas físicas, ou seja, sistemas de infraestrutura que possibilitam a conexão global das redes, computadores e usuários; além das informações presentes nesse ambiente, que permitem que esses conteúdos sejam acessados em qualquer hora e lugar. Isso quer dizer que, a depender de como o ciberespaço é utilizado, ele pode afetar e impactar outros espaços e elementos da realidade (Kuehl, 2009).

O ciberespaço favorece o uso e a exploração da informação. Ele foi projetado e criado com o propósito de acelerar o fluxo das informações. As interações e comunicações que ocorrem nesse espaço permitem a conexão e o acesso de indivíduos e instituições, possibilitando que conduzam suas atividades cotidianas e alcancem grandes impactos com base em suas ações, conferindo-lhes papel de poder. Pode-se considerar o ciberespaço como um domínio para além dos territórios terrestre, marítimo, aéreo e espacial, pois nele também operam os elementos de poder. Assim, é possível envolver a influência estatal, seja direcionada a indivíduos, organizações ou outros Estados. Em resumo, nesse espaço, é viável estabelecer estratégias de influência, de maneira semelhante à esfera física (Kuehl, 2009).

O ciberespaço faz parte da estratégia dos Estados. O sistema internacional passou a contar cada vez mais com as regras do espaço cibernético para tratar das questões cotidianas. Os processos tradicionais das transações das relações internacionais, foram começando a ser debatidos em sua lógica operacional e repensados sob a perspectiva das relações estatais e do poder cibernético. No trecho a seguir é possível observar um exemplo de como essas mudanças foram acontecendo ao longo do tempo.

> O mercado usa o ciberespaço para facilitar o comércio global, intercambiar fundos, gerenciar empresas distantes, e realizar outras inúmeras atividades vitais. Na realidade, o ciberespaço é onde criamos e usamos a informação digital que roda a economia global. Todos os dias, a comunidade dos negócios globais troca trilhões de dólares via ciberespaço, transações nas quais nenhum centavo de moeda física é movido. O estrategista político não pode ignorar o ciberespaço, porque a efetividade de seu uso pode significar a diferença entre uma vitória e uma derrota no processo eleitoral (Kuehl, 2009, p. 29, tradução própria).[27]

Desta forma, a habilidade de desenvolver estratégias cibernéticas que apoiam a proteção contra os potenciais riscos oferecidos pelas capacidades oferecidas pelas vulnerabilidades advindas do ciberespaço (Kuehl, 2009).

Os primeiros domínios em que o poder foi reproduzido foram a terra e o mar. Há um século, o desenvolvimento tecnológico permitiu o acesso a um novo ambiente, o aeroespacial, que trouxe mudanças militares e comerciais para os Estados. Primeiro, houve o domínio do ar e, em 1957, apesar de ainda não ter uso comercial e militar, iniciou-se o uso do espaço como recurso essencial para o desenvolvimento e as conexões dos outros ambientes. Aos quatro ambientes já conhecidos, adicionou-se nos últimos anos o quinto ambiente, o ciberespaço. A partir desse momento, os Estados passaram a desenvolver habilidades estratégicas para atuação no ciberespaço com o objetivo de garantir a segurança nacional (Kuehl, 2009).

O controle e monitoramento de ameaças são algumas das preocupações dos Estados. O contexto do ciberespaço submeteu os atores estatais a circunstâncias que os fazem assumir a responsabilidade por melhorias em seu desenvolvimento técnico e tecnológico. Essas ações visam evitar perdas significativas de poder relacionadas ao uso de tecnologias. Uma situação em que ocorram danos ou prejuízos em termos de poder pode criar um distanciamento entre o controle do mundo físico e virtual. Isso gera vulnerabilidades para os governos, pois há mais recursos disponíveis no ciberespaço do que o Estado consegue controlar. Por essa razão, para além da ausência de fronteiras e da ideia de liberdade intrínsecas ao ciberespaço, há uma realidade que dispensa normas e regras, podendo ceder espaço ao crime - desde invasões a computadores individuais até a espionagem e roubo de informações

[27] Traduzido de: The business community uses cyberspace to facilitate global trade, exchange funds, manage far-flung enterprises, and do innumerable other vital things. In a real sense, cyberspace is where we create and use the digital information that fuels the global economy. Every day, the global business community exchanges trillions of dollars via cyberspace, transactions in which not a single dime or euro of hard currency is moved. The political strategist cannot ignore cyberspace, because its effective use may well mean the difference between victory and defeat in the electoral process (Kuehl, 2009, p. 29).

governamentais. Assim, a integração da internet a nível global representa um dos maiores desafios para a soberania estatal, uma vez que a dissociação entre o Estado e a internet se torna mais complexa (Martins, 2012).

Tim Jordan (1999) analisa três teorias de poder para compreender o poder cibernético. A teoria desenhada por Max Weber entende que o poder é intencional, pois em algum momento uma ação precisa ser realizada e, então, o poder influenciará algo. Nesse sentido, o poder é posse; se um ator tem o poder, ele pode agir conforme o que possui, caso seja necessário. Logo, pode-se entender que o poder é conhecido pelos efeitos que o ator que o possui pode causar aos demais, como uma força que rege a obrigação da realização de ações por outros atores. Assim, o detentor do poder tem a capacidade de estrategicamente estabelecer uma relação de dominado e dominador (Jordan, 1999).

Para Barry Barnes, o poder surge do senso comum. Em sua concepção, o poder advém da estrutura construída a partir da identidade coletiva e é validado por meio de cada indivíduo, sendo traduzido a partir do pensamento do grupo, ou seja, a sociedade. O poder também pode ser a posse de indivíduos ou objetos. Isso é determinado pela maneira como a ordem social é estabelecida e pela distribuição de poder em uma sociedade, o que está diretamente ligado ao conhecimento e às capacidades individuais que refletem na criação da consciência da sociedade. Em resumo, o poder que está na estrutura é moldado a partir da identidade coletiva construído por cada indivíduo que compõe a sociedade (Jordan, 1999).

Michel Foucault lê o poder como uma forma de dominação. Na interpretação feita por Jordan (1999) desse autor, o pensamento deriva da ideia de que o poder é uma força que gera desigualdade entre os indivíduos. Para ele, o poder não pode ser posse, uma vez que é resultado da relação entre as pessoas. A denominação sugerida por Foucault tem efeitos sobre o dominado e o dominador, e o poder que enxergamos na esfera estatal, por exemplo, é advindo de micro relações de poder que sustentam o exercício do poder e dominação dos Estados. Dentro do poder estatal, é possível que existam diferentes tipos de dominação, gerando uma infinidade de posições a serem ocupadas na elaboração das estratégias de poder. Isso acontece pela manutenção da viabilidade de interações e estratégias. Sendo assim, poder é fonte de repressão e de produção, e a resistência é essencial para que a relação de poder seja firmada (Jordan, 1999).

3 TEORIA CONSTRUTIVISTA, TEORIA REALISTA E OS ELEMENTOS QUE MOTIVAM POLÍTICAS QUE REFORÇAM A SEGURANÇA ESTATAL

3.1 TEORIA CONSTRUTIVISTA E A CONTRIBUIÇÃO DO CONCEITO DE IDENTIDADE PARA AS RELAÇÕES INTERNACIONAIS E O CIBERESPAÇO

A construção social dos Estados é a integração entre identidade das unidades estatais e os seus interesses. Uma das abordagens que explicam essa ideia é o construtivismo, teoria do sistema internacional que se desenvolve e se fundamenta com os seguintes elementos:

> (1) os estados são as principais unidades de análise para teoria política; (2) as principais estruturas do sistema estatal são intersubjetivas, e não materiais; e (3) as identidades e interesses estatais são em parte importante construídas por essas estruturas sociais, em vez de dar exogenamente ao sistema por natureza humana ou política doméstica (Wendt, 1994, p. 385).[28]

A teoria construtivista estuda a construção da sociedade por meio das relações sociais. Os arranjos sociais, as regras e as dinâmicas de poder surgem como resultados de um processo duplo: pessoas construindo a sociedade e a sociedade construindo as pessoas. Criada no final dos anos 1980 por Nicholas Onuf, a teoria construtivista afirma que os seres humanos são essencialmente sociais e que são as relações sociais que os constroem. Segundo o construtivismo, o ato da constituição social é responsável pela existência da história. Sendo assim, a realidade social é aquilo que as pessoas consideram possível, e a sociedade torna possível na prática, havendo uma relação com a identificação individual que converge na coletividade (Onuf, 1989).

Adler (1999) teoriza o construtivismo como “o modo pelo qual o mundo material forma a, formado pela ação e interação humana, e depende de interpretações normativas epistêmicas dinâmicas do mundo material” (Adler, 1999, p. 205). Por esse ponto de vista, as instituições são baseadas na coletividade. É essa consciência coletiva humana que impacta na maneira como os indivíduos e atores sociais entendem o campo material e percebem e a realidade que as cerca.

---

[28] Traduzido de: (1) states are the principal units of analysis for inter-national political theory; (2) the key structures in the states system are intersubjective, rather than mate-rial; and (3) state identities and interests are in im-portant part constructed by these social structures, rather than given exogenously to the system by human nature or domestic politics (Wendt, 1994, p. 385).

Estruturas são reproduzidas ou transformadas pelo contexto prático. Uma dada circunstância pode facilitar ou inibir a formação da identidade coletiva, pois essa identidade possui uma base passível de movimento. Em outras palavras, os processos intrínsecos ao sistema internacional estão fora do controle isolado de um Estado, devido ao fato das nações coexistirem em um espaço e interagirem umas com as outras. Diante dessa perspectiva, para Wendt (1994), há alguns caminhos para solucionar problemas relativos à maneira como a comunidade internacional observa os componentes que constroem a identidade de um Estado. O primeiro é o processo de interdependência, onde há maior interação entre as unidades estatais como, por exemplo, no comércio, o que demanda uma necessidade maior de acompanhar o fluxo da atuação dos Estados à nível internacional. O segundo fator é a existência do outro; para a manutenção da política do Estado, é necessário manter um equilíbrio entre os interesses dos Estados, criando dilemas de interesses comuns que geram ameaças e a sensação de vulnerabilidade de um ator em relação ao outro. Após descrever essas formas de interdependência, Wendt (1994) argumenta que elas se tornam determinantes, constatando que os sistemas são socialmente construídos e dependem do interesse e da identidade que está no tecido ou na essência de cada Estado (Wendt, 1994).

Os Estados se adaptam a mudanças. Quando surgem alterações no cenário internacional capazes de causar desarranjos políticos em determinada sociedade, os atores estatais precisam se readequar, estabelecer alianças e redefinir sua própria identidade e interesses. Em situações que demandam interação entre os Estados, há incentivos para uma maior interdependência, e esses momentos são acompanhados por métodos de identidade coletiva. Ao mesmo tempo, esse cenário de interdependência pode gerar a sensação de vulnerabilidade. Para responder às ameaças criadas pelos processos do próprio sistema de interdependência, os Estados podem decidir agir unilateralmente e adotar identidades egoístas e autocentrados em momentos oportunos. Isso mostra que a dependência que um Estado possui no sistema é que molda a identidade de um ator para a sua interação (Wendt, 1994).

Existem críticas à concepção de que a ordem internacional é um pensamento simples. Autores institucionalistas, por exemplo, defendem a ideia de que o mundo interdependente e interconectado não significa mudanças políticas automáticas. Para os teóricos construtivistas das relações internacionais, também não é possível que a

evolução da interação entre os países seja estudada por meio de entendimentos básicos sobre intencionalidade. Isso pode ser explicado pela existência de uma série de variáveis que alteram a política internacional e que se adaptam a cada realidade, deixando claro que as relações estão em transformação. Esses fatores podem ser criados por pessoas, grupos políticos, organizações e instituições, conduzindo a maneira como um Estado pode agir mediante a diferentes contextos no sistema. Assim, as ações estatais são adaptadas localmente e estão em busca de contemplar todas as identidades pertencentes aos espaços de influências da nação (March; Olsen, 1998).

O arranjo político de um Estado é um movimento constante. Algumas mudanças da ordem internacional acontecem de maneira rápida. Isso mostra que a constituição dos países no formato em que estão hoje é passível de mudança. Essa afirmação pôde ser observada no Tratado de Vestfália, em que houve transformações significativas no cenário internacional, a partir de movimentos estatais. Alguns exemplos disso são separações e fusões entre Estados, que alteraram fronteiras e a própria constituição de territórios e fronteira, além da política das regiões envolvidas nessas movimentações. Esse cenário indica que os Estados podem se transformar a todo momento (March; Olsen, 1998).

Finnemore (2001), observa criticamente a teoria construtivista. A autora afirma que os maiores pensamentos em torno do construtivismo, incluindo os textos de Wendt “Anarchy is what the states make of it” de 1992, ”Collective identity formation and the international state” de 1994 e Katzenstein “The culture os national security norms and identity in world politics” e ”Cultural norms and national security police and military in post-war Japan” de 1996, se baseiam na ideia de que é a identidade de um Estado que materializa características centrais para a formação de tendências que coordenam as ações de uma unidade estatal. A teórica afirma que a construção da identidade reflete a sociedade na dimensão da política interna e externa dos Estado e, ao mesmo tempo, discorda dos conceitos de identidade e da ênfase dada a nível nacional e internacional na formação de tal definição. Enquanto o pensamento de Wendt se constitui a partir de uma visão do sistema internacional, Katzenstein observa que a política interna é o que tem mais peso sobre a identidade. Assim, Finnemore (2001) mostra que o construtivismo é uma teoria que está em constante discussão (Finnemore, 2001).

O construtivismo explora as escolhas racionais dos Estados. Um dos objetivos dessa abordagem é compreender como os agentes que moldam a política e os próprios Estados interagem na busca pela otimização de esforços na construção de sua identidade. Essa perspectiva está intrinsicamente ligada à estrutura do pensamento construtivista, que organiza agentes e estrutura de forma interconectada. Ao contrário de teorias como o realismo, o construtivismo realiza análises abrangentes, considerando diferentes atores e contextos nos quais os Estados estão inseridos (Finnemore, 2001).

A definição da política internacional em termos de poder é uma característica distintiva da teoria realista das relações internacionais. Contudo, essa abordagem não é a única responsável pelos estudos que visam entender a política dos Estados com base em relações de poder. No construtivismo, o poder é considerado tanto em termos materiais quanto em relação aos interesses dos Estados. Wendt (1999) destaca que, enquanto o neorrealista Waltz enfoca a capacidade material na definição da estrutura internacional, o construtivismo abrange aspectos sociais que moldam a sociedade. Assim, os estudos teóricos de Waltz seguem um modelo de distribuição de poder baseado em interesses materiais, enquanto o construtivismo expande essa compreensão, incorporando elementos sociais (Wendt, 1999).

Wendt (1999) argumenta em favor da presença de ideias como moldadoras dos interesses estatais. Ele destaca a hipótese de que Waltz, de maneira implícita, recorre à distribuição de interesses e de poder, oriunda das capacidades materiais de um Estado no sistema internacional. Para Wendt, é crucial estabelecer uma interseção entre as motivações dos agentes, a estrutura e o processo que conecta todas essas variáveis na condição de anarquia. Além disso, torna-se relevante avaliar como os princípios estão organizados, especialmente se desempenham papéis igualitários ou de subordinação. Dessa forma, na teoria de Waltz, as unidades estatais são consideradas igualmente soberanas no âmbito internacional, e, no nível doméstico, as ações dos Estados são percebidas como homogêneas. Vale ressaltar que a análise realista das relações internacionais difere substancialmente da perspectiva construtivista (Wendt, 1999).

No construtivismo de Wendt, a estrutura se define a partir das ideias. Assim, essa teoria afirma que existe um modelo de estrutura ideacional e que, a partir disso, os atores constroem seu comportamento e interesse no sistema internacional. As

ideias que moldam os Estados se estabelecem pela sociedade como um todo e, conforme acontece esse movimento, são constituídos as identidades e os interesses. Dessa forma, a construção social pode ser entendida como estrutura formada a partir de ideias compartilhadas por atores do sistema que, se pensadas ou tomadas de forma homogênea, podem gerar estabilidade e possibilitar previsões sobre as ações desses atores. Com base nisso, pode-se dizer que as estruturas sociais que configuram interesses, ações e preferências dos Estados dependem do comportamento dos governos, agentes, preceitos e motivações. Ou seja, são as ideias compartilhadas que guiam os interesses e ações dos Estados (Wendt, 1999).

As identidades existem e são importantes para os Estados pois firmam previsibilidade e ordenamento para as atividades desses atores. Existem alguns padrões seguidos pelos atores no sistema internacional e esses, por sua vez, são institucionalizados. Como são os Estados que constituem as instituições e não o contrário, as ideias existentes dentro desses espaços é formada pelos atores que fazem parte do ambiente. Isso significa que, ao considerar que as instituições possuem um papel importante no sistema internacional, os atores compartilham ideias e transmitem as suas ações através dessa instância (Nogueira, 2011).

Todos os elementos que compõe a política dos Estados são considerados na construção da identidade de estrutura. Isso pode ser observado na teoria construtivista quando,

> Wendt (1999) conclui que a identidade estatal, ou seja, aquilo que diz ao estado o que ele é, quem são os outros estados e qual é o seu papel em determinada situação, emerge de sua interação com os outros Estados. Através da repetição, as identidades geram compartilhamento de ideias e conhecimentos que permitem aos Estados se entenderem e agirem na consecução de seus objetivos. Reconceituando a ideia de sistema internacional, Wendt (1999) apresenta uma compreensão que nega que a distribuição horizontal de poder necessariamente sugere competição entre os Estados (Nogueira, 2011).

Isso mostra que a teoria construtivista realiza análises que buscam compreender a realidade estatal a partir do comportamento dos atores que compõe o sistema internacional (Nogueira, 2011).

As políticas de segurança de um Estado são intrinsecamente ligadas à cultura, um elemento constituinte que reflete na formação da identidade nacional. Essa identidade não apenas legitima as práticas do Estado, mas também reforça sua

autoridade, consolidando-o como um ator soberano no sistema internacional. A interconexão entre cultura, identidade e autoridade estatal estabelece a base para a compreensão da relação entre identidade e interesses. Essa inter-relação é essencial para a análise das dinâmicas da política internacional em nível sistêmico. No contexto da segurança estatal, surgem planos coletivos que se viabilizam pelas relações entre os Estados e pelas metas construídas em conjunto (Nogueira, 2011).

Essa identificação entre os Estados do sistema internacional refere-se à identidade construída entre os comportamentos e interesses. Dentro desse contexto, os atores estatais têm a capacidade de delinear opções de plano de ação, proporcionando uma compreensão de como suas atividades influenciam o coletivo. O construtivismo, ao abordar tópicos de segurança, argumenta que a estrutura influência o modo de operar dos atores. Nesse cenário, a configuração e identidade de um ator, em relação a outros atores e à política interna, desempenham papéis cruciais. Isso ressalta a importância de examinar os atores sociais proeminentes em uma sociedade para a análise do comportamento resultante da política e identidade estatal (Nogueira, 2011).

A anarquia é o que os Estados fazem dela. A partir do texto de Alexander Wendt de 1992, percebe-se que é na anarquia que os Estados encontram problemas na ação coletiva, pois é nela que cada Estado possui a possibilidade de uso da força para o garantir os seus próprios interesses. A anarquia é um conceito que traz a percepção do sistema internacional como um ambiente em que os Estados estariam em um local de autonomia estatal, onde podem projetar poder, por isso eles ficariam em constante competição, levando ao equilíbrio de poder (Wendt, 1992).

A estrutura, seja ela regional ou global, constitui as interações entre Estados. Cada vertente do pensamento político dos Estados compreende a anarquia de uma maneira diferente. Wendt (2003), ressalta que as estruturas intersubjetivas são os elementos constitutivos da anarquia, proporcionando a base para a formação da identidade coletiva em um sistema de Estados. Essa perspectiva implica em visões de mundo distintas quando consideramos as interpretações de Hobbes, Locke e Kant sobre o significado do Estado (Wendt, 2003).

Para Hobbes, em um sistema caracterizado pelo conflito e pelo temor mútuo entre Estados, a anarquia naturalmente conduz a identidades egoístas, com uma escassa ocorrência de identificação entre as unidades devido à constante ameaça de

guerra generalizada. Locke, por sua vez, sugere que, ao estabelecerem uma soberania mutuamente reconhecida e construir confiança, os Estados podem se engajar em processos de identificação. Isso acontece pois o Estado tem o direito de se defender, dado que a guerra existe. Na anarquia de Locke, ao mesmo tempo em que a guerra existe, há o entendimento de que ela pode prejudicar ou mesmo dizimar a existência dos Estados. Nesse sentido, para que os conflitos sejam evitados, faz-se a opção pelo equilíbrio de poder, visto o reconhecimento dos Estados como unidades soberanas que seguem normas e regras, criando respeito entre eles. Em contraste, a visão idealista de Kant sugere uma proximidade nas relações entre Estados, eliminando a possibilidade de guerra direta. Nessa visão, existe uma identificação e torna-se possível a ausência de conflitos na anarquia, sendo uma escolha realizada por parte dos Estados (Ayres Pinto, 2016).

Mesmo passado muitos anos, o formato do Estado pensado por Locke, amparado pelas regras e normas que garantem restrições quanto ao uso da força e violência estatal, advindo da concepção de Estado Moderno que se mantém hoje e que demonstra uma estrutura vigente de poder nas Relações Internacionais. O que se diferente da lógica kantiana, no qual o ambiente anárquico de Kant, a existência de atores dispostos a cooperação torna plausível a construção de um novo molde de poder, que amplia as relações entre atores, respeita mutuamente os interesses das partes e gera recompensas a todos (Wendt, 2003; Ayres Pinto, 2016).

No contexto do construtivismo de Wendt, os Estados assumem um papel central na anarquia internacional. O autor fundamenta seus argumentos na premissa de que os Estados são unidades autônomas no sistema internacional, organizados socialmente em comunidades políticas autônomas. A principal forma de interação nesse cenário é através dos grupos políticos, ou seja, os Estados. Wendt destaca que esses atores, conforme a definição de Weber, detêm o monopólio legítimo do uso da força, o que implica um potencial para empregar a violência na comunidade internacional quando necessário. Além disso, a legitimidade desempenha um papel crucial, ancorada na autoridade política coercitiva, onde a sociedade confere ao Estado a responsabilidade pela manutenção da ordem social (Wendt 2003; Wendt, 2013).

As análises de segurança podem se relacionar com as definições e conceitos do construtivismo. As condições em que os Estados estão imersos, tanto em termos

domésticos quanto internacionalmente, é um dos fatores que possibilita compreender as interações que um ator estatal tem no sistema internacional. A exemplo disso, a identidade é, por características, um dos pontos centrais no construtivismo, e ela define como os Estados observam, concentram seus interesses e comportamento em relação aos demais, se impondo politicamente. As práticas dos Estados como unidades soberanas é um processo construído socialmente e tem como base elites sociais que são mais influentes e capazes de moldar ideias em outros atores (Isnarti, 2016).

As unidades estatais podem ser aliadas ou inimigas de outros atores do sistema internacional. A constância, a necessidade e a efetividade dessas interações contribuem para a formação de normas ou padrões de legitimidade que orientam as ações dos Estados. São formadas redes que permitem o inter-relacionamento no sistema. Essas conexões são baseadas nos interesses construídos socialmente por atores que desempenham papéis significativos na política internacional, não deixando de considerar as definições domésticas dos países. Assim, a constituição e manutenção das normas refletem como os Estados conseguem modelar e remodelar seus interesses, adaptando-os de acordo com as circunstâncias. Essa adaptação é realizada por meio da comunicação e do estabelecimento de redes que permitem a interação no sistema conforme a identidade assimilada e posta em prática, com base no tipo de conexão estabelecida entre os atores. (Isnart, 2016).

A experiência que um Estado tem no sistema internacional influencia suas ações futuras. Isso acontece porque fatores culturais, resultantes das relações e da construção social da identidade de uma unidade estatal, influenciam nas ideias compartilhadas que moldam as interações de um país ao longo do tempo. A exemplo disso, a ideia de guerra cibernética pode ser analisada pela teoria construtivista através da vertente da construção social. A partir do momento em que as inovações tecnológicas avançaram e a internet protagoniza as redes e os meios de comunicação, o espaço cibernético e o conflito entre os Estados, a teoria construtivista passou a se atrelar a esse ambiente. Com isso as definições de segurança estudados nesse trabalho avançaram em diferentes correntes teóricas (Isnarti, 2016).

Os estudos em segurança internacional tradicionais passaram a considerar outros domínios. A esfera física: terra; mar; e ar; deixou de ser o único objeto de estudos sobre guerra, pois o espaço cibernético, ou o domínio virtual, tornou-se

virtualmente importante nas discussões sobre o tema. A partir do momento em que a internet começou a tomar espaço nas relações internacionais, os atores estatais começaram a se preocupar com as interações entre uns e outros para definir quais ações seriam razoáveis para não prejudicar as relações no sistema internacionais. Assim, as questões pertinentes a segurança mudou rumo ao ciberespaço (Isnarti,2016).

A identificação dos responsáveis por ataques cibernéticos assume um papel crucial na guerra cibernética. No ciberespaço, os Estados alvos categorizam os perpetradores como inimigos. Contudo, em muitos casos, intrusões ou ataques são executados por Estados cujas identidades guardam semelhanças com aquelas das nações que enfrentam as ameaças cibernéticas. Essa similaridade de identidades frequentemente resulta em interesses compartilhados, precipitando situações em que ocorrem ataques ou espionagem cibernética como meio de obter vantagens sobre outros Estados e atores. Tais incidentes emergem das percepções que os atores têm uns dos outros, frequentemente exacerbadas pela falta de interações substanciais sobre questões de segurança e pela escassez de compartilhamento de acordos e normas. Assim, alguns autores argumentam que, quanto maior a desconfiança entre Estados, maior a probabilidade de ataques à segurança, especialmente num mundo caracterizado por um desenvolvimento contínuo de tecnologias da informação, tornando os ataques cibernéticos uma ocorrência recorrente (Isnarti, 2016).

O construtivismo emerge como uma alternativa às correntes teóricas convencionais das relações internacionais no contexto do ciberespaço. Na análise proposta por Rika Isnardi (2016), o construtivismo é concebido como um arcabouço que permite explorar as ideias que delineiam o espaço cibernético, expandindo a compreensão do que tradicionalmente se considerava como segurança. Nessa perspectiva, é possível voltar os esforços para pesquisas que analisam como o novo domínio absorve as interações do sistema internacional, gerando respostas sobre os potenciais guerras entre Estados. Outras teorias, como o liberalismo e o neorrealismo, contribuem com argumentos valiosos para entender a guerra cibernética, enfatizando as práticas de instituições, iniciativas privadas e o papel central dos Estados nas relações internacionais. Contudo, essas teorias, por si só, não oferecem explicações robustas sobre como prevenir conflitos no ciberespaço. Nesse cenário, a construção da identidade estatal permanece um dos principais elementos para a interação entre

os Estados, fundamentada em interesses compartilhados, o que pode potencialmente gerar alianças e promover a paz no ciberespaço (Isnarti, 2016).

A construção da identidade é intrinsecamente ligada a ideias compartilhadas, um princípio que, em teoria, molda os espaços sociais permeados por uma diversidade de atores na sociedade. Essa dinâmica exerce influência tanto nas políticas domésticas quanto nas internacionais, dando origem a interações complexas, formação de alianças e criação de redes nas quais os Estados se comparam e se diferenciam, gerando um sentido de pertencimento. As particularidades dos Estados geram princípios que norteiam suas relações internas e externas, colocando-os em posições frente a inimigos e parceiros. Assim, a lógica da violência e conflito está relacionada com a maneira como o Estado quer ser visto no sistema internacional. Um exemplo ilustrativo desse fenômeno reside nas nações que são percebidas como securitizadas. Esses Estados empregam elementos discursivos e narrativas estratégicas alinhadas à mensagem que desejam comunicar a outros Estados, à sociedade civil e a instituições públicas ou privadas. Nesse contexto, no âmbito da segurança internacional, os atores estatais posicionam a identidade como um elemento central para orientar suas ações (Tulga, 2022).

As identidades estatais desempenham um papel crucial ao refletir o que um Estado representa e como percebe os outros atores na comunidade internacional. Essa perspectiva aborda a maneira como um ator estatal é visualizado globalmente e como ele identifica seus pares, resultando em um movimento compartilhado de construção de identidade. Alguns autores argumentam que as identidades, construídas socialmente, não derivam apenas dos eventos nacionais, mas são forjadas principalmente pela interação entre Estados, pelos pensamentos compartilhados e por meio de um processo político contínuo. Em consonância com os princípios do construtivismo, Fierk (2007) concebe a identidade estatal como um fenômeno fluido, sujeito a constantes transformações. Nesse contexto, à medida que a segurança permeia o ciberespaço, os Estados se deparam com situações que representam riscos quanto à sua percepção no ambiente digital, sentindo-se ameaçados pela presença e ações dos demais atores (Fierk, 2007; Tulga, 2022).

A teoria construtivista observa a construção social nas relações internacionais. A formação de ideias, protagonizada por atores, instituições e eventos no cenário global, é reflexo do pensamento e comportamento de pessoas e Estados na política

internacional. A partir da observação da própria identidade, ideias e crenças, o comportamento das unidades estatais é moldado. Dessa forma, as práticas e ações desdobram-se a partir da construção social interna, influenciando e sendo influenciadas pelo sistema internacional, sendo um conjunto de fatores que influenciam na identidade e interesses estatais (Hurd, 2008).

O construtivismo não rejeita as capacidades materiais. As potencialidades e o poder que uma nação possui é importante na formação das estratégias dos Estados. Os interesses têm como um dos componentes centrais o poderio instrumental, no entanto, isso não deve ser a ideia central para e existência e manutenção da atividade dos Estados. A inferência que fortalece o argumento construtivista é que os processos e interações sociais constroem o poder que as unidades estatais possuem e representam sua relevância nas relações internacionais. Assim, a construção social é responsável pela formação das características que constituem, por consequência, as ideias que os Estados disseminam por meio de ações (Hurd, 2008).

3.2 COMO OS CONCEITOS DA TEORIA REALISTA EXPLICA A INFLUÊNCIA DA GEOPOLÍTICA PARA O CIBERESPAÇO

A teoria realista, teoria de política internacional proposta por Waltz (1979), debate as causas sistêmicas da guerra. O objetivo dessa teoria é mostrar a dinâmica do sistema internacional a partir da interação entre níveis. Um sistema é definido como

> [...] um conjunto de unidades que interagem. Em um nível, um sistema consiste em uma estrutura, e a estrutura é o componente em nível de sistema que torna possível pensar nas unidades como formando um conjunto, diferente de uma mera coleção. Em outro nível, o sistema consiste em unidades que interagem (Waltz, 1979, p. 40).[29]

As unidades citadas no conceito de Waltz são os Estados, e o conjunto de interações dessas unidades forma o sistema internacional. Assim, a teoria sistêmica, como denominada pelo autor, será compreendida através dos elementos e análise realizada neste subtópico do capítulo.

[29] Traduzido de: A system is then defined as a set of interacting units. At one level, a system consists of a structure, and the structure is the systems-level component that makes it possible to think of the units as forming a set as distinct from a mere collection. At another level, the system consists of interacting units (Waltz, 1979, p. 40).

Três elementos fundamentais integram a estrutura, cada um desempenhando um papel crucial na definição dos efeitos e características dos Estados. A compreensão desses elementos, quando considerados de maneira isolada, é essencial para elucidar as dinâmicas do sistema. O primeiro desses elementos é o princípio ordenador, que pode se manifestar como anarquia ou hierarquia, delineando a natureza das relações entre os atores políticos na estrutura. Em seguida, temos o segundo elemento, relacionado à distribuição de funções nessa estrutura. Os atores no sistema internacional assumem especializações em funções específicas, contribuindo para a complexidade e interconexão do sistema. Na hierarquia, conceituada como,

> relações de super-e subordinação entre as partes de um sistema, o que implica em sua diferenciação. Ao definir a estrutura política interna, o segundo termo, assim como o primeiro e o terceiro, é necessário porque cada termo aponta para uma possível fonte de variação estrutural. Os estados que são as unidades dos sistemas políticos internacionais não são formalmente diferenciados pelas funções que desempenham (Waltz, 1979, p. 93).[30]

Isso o significa que é necessário atribuir de tarefas entres os Estados que formam o sistema, pois os atores podem presentes nesse espaço político tem diferentes papéis na estrutura — diferenciando-se da anarquia, em que as unidades são semelhantes e desempenham funções parecidas. Por fim, a distribuição de capacidades é relevante para os dois casos, anarquia e hierarquia. Isso determina a maneira como os Estados se posicionam em relação aos demais, visto que a posição relativa das unidades que fazem parte da estrutura é determinada pelas diferentes capacidades de cada Estado, mesmo que, no caso da anarquia, essas unidades possuam funções semelhantes (Waltz, 1979).

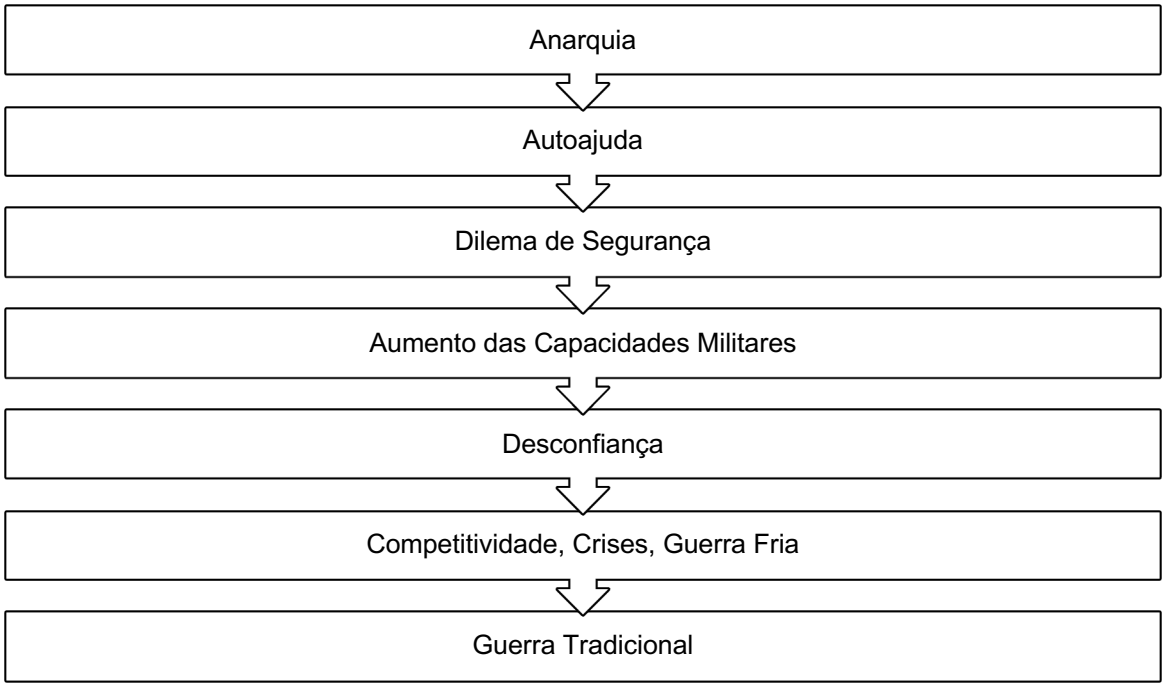
Os Estados buscam a sobrevivência. Os Estados se guiam pela ideia de que a melhor opção para firmar sua soberania é garantir aquilo que precisa pelos próprios meios, ou seja, capacidades, e depender daquilo que autogarante poder, sendo autossuficiente. Na anarquia, o sistema é guiado pela lógica da autoajuda. Não é possível prever se outra unidade poderá fornecer ajuda e salvaguarda. A autoajuda refere-se a todos os pontos que são relevantes ao Estado e, principalmente, à

[30] Traduzido de: super- and subordination among a system's parts, and that implies their differentiation. In defining domestic political structure the second term, like the first and third, is needed because each term points to a possible source of structural variation. The states that are the units of international-political systems are not formally differen tiated by the functions they perform (Waltz, 1979, p. 93).

sobrevivência. Isso ocorre para que um Estado não fique à mercê da ameaça de outro. Para garantir a sobrevivência e conter a ação de Estados que possam ter capacidades de ação mais imponentes, as unidades percebem a necessidade de manter o poder equilibrado. Assim, como não existem exércitos globais para os defender ou governos para fornecer essa proteção, os Estados utilizam façanhas que possibilitam o aumento de suas capacidades militares, o que gera, consequentemente, o dilema de segurança (Waltz, 1979).

O dilema de segurança surge a partir do mecanismo de autoajuda. Com o objetivo de aumentar e garantir a segurança estatal no sistema, atinge-se um cenário de insegurança no sistema internacional. Esse estado é gerado pela necessidade incessante de elevar o nível de segurança de um Estado, provocando a diminuição da margem de proteção de outra nação. O sentimento de insegurança gerado pelo sistema internacional anárquico e a criação de mecanismos de autoajuda aumentam a desconfiança. Com isso, o dilema de segurança torna o sistema competitivo e propenso ao conflito (Waltz, 1979). O fluxo desse processo pode ser desenhado da seguinte forma:

Figura 1: Fluxograma do Sistema Anárquico



Fonte: Waltz, 1979; Elaboração própria.

A segurança dos Estados depende do equilíbrio de poder. A diferença das capacidades entre os Estados provoca descontrole geral, e isso acontece porque o número de recursos disponíveis se difere em maior ou menor quantidade entre eles. Por essa razão, as unidades estatais estão em posições de poder diferentes. Em momentos em que há desequilíbrio, tanto os Estados considerados mais fracos quanto os mais fortes, podem ser prejudicados pelos que estão interessados em ampliar seu controle e projetar poder. Esses atores podem ser corajosos e destemidos. No entanto, o cenário ideal seria atingir a condição em que cada Estado conseguiria garantir a própria integridade. Logo, a falta do equilíbrio de poder gera instabilidade no sistema internacional (Waltz, 1979).

Ruohonen (2020) questiona a teoria do realismo estrutural de Waltz (1979) no contexto da segurança cibernética, destacando a dificuldade de controle das ações dos atores no ciberespaço. Sendo assim, em uma dimensão em que um Estado ou os Estados não estabelecem domínios concretos e não conseguem conjunta e individualmente elaborar regras bem definidas para as atividades que permeiam esse espaço, existe um grande desafio para a centralidade tradicional dos Estados. Enquanto faz essa observação sobre a estrutura, o autor levanta também o debate sobre o equilíbrio de poder. Em vez de adotar uma abordagem de confronto, Ruohonen propõe considerar resultados negativos como uma oportunidade para evitar conflitos, permitindo que os alvos de ataques cibernéticos busquem soluções alternativas (Ruohonen, 2020).

Os Estados, na estrutura internacional, apresentam desigualdades, impulsionadas pelos poderes hegemônicos que, mesmo sem um domínio permanente, geram competição entre eles. Na anarquia, a grande preocupação dos Estados é a sobrevivência, ameaçada pela competição que limita as unidades que aspiram alcançar a posição de grande potência. Para evitar a dominação por outros atores do sistema, os Estados projetam poder, ampliando suas capacidades e buscando autonomia. Assim, a razão para o equilíbrio de poder é reparar a distribuição de poder no sistema internacional (Layne, 1993).

A teoria neorrealista oferece explicações sobre o surgimento das grandes potências, sugerindo que a própria estrutura do sistema impulsiona esse fenômeno. Pressupõe-se que variações na quantidade de grandes potências provoca mudanças estruturais no sistema internacional, e os efeitos dessas mudanças geram a

alterações das unidades. Permite-se assim, a passagem da bipolaridade para unipolaridade ou multipolaridade, unipolaridade para bipolaridade ou multipolaridade, e multipolaridade para bipolaridade ou unipolaridade. A emergência de uma potência, assim como aconteceu pós Guerra Fria, tem um grande efeito estrutural. De forma geral, há um ciclo – limitações da estrutura pressionam os estados a se tornarem grandes potências, os estados precisam tomar decisões em nível de unidade para responder a essas restrições, essa busca por poder afeta a polaridade, impactando a estrutura (Layne, 1993).

A rivalidade entre Estados serve como estímulo à busca pelo poder. À medida que uma unidade política amplia sua influência, tornando-se mais ameaçadora, os Estados mais fracos tendem a se unir para contrabalançar o poder crescente. Contrariamente à expectativa de que a maximização do poder aumenta a segurança, Layne (1993) argumenta que, na realidade, ela resulta em diminuição da segurança. Esse cenário cria desequilíbrios, especialmente em um sistema unipolar, onde Estados buscam desenvolver suas capacidades relativas para evitar a exploração por uma potência hegemônica. Contudo, ter parte das capacidades da superpotência não garante segurança, e pode até expor um Estado de maneira mais significativa do que aqueles que optam por não possuir esses instrumentos no sistema de autoajuda (Layne, 1993).

O conflito entre Rússia e Ucrânia não se restringe apenas ao âmbito militar, estendendo-se à dimensão cibernética. Desde os ataques à Ucrânia em 2014, o governo russo tem sido acusado de invadir os sistemas conectados à rede de computadores do país. Em 2022, durante a invasão militar russa no território ucraniano, paralelamente, ocorreram significativas campanhas no ciberespaço. No início da guerra, em fevereiro de 2022, a Rússia, conforme informações de fontes públicas, realizou interferências nas redes conectadas da Ucrânia, buscando minar e sobrecarregar as defesas do país. Nesse contexto, foram executados ataques destinados a instalar malwares destrutivos, explorando as vulnerabilidades nos softwares ucranianos. Os principais alvos dessa ofensiva foram os sites governamentais, especialmente nos setores de energia e telecomunicações, evidenciando uma tentativa de atingir não apenas a infraestrutura crítica, mas também o sistema financeiro e os meios de comunicação (Lewis, 2022).

No ciberespaço, a Rússia enfrentou desafios significativos e não obteve ganhos militares expressivos durante o conflito com a Ucrânia. Os ataques cibernéticos elaborados antecipadamente pelos russos não resultaram no sucesso desejado, uma vez que a Ucrânia foi capaz de restabelecer suas conexões em um curto espaço de tempo, surpreendendo as estratégias russas. Este cenário destaca a importância da dinâmica estruturada e testada no ciberespaço para interferir efetivamente no campo de batalha do oponente e garantir vantagens informacionais. Para alcançar tais vantagens, campanhas de desinformação, ataques antissatélites e o uso de munições de alta precisão são ferramentas cruciais. Essas ações têm o propósito de prejudicar as comunicações adversárias, minando potenciais vantagens operacionais e, por conseguinte, informacionais (Lewis, 2022).

A Ucrânia demonstrou um significativo avanço na arena cibernética após os ataques ocorridos em 2014. Em busca de vantagens ofensivas em potenciais conflitos cibernéticos, o país implementou medidas proativas para proteger suas infraestruturas críticas e fortalecer a resiliência de suas redes contra invasões externas. Adotando uma estratégia abrangente de defesa cibernética, a Ucrânia estabeleceu parcerias sólidas com aliados internacionais e entidades privadas, fomentando relações cooperativas nesses setores. Essa abordagem defensiva permitiu que a Ucrânia se esquivasse de operações cibernéticas russas pós-2014 e enfrentasse os desafios de 2022 com uma preparação mais robusta (Lewis, 2022).

O poder de barganha desempenha um papel fundamental nas relações entre Estados, onde a disputa por recursos, opções políticas e a resolução de conflitos frequentemente gera discordâncias. De acordo com Reiter (2003), os estudos sobre guerras destacam que o poder de barganha é percebido como um processo dinâmico, comparável ao campo de batalha, em que os Estados veem seu poder se dissipar ao longo das negociações. Enquanto a guerra demanda recursos, o poder, durante o conflito, é um elemento negociável. No âmbito político, as interações entre nações ocorrem diariamente, e os Estados buscam os melhores acordos possíveis. Nesse contexto, as organizações internacionais desempenham um papel crucial, fortalecendo alianças e promovendo o comprometimento dos Estados envolvidos nas negociações. Dessa forma, o poder de barganha emerge como o principal determinante na definição dos resultados de uma negociação (Reiter, 2003).

Existem objetivos políticos por trás do conflito. Se não os houvesse, a guerra seria mera consumação de recursos. Nesse contexto, a guerra é compreendida como uma competição na qual os Estados buscam uma solução que traduza o melhor acordo possível, mesmo que para isso seja necessário arcar com os custos de um combate. O modelo que emprega a barganha como objeto de estudo também reconhece que, como consequência da guerra, pode-se alcançar estabilidade no período pós-conflito. Essa perspectiva argumenta que, durante a guerra, os Estados adquirem informações cruciais sobre o poder e as capacidades de seus oponentes. Esse conhecimento adquirido durante o conflito leva a um ajuste na distribuição de poder. Em outras palavras, à medida que mais conflitos ocorrem, mais informações são reveladas sobre o inimigo. Assim, a guerra não é apenas um meio de atingir objetivos políticos; também serve como uma estratégia para obter informações que podem contribuir para uma maior estabilidade no pós-conflito (Reiter, 2003).

A motivação desempenha um papel crucial na condução de conflitos armados. A guerra pode ser entendida como um conjunto de ações para alcançar objetivo político. Ou seja, ela é “um ato de força para obrigar o inimigo a fazer a nossa vontade” (Howard; Paret, p. 75, 1989). Isso significa que, ao entrar em batalha com o oponente, deve-se ter como foco deixá-lo sem ação, desarmá-lo e quebrar todas as suas defesas, de modo que ele não consiga mobilizar forças para um contra-ataque. No entanto, a guerra não consiste em um tipo ideal de conflito. Na realidade, ela possui contraste com as emoções humanas hostis e intenções hostis, afetando tanto os interesses quanto a duração do confronto. Por isso, para o emprego das forças, é necessário ter o propósito do conflito claramente definido (Howard; Paret, 1989).

Os Estados não estão preparados para as adversidades das tecnologias do século XXI. Eles estão preparados para conflitos convencionais, deixando uma lacuna substancial na abordagem de conflitos cibernéticos. Para definir o melhor plano de ação para o ciberespaço, é necessário compreender a melhor forma de empregar os recursos estratégicos inicialmente concebidos para o domínio cinético. Para aplicar as capacidades estatais ao âmbito cibernético, é necessário construir uma estratégia específica para esse novo cenário de defesa, no qual as ações preventivas são a melhor forma de evitar a possibilidade de ataques (Ecke, 2018).

A segurança no ciberespaço deve ser uma preocupação prioritária para os atores estatais. As novas estratégias nacionais devem reconhecer que os sistemas

cibernéticos, tais como existem hoje, são incapazes de manter-se completamente protegidos. Nos sistemas existentes atualmente, o ataque sempre consegue vencer a defesa, pois há uma assimetria que favorece o ataque. Essa assimetria existe pois, no ciberespaço, o custo de um ataque é baixo e a defesa não consegue contra-atacar causando os mesmos danos que o acometeram. O Estado que ataca acaba causando danos desproporcionais ao oponente, gerando consequências significantes. Assim, diferenciando-se dos conflitos tradicionais, é necessário um grande ato para conseguir excelentes resultados. Diante disso, torna-se necessário que a segurança estatal consiga explorar o domínio cibernético para não deixar que as lacunas e vulnerabilidades facilitem potenciais ataques (Ecke, 2018).

O uso do espaço cibernético exerce profundos reflexos na sociedade contemporânea. A capacidade dos atores tem sido alterada com a conexão ao ciberespaço. Estima-se que cerca de 75% da população mundial tem acesso a um aparelho celular e que aproximadamente 2,7 bilhões de pessoas estão conectadas à internet. Esses números evidenciam o quanto a informação e a comunicação passaram a fazer parte da vida política, econômica e social do indivíduo e da sociedade. Se no contexto da Guerra Fria poucos países tinham poder econômico e tecnológico para elaborar bombas nucleares, no contexto das guerras cibernéticas isso não é mais uma verdade. No ciberespaço, diversos atores podem realizar ações, uma vez que não há limitações físicas significativas, proporcionando maior flexibilidade para superar obstáculos ambientais. Assim, o comportamento político dos atores pode ser influenciado pelas alternativas permitidas por este domínio (Segal, 2016).

A atribuição dos responsáveis por ataques cibernéticos é uma tarefa desafiadora. O acesso às informações que vinculam as ações realizadas ao percursor dos ataques é um obstáculo significativo na investigação desses incidentes. Nas guerras tradicionais, a autoria dos ataques é anunciada antes que eles sejam colocados em prática, esse é um momento estratégico para o conflito. Essa falta de clareza na autoria impacta diretamente as relações internacionais, gerando instabilidade e abalando a geopolítica do ciberespaço, resultando em tensões entre as nações. Diante desse cenário, a distribuição de informações assume um papel que impulsiona a interação entre o ciberespaço e os Estados. Um exemplo disso é a propaganda e a desinformação, que são estratégias utilizadas para minar as

democracias e gerar constrangimento a governos. Um exemplo emblemático é a suspeita de interferência russa nas eleições presidenciais dos Estados Unidos em 2016, com alegações semelhantes também surgindo nas eleições de 2020. O que aconteceu no evento citado foi uma tentativa de disseminar ideologias, arranjos políticos, econômicos ou sociais divergentes através do uso de informações falsas que levam a uma divisão da sociedade e interferem nas movimentações dos Estados. Diante dessas ameaças, os Estados são levados a desenvolver estratégias tanto defensivas quanto ofensivas para proteger seu espaço cibernético. Os eventos de 2016 nos Estados Unidos, por exemplo, levaram à formulação de estratégias destinadas a defesa contra táticas inimigas que comprometem a segurança estatal e minam as relações exteriores, mesmo quando os autores permanecem não declarados (Wilner, 2018).

O mundo enfrenta uma convergência para a fragmentação, e a pandemia de Covid-19 desempenhou um papel significativo nesse movimento, impactando diversos aspectos da globalização. Foram restringidas a circulação de pessoas, bens, serviços e capital. O fechamento de fronteiras fez aumentar o protecionismo e acabou atingindo um ponto fraco da globalização. O uso de ferramentas tecnológicas, mais uma vez, atingiu o comportamento de diferentes atores no ciberespaço. As informações, a comunicação e a mídia foram altamente responsáveis por gerar insegurança, divisão política e questionamentos quanto ao funcionamento das organizações internacionais. O espaço aberto pelos Estados para o acesso ao público global representou em muitos níveis oportunidades de ameaça para a segurança. Por essa razão, ao analisar detalhadamente a segurança internacional no contexto atual do desenvolvimento tecnológico, torna-se necessário impor algum tipo de controle sobre a forma como essas ferramentas são difundidas e utilizadas (Zendelovsk; Cvetkovski, 2021; Bhatt, 2022).

As tecnologias de informação geram mudanças constantes, e a capilaridade do acesso à internet impacta a política internacional. A abertura para esse acesso provoca ameaças substanciais à segurança estatal. Isso inclui a possibilidade de uso dessas ferramentas por atores não estatais, terroristas, organizações criminosas e hackers, manipulando o espaço digital e a sociedade de modo geral, em prol de ações maliciosas, o que leva os agentes estatais a reforçarem a sua proteção. Dessa forma,

a livre circulação de informações em alta velocidade através dos canais de comunicação corrobora para crises políticas (Zendelovsk; Cvetkovski, 2021).

O conflito militar direto entre a Rússia e a Ucrânia tonificou as interações históricas entre os dois países. Iniciada em fevereiro de 2022, a agressão armada contra a Ucrânia realçou o empreendimento russo em operações de guerra. Ao longo do conflito Rússia-Ucrânia, a comunidade internacional adotou providências para retaliar as ações do agressor. Com a comoção gerada em torno do comportamento russo na guerra, diferentes espaços e formas de conflito da Rússia vieram à tona, um deles no ciberespaço. Isso aconteceu, pois, a dinâmica das relações atuais entre os países em guerra deixa claro que a dimensão do poder sobrepõe esferas de influências e domínio dos Estados. Assim, o poder no ciberespaço concentra-se na projeção de cada país sobre os temas que permeiam objetivos políticos e econômicos (Štrucl, 2022).

A análise e monitoramento dos eventos no ciberespaço desempenham um papel crucial no controle das respostas e ações dos atores envolvidos em ataques. Ao monitorar estruturas físicas, redes de comunicação e ao expor conflitos cibernéticos internacionalmente, aumenta-se o potencial de realização de movimentos e resultados inesperados, gerando outras dinâmicas para os conflitos. Esses elementos foram identificados através das análises do incidente russo-estoniano, que foram impostas a ameaças e desafios inesperados. O conflito, que teve início em 2007, teve dimensões limitadas, diferenciando-se do cenário observado desde 2022 com a interferência russa nos domínios ucranianos (Štrucl, 2022).

Alguns países desenvolvem maneiras de operar no ciberespaço em táticas defensivas e ofensivas. Os Estados conduzem essa assistência em segurança através de atores privados, ou seja, não estatais. Em primeiro lugar, são contratadas pessoas capacitadas para a máquina do Estado, abrindo espaço para o que pode ser chamado de milícias cibernéticas especializadas em serviços cibernéticos contra ameaças. Uma alternativa adotada são os hackers patrióticos, que tiveram suas operações observadas de perto desde os ataques a Estônia em 2007 e Geórgia em 2008. Por fim a defesa dos interesses de países como a Rússia podem ser observadas em casos de espionagem, nos quais os hackers garantiram ganhos políticos aos russos. Assim, cada ação, contexto e conflitos de interesses entre os atores fica a cargo da análise realizada sobre a interação dos Estados (Egloff, 2018).

4 A INFLUÊNCIA DA AÇÃO DOS ATORES NÃO ESTATAIS NA CONFIGURAÇÃO CONFLITUOSA DO CIBERESPAÇO

4.1 CAPACIDADE DE PODER DOS ATORES NÃO ESTATAIS NA GEOPOLÍTICA DO CIBERESPAÇO

Novos conceitos sobre guerra se tornaram componente das relações internacionais. Entre as definições pontuadas, uma categoria se destacou, a guerra híbrida. Conhecida como guerra de quarta geração por ser a categoria de guerra que mais apresenta mudanças desde o Tratado de Vestfália, considerando agora a existência de atores não estatais em detrimento do monopólio do Estado na guerra, ela se sobrepõe a três outros tipos de guerra:

- Guerra de Primeira Geração: ocorreu após o Tratado de Vestfália, entre 1648 e 1860. Marcada pelo Estado como detentor do monopólio da guerra, sua característica principal é a mão-de-obra em massa, com uma cultura baseada na ordem, soldados organizados em fileiras e uniformes militares para manifestar descontentamento com a desordem dos campos de batalha;
- Guerra de Segunda Geração: se inicia com o Exército francês sendo encerrada com a Primeira Guerra Mundial. Sua característica essencial foi a capacidade ofensiva, pois, nesse momento, a artilharia é inserida ao conflito;
- Guerra de Terceira Geração: também conhecida como guerra de manobra, foi predominante na Segunda Guerra Mundial. Introduziu a guerra tática de surpresa com o intuito de contornar e minar o inimigo, dessa vez a cultura estava ligada a obediência e autodisciplina
- Guerra de Quarta Geração: possui avanços característicos da obtenção de conhecimento para garantir benefícios sobre o inimigo (Fernandes, 2016; Qureshi, 2019).

A partir da globalização e do aumento do uso de recursos tecnológicos, abriu-se mais espaço para a ação de atores não estatais em termos políticos. Com potencial e capacidade de ser influenciado ou envolver-se com outros atores, a atuação de diferentes organizações, grupos e indivíduos no ciberespaço virou foco de atenção dos Estados. Isso aconteceu pela necessidade de estar sempre a frente do inimigo, ou seja, ter consciência das ações atuais e futuras de prováveis oponentes. Isso justifica o fato de que na guerra híbrida, é necessário entender quais são as

motivações dos atores não estatais e quais são os interesses políticos por trás de uma ação (Peters, 2009; Qureshi, 2019; Ferreira; Framento, 2021).

É importante ressaltar que a guerra híbrida é frequentemente destacada nas discussões políticas, como foi no caso da Invasão russa a Crimeia em 2014, conflito que convergia atores locais armados, influências econômicas, desinformação e a questão da polarização sociopolítica na Ucrânia. Outras duas características importantes para o entendimento da guerra híbrida é entender que o limiar entre a paz e a guerra é cinzento, o que ocorre devido ao uso força durante os períodos de guerra e de paz, por estratégias assimétricas através de meios ilegais, culpando os Estados pelos danos colaterais e utilizando escudos humanos para se proteger (Bilal, 2021; Qureshi, 2019).

O outro aspecto está ligado ao fato de que os ataques híbridos são imprecisos, essa zona cinzenta é criada intencionalmente para dificultar tanto a atribuição quanto a resposta aos ataques. Explicado de outra maneira, se um país alvo é incapaz de detectar um ataque híbrido ou não consegue atribuir responsabilidade a outro Estado que possa tê-lo realizado e patrocinado, ele fica na chamada zona cinzenta. Assim, ao limitar a detecção e atribuição, dificulta-se a capacidade de o Estado de desenvolver políticas e respostas estratégicas. Os custos e riscos envolvidos nesse tipo de operação são menores, ou seja, é mais viável patrocinar e divulgar desinformação em colaboração com atores não estatais, do que deslocar aeronaves para outro território. Sendo possível a existência de uma guerra sem combate direto e com a vantagem de que os danos causados serão os mesmos. Além desse quesito, a guerra híbrida também é considerada obscura porque mais do que oferecer ferramentas para minar o adversário, ela permite que a segurança do inimigo seja prejudicada em decorrência de dois aspectos: 1. Enfraquece a capacidade, as vulnerabilidades nos domínios políticos, militar, econômico, social, informacional e estrutural; 2. É minada a legitimidade do Estado (Bilal, 2021).

As ameaças híbridas, portanto, estão adaptadas a aproveitar as vulnerabilidades dos concertos políticos com o objetivo de explorá-los conforme é percebida a necessidade de exacerbar a polarização, levando a uma erosão dentro dos valores morais que constrói as sociedades democráticas e a tomada de decisão dos líderes, minando, assim, a confiança (Bilal, 2021). Assim, mesmo que não haja o declínio da guerra convencional, a guerra híbrida dificultou o processo de decisão e a

coordenação de resposta nos conflitos, diferindo-se do que o campo militar conhecia até o momento em relação às competências e atribuições (Fernandes, 2016).

O ciberespaço se tornou um dos focos da agenda securitária estatal. Nesse espaço, os setores públicos e privados se tornaram objeto de ameaça graças ao empenho dos Estados em proteger seus dados, redes e sistemas governamentais e privados que armazenam ou controlam informações sensíveis (Ayres; Grassi, 2020). Para tornar as redes interconectadas, foi necessário o aumento da consciência dos países em torno das estratégias de segurança nacionais e internacionais direcionadas ao ciberespaço. Com o objetivo de proteger sistemas e realizar a manutenção de sistemas de interesse nacionais, houve empreendimentos no desenvolvimento de conexões seguras para gerar potencial de respostas coordenadas aos possíveis ataques e interferências externas. Outros fatores importantes para o novo formato das relações internacionais, a partir das interações no ciberespaço, foram a formulação de parcerias para o combate às ameaças; investimento na área de tecnologias de informação e comunicação; gerenciamento de políticas públicas direcionados para o espaço cibernético; coordenação para o desenvolvimento de alianças nacionais e internacionais no setor; e instituições que possam implantar diretrizes e iniciativas na área. Todos esses elementos resultaram no posicionamento padrão dos Estados para um espaço mais seguro e regulado (Machado, 2014).

Implementar sistemas de segurança eficazes nas infraestruturas críticas é um dos desafios dos Estados no ciberespaço. O gerenciamento de crises e respostas ofensivas aos ataques é o cenário ideal para países que sofrem com ameaças cibernéticas. Uma das maneiras de combater atividades maliciosas é a “identificação do ator agressor, regulação dos comportamentos no ciberespaço dando aos Estados a capacidade de demarcar seus limites soberanos e a delimitação de ações legais e sanções possíveis ao transgressor [...]” (Ayres; Grassi; 2020 p. 104). Com isso, potencializa-se a tendência de associar assuntos relacionados as tecnologias da informação e internet às Forças Armadas. Com esse formato, a atividade operacional do Estado demanda aumento de pessoas especializadas na área de TI, permitindo a interação de assuntos tradicionais com as capacidades necessárias para resolução de problemas advindos do ciberespaço. Considerando uma coordenação ofensiva ativa no espaço cibernético, doutrinas e estratégias devem ser elaboradas com foco

na efetividade das práticas dissuasivas. Por isso, percebe-se a recente necessidade de profissionais treinados para atuar no novo domínio do conflito (Machado, 2014).

Em consequência da globalização e do uso de recursos tecnológicos, os riscos e exposição dos Estados a ameaças aumentou. No sistema internacional, a presença de atores estatais e não estatais incorporou novos elementos ao conflito (Qureshi, 2019). Em relação aos atores não estatais, surgiram questionamentos sobre poder, zonas de influência e interesses políticos ligados aos alvos de ataques cibernéticos. A razão disso é que, no conflito cibernético, o combate ao inimigo também envolve fatores que estão além do domínio em que ele acontece, podendo estar conectado a políticas, estratégias e assuntos preponderantes a debates tradicionais. Assim, as análises que incluem o espaço cibernéticos e a internet devem compreender o contexto político em que o conflito está inserido (Peters, 2009; Ferreira; Framento, 2021).

Pode-se observar nas interações no ciberespaço que as capacidades dos atores não-estatais são diversificadas. Esses atores podem ser incluídos em categorias:

- Instituições multinacionais e transnacionais;
- Organizações não governamentais;
- Organizações intergovernamentais;
- Organizações regionais;
- Atores violentos.

Os atores citados podem ter diferentes relações com o Estado. Uma das opções é o surgimento de grupos insurgentes, rebeldes e guerrilheiros como uma resposta a ação e a autoridade do Estado. Outro tipo de interação é a emergência de grupos paramilitares, gangues e crime organizado, como resultado de condições sistêmicas em relação à atuação do Estado e a sua segurança. Isso mostra que a dinâmica do conflito está relacionada com a organização política e interação entre atores (Peters, 2009; Ferreira; Framento, 2021).

Quadro 3: Atores não-estatais no Ciberespaço

Ator	Motivação	Alvo	Método
Cidadão Comum	Nenhuma ou Fraca	Nenhum	Indireto
Hacktivista	Mudanças políticas ou sociais	Tomadores de decisão ou vítimas inocentes	Protestos via páginas da web ou ataques DDoS
Hacker Patriotas	Patriotismo	Adversários do próprio Estado	Ataques DDos ou defacement
Ciberterrorista	Mudanças políticas ou sociais	Vítimas inocentes	Violência ou destruição baseada em sistema de computadores
Autores de malwares	Ganho econômico, ego, animosidade pessoal	Nenhum	Exploração de vulnerabilidades
Ciber Scammers	Ganhos Financeiros	Indivíduos e pequenas empresas	Engenharia social
Crime Organizado	Ganhos Financeiros	Sistemas e infraestruturas baseados em TIC (privados ou públicos)	Malwares para fraude e roubo de identidade
Agentes Espiões	Ganhos políticos e financeiros	Indivíduos, empresas e governos	Técnicas para obter informações
Ciber Milícias	Patriotismo e Desenvolvimento Profissional	Adversários do próprio Estado	Se baseia nas capacidades do grupo

Fonte: Sigholm, 2013. Adaptado.

O ciberespaço é vulnerável às ameaças. A conexão entre diferentes setores da sociedade aumentou o risco de ataques cibernéticos. Com esse cenário, os Estados estão engajados na defesa das infraestruturas cibernéticas da esfera civil e militar. Assim, esforços se concentram em mover ações tanto nas forças armadas quanto nas organizações de segurança nacional em diferentes nações. As medidas adotadas pelos países podem ser defensivas ou ofensivas e, a depender do Estado que opta por empreender em uma dessas operações, elas podem ser realizadas de forma independente ou como uma extensão da guerra tradicional. Com essas informações, os Estados aparentam ser os únicos atores nos acontecimentos no ciberespaço, mas, na verdade, os atores não estatais também assumem papel primordial em determinados eventos dessa esfera. Nesse ambiente, acessado por praticamente todas as pessoas com acesso a aparelhos conectados à internet, as possibilidades são incalculáveis. Por essa razão, atores de variados tipos, com necessidades,

objetivos e intenções diversas podem perpetrar suas ações gerando riscos aos Estados (Sigholm, 2013).

As ameaças cibernéticas se tornaram alvo dos Estados. Com o progresso da internet, juntamente com seu domínio parcialmente universal, os países precisaram desenvolver capacidades para engajar operações militares cibernéticas, cerceando redes que envolvem forças armadas e departamentos de inteligência de todo o mundo. Com isso, foi necessário a promoção do aumento do potencial defensivo para resguardar as infraestruturas de rede vulneráveis a ataques cibernéticos. Sendo assim, com a emergência de conflitos no ciberespaço, os Estados aceleraram o processo de desenvolvimento de recursos capazes de garantir a privacidade, segurança e governança da internet (Sigholm, 2013).

A segurança cibernética tornou-se parte da estratégia estatal. Como resultado dos incidentes decorrentes das atividades no ciberespaço e o potencial de escalada de conflitos, os Estados passaram a usar esse meio para atingir fins estratégicos. Isso levou ao aumento do uso político do espaço cibernético, incorporado por outros meios da prática política. Esse movimento chamou a atenção de atores estatais e não estatais que, na face do conflito, atuam em um espaço com a possibilidade de desestabilizar as redes e as transações de outros atores ou outros Estados, a fim de se beneficiar do anonimato. Diante disso, a dimensão cibernética representa para a segurança estatal um aumento de ameaças sérias e desestabilizantes (Choucri; Goldsmith, 2012; Strategic Trends, 2015).

No ciberespaço, os atores agem concomitantemente. As características, necessidades, objetivos e intenções dos diferentes atores é o que define o que ele representa em uma determinada situação. No ciberespaço, os atos podem ser realizados de maneira independente, em redes ou através de estruturas mais elaboradas. Em alguns casos, há a possibilidade de os atores realizarem movimentos conforme o objetivo ou interesse de cada momento. O espaço cibernético é uma zona de conflito marcada pelo acesso e controle de informações, as atividades que envolvem esse espaço dependem do fluxo de informações da rede e de como elas são disponibilizadas, o que também depende do ator que detém os dados e qual o nível de sigilo. Assim, a prática e o uso do ciberespaço, apesar de fluído, está vinculado com o nível de poder que uma informação possui para atores estatais ou não estatais (Sigholm, 2013).

Os conflitos na esfera física se estenderam ao ciberespaço. A difusão e o acesso à rede possibilitaram que os embates acometidos no meio cinéticos tivessem influência em ações no ciberespaço, desencadeando atos que atingiam o Estado. Esses movimentos tinham como perpetradores sobretudo atores não estatais. Como exemplo, pode ser citado o grupo de hackers nacionalistas sérvios chamado *Black Hand,* que atuou no conflito de Kosovo em 1999 realizando ataques cibernéticos contra um site albanês no Kosovo e geraram ameaça aos computadores da OTAN. Esse foi o primeiro registro de ações cibernéticas potencializando conflitos tradicionais. Com as restrições à mídia independente no Kosovo, uma das reivindicações dos hackers passou a acontecer através de uma guerra de propaganda, em que eram emitidas mensagens e opiniões em sites da internet e, em outros casos, sites que se opunham a opinião dos hackers eram sabotados. Assim, gradativamente os conflitos assumiram forma na internet e se tornaram de conhecimento do público (Sigholm, 2013).

Com poucas normas e regulações, o ciberespaço, para alguns autores, caracterizou-se como um espaço não governado. Segundo Tsagouria (2016), da mesma forma que um Estado fracassado[31] é um espaço sem a predominância de um governo, o espaço cibernético encontra-se sem as diretivas estatais em seu domínio. Quando um Estado é considerado fracassado, suas ferramentas de poder que formam as políticas e a ordem de uma nação estão em declínio ou inexistem. Esse cenário gera o não reconhecimento do Estado como uma unidade soberana do sistema pela comunidade internacional. Os conceitos de Estado fracassado e não governado se cruzam quando apresentam uma corrosão na capacidade do Estado de exercer poder em um espaço em termos geográficos e de governança. Com essa semelhança, os espaços não governados são a opção mais próxima do ciberespaço, pois a definição dessa expressão é mais inclusiva. Esse pensamento decorre da ideia dos Estados como ponto central das relações internacionais, em que necessariamente há uma autoridade central nas interações no sistema. Em segundo lugar, ao tratar-se de espaços não governados, pode ser que o poder não esteja centrado no Estado, mas em atores não estatais. Isso significa que a ausência de governos estatais não impede

[31] “A terminologia “Estados fracassados” foi adotada, por se entender que o fracasso estatal se dá em termos de falência institucional, não apenas uma alusão à falência econômica, como sugere o termo “falido”” (Bijus; de Oliveira, 2011).

a organização de estruturas alternativas. Assim, fica aberta uma lacuna que ameaça a segurança e a ordem internacional (Tsagourias, 2016).

A responsabilização de atores não estatais fica a margem de autoridades com capacidades legais no cenário internacional. Essa tarefa depende do poder de impor o cumprimento de normas e regras para controlar territórios e pessoas. No entanto, tudo isso depende da organização em que os Estados estão submetidos, regras e processos claros. A manutenção do poder estatal depende, nessa circunstância, da maneira pela qual os atores não estatais estão organizados e sustentam a sua autoridade perante a estrutura social levantada por eles. No caso dos grupos atuantes no ciberespaço eles exercem atividades semelhantes ao que acontece nos domínios tradicionais. Apesar da possibilidade inexistente de controlar em primeiro momento espaços físicos, há o exercício de poder sobre as pessoas. Por isso uma das estratégias usadas por esses atores é incentivar os membros a agir em publicações de alvos, selecionar armas cibernéticas e engajar nos ataques. As armas cibernéticas são ferramentas tecnologicamente elaboradas com o aparato de softwares e construídas com complexidades e especificidades para invadir espaços vulneráveis de sistemas de informação altamente protegidos. Sendo assim, a organização dos atores não estatais no ciberespaço é uma das variáveis mais importantes do trabalho realizado, uma vez que são as ferramentas utilizadas que garantem a perpetuação de sua ameaça a segurança internacional (Rid; McBurney, 2012; Tsagourias, 2016).

As mídias sociais possuem papel importante na internet. Os principais debates realizados na esfera física são colocados em discussão no ambiente virtual e geram choques nas mídias sociais, principais meios de interação na internet. A disputa existente no uso e controle de informações colocam em pauta debates como a privacidade, o compartilhamento de informações confidenciais, os limites da liberdade de expressão, a segurança, a governança e a existência da neutralidade na internet. As interações realizadas na internet estão além do que acontece nesse meio, elas são vetores de mobilização social, usam o que acontece em manifestações nas ruas, por exemplo, para coordenar respostas, impulsionar e divulgar informações. Com isso, em momentos conflituosos, o ciberespaço, os recursos e informações dos usuários, ficam expostos às ações dos atores que coordenam e estão liderando e utilizando as ferramentas cibernéticas em prol de um objetivo político (Sigholm, 2013).

A participação política dos hackers na internet utilizou de diferentes tecnologias. O hashtag é um exemplo de recurso usado por hacktivistas para organizar protestos. Além desse, o envio de mensagens via e-mail é um artifício comum. Essas comunicações são intensificadas pelo uso das mídias sociais como o Twitter, Facebook e Youtube em que os grupos conseguem mobilização e engajamento por parte de pessoas que participam de lutas políticas. As principais ações dos hacktivistas nesse espaço são:

- Atacar a configuração de sites;
- Invadir sistemas para o vazamento de documentos sigilosos;
- Realização de ataques DoS.

A comoção da sociedade é um elemento que desafia autoridades quanto a ação dos hackers. Devido ao impacto gerado pelas campanhas subversivas nas redes sociais surgem conflitos com atores estatais e autoridades legais. Após operações em que grupos hacktivistas realizou de discursos em defesa da democracia e liberdade de expressão houve a ausência de debates sobre ativismo social nas mídias. Esse vazio foi ocupado por elites neoliberais financiadas pelos Estados, manipulando a ordem social. Essas ações prejudicaram discussões políticas internacionalmente como a campanha do Brexit entre Reino Unido e União Europeia, e a corrida eleitoral de 2015 nos Estados Unidos. O principal foco nos casos apontados foi a disseminação de informações falsas que dividiu a sociedade com publicações acompanhadas de memes com teoria da conspiração. Assim, no lugar de unificar a opinião pública, influenciando multidões de internautas as ações promovidas por grupos com o apoio estatal dividiram a sociedade em opostos (Sharevski; Kassell, 2023).

As eleições dos EUA em 2016 foi alvo de hackers. Durante a corrida eleitoral, o país enfrentou problemas com notícias falsas veiculadas em redes sociais como Facebook e Twitter. Segundo os políticos que pleiteavam o cargo da presidência dos Estados Unidos, essa atividade teria manipulado a opinião pública e consequentemente o voto dos eleitores. Esse momento marcou a política norte americana e foi importante para o cenário internacional pois reforçou o poder político dos hackers na internet. Para o governo russo, os ocorridos referente as atividades de hackers patrióticos, aconteceram a partir da observação das interações estatais em que foi verificada a necessidade da expressão de suas lutas em prol dos interesses da nação. Com isso líderes do governo, em seus discursos expressaram falas em que

comunidade internacional concluiu como cobertura e apoio as práticas dos grupos para fins estratégicos. Apesar disso, há indícios que a polícia russa tenha realizado prisões relacionadas com os acontecimentos de 2015 e 2016, tem como exemplo a prisão de hackers associado ao Trojan Dyre[32] e ao grupo Lurk [33]. Assim, a responsabilização de diferentes atores em atividades no ciberespaço depende da interpretação do contexto e dos elementos que compõe todo o cenário (Egloff, 2018).

4.2 A ATUAÇÃO DOS HACKERS NO CIBERESPAÇO

Os conflitos no ciberespaço são complementos das disputas políticas. O entendimento sobre o cenário atual da cibersegurança é o que possibilitará que os Estados estabilizem suas relações. Isso significa que é importante analisar as tendências da internet em relação a teoria e a realidade. No início dos estudos sobre as disputas no ciberespaço, o termo mais utilizado para falar sobre o conflito nessa esfera era guerra cibernética. No entanto, os conflitos cibernéticos de baixo nível também têm sido objeto de análise. Isso acontece pois, desde o surgimento da internet e dos primeiros ataques cibernéticos, as principais preocupações do Estado eram sobre os riscos das vulnerabilidades de suas infraestruturas críticas. Esse ponto de atenção se fortaleceu em razão da crescente dependência do ciberespaço para a gestão da informação, comunicação e controle da máquina estatal. Dessa maneira, as nações empreenderam políticas e estratégias para evitar o poder destrutivo de um ciberataque que poderia destituir todo o aparato cibernético do país (Dunn Cavelty *et al*, 2015).

Os conflitos cibernéticos têm sido observados em novas perspectivas. É pouco provável que ferramentas cibernéticas sejam utilizadas a longo prazo para atender a objetivos estratégicos, por razões práticas. Isso quer dizer que não é sustentável manter e monitorar os efeitos das armas cibernéticas no período necessário para

[32] O trojan bancário Dyre era normalmente distribuído por meio de campanhas de spam e foi responsável por mais de centenas de milhões de dólares em perdas em instituições bancárias e financeiras, incluindo o Bank of America Corp, o PayPal e o JPMorgan Chase & Co" (Khandelwal, 2016). O Dyre foi o trojan mais ativo em 2015, acumulando milhões para seus operadores. Por exemplo, acredita-se que ele tenha sido usado em um ataque de US$ 5 milhões à companhia aérea de baixo custo Ryanair em maio de 2015 (Muncaster, 2016).

[33] Um tribunal russo condenou o suposto líder do grupo de hackers Lurk e autoproclamado hacker por trás do vazamento de e-mails do Comitê Nacional Democrata dos EUA em 2016 a 14 anos de prisão. Os investigadores acusaram Konstantin Kozlovsky e seu grupo de criar o vírus Lurk, que lhes permitiu roubar mais de 1 bilhão de rublos (US$ 13,2 milhões) de bancos e empresas russas desde 2013(The Moscow Times, 2022).

garantir que o propósito seja cumprido. Assim, com todo o cenário de disputa entre variados atores, o ciberespaço continua sendo instrumento essencial para o funcionamento do Estado em serviços governamentais, militares, econômicos e sociais. Por esse motivo, os conflitos de baixo nível surgem como uma extensão dos conflitos convencionais. As atividades mais comuns nesse cenário são a difusão de informações tendenciosas e o hacktivismo. Esses eventos têm chances maiores de acontecer e menores impactos segundo o artigo do *Strategics Trends* de 2015. Também existem eventos de baixo nível com alto impacto, nessa categoria podem ser destacados os acontecimentos na Estônia em 2007, Georgia em 2008 e Ucrânia 2013, descritos abaixo. Assim, atores estatais e não estatais agem na tentativa de influenciar os conflitos com base nas oportunidades geradas pelo uso e empreendimento de campanhas de informação (Dunn Cavelty *et al*, 2015).

Quadro 4: Nível dos conflitos no ciberespaço: descrição e atores

Incidente	Descrição	Atores
Estônia (2007)	3 três semanas de uma onda de ataques cibernéticos acompanhados de tumultos na Estônia provocados pela remoção de uma estátua de um soldado do Exército Vermelho	- Hackers patriotas (pró-Rússia); - Nenhuma prova de envolvimento do Estado mas houve falha e indisponibilidade para cessar os ataques.
Georgia (2008)	Ataques cibernéticos acompanhados de cinco dias de conflito militar entre Georgia e Rússia	- Hackers Patriotas Russos - Rede Comercial Russa (Provedor de Serviços de Internet Criminal); - Nenhuma prova de envolvimento do Estado mas houve falha e indisponibilidade para cessar os ataques.
Ucrânia (2013)	Ataques cibernéticos acompanhados por crise Russo-ucraniana	- Ciber Berkut (e outros grupos hacktivistas pró-Ucrânia); - Hackers Patriotas Russos; - Trolls pagos.

Fonte: Dunn Cavelty *et al*, 2015

Quadro 5: Nível dos conflitos no ciberespaço: métodos, alvos e impactos

Incidente	Métodos	Alvos	Impactos
Estônia (2007)	- Ataque Distribuído de Negação de Serviço (DDoS), usando bots; - Websites defacements (Propaganda Russa).	- Websites do Parlamento, Primeiro Ministro e Presidente; - Websites do Ministério das Relações Exteriores e Ministério da Justiça; - Jornal Diário Estoniano e Emissoras; - Hansabank.	- Impacto primário muito baixo: websites indisponíveis, danos econômicos); - Grande impacto secundário: tonou-se um evento que se assume para provar o quão perigoso é o ciberconflito.
Georgia (2008)	- Ataques DDoS; - Websites defacements.	- Website do Presidente da Georgia; - Websites Governamentais da Georgia; - Websites de notícias da Georgia e da Rússia; - Bancos da Geórgia.	- Impacto direto muito baixo, muito relacionado ao fato de que a Georgia não é muito dependente da infraestrutura de TI; - Outro evento que assume a guerra cibernética.
Ucrânia (2013)	- Ataques DDoS; - Websites defacements; - Esvaziamento de dados; - Desinformação e campanhas de propaganda; - Perturbação e infiltração da internet e do tráfego telefônico.	- Sites do Governo e telecomunicações para veículos de mídia de destaque; - Tráfego da internet.	- Baixo efeito sobre o conflito em si.

Fonte: Dunn Cavelty *et al*, 2015

As instituições estonianas foram atacadas por hackers. Em 2007, investigações em cibersegurança identificaram a ação de atores não estatais como autores de ataques cibernéticos contra a Estônia. Esse movimento foi decorrente das tratativas da Estônia para a alteração da alocação do Monumento do Soldado de Bronze de Tallinn, inaugurado em 1947 como representação de soldados soviéticos que foi mantido até aquele momento no memorial da Segunda Guerra Mundial no centro de Tallinn para cemitério militar. A Rússia observou essa ação como uma tentativa de mudar a história da guerra. Com isso, a câmara legislativa russa passou a sinalizar a possibilidade de romper as relações diplomáticas com a Estônia (Pernik, 2018).

A troca entre os dois países foi prejudicada. O objetivo dos ataques cibernéticos era interromper a realocação do monumento soviético da Segunda Guerra Mundial. O meio utilizado para atingir esse fim foi perturbar as instituições estonianas. A partir disso as maiores consequências dos acontecimentos decorrentes

dos atos hackers foram monetários. A Rússia impôs limitações às exportações e suspendeu contratos com empresas estonianas. Além disso, o trânsito de mercadorias entre os territórios diminuiu e a conexão via ferrovia foi interrompida. Nesse cenário canais de comunicação russos passaram a disseminar desinformação estimulando a população estoniana colocar-se contra o governo. Esses acontecimentos permitiram que os hackers russos influenciassem o processo interno com ataques cibernéticos à partidos políticos, sites do governo, agência de notícias bancos e outras instituições. Esses atos começaram em 27 de abril e durou até 18 de maio com ataques DoS, DDoS, *defacements* de sites, e-mails com spams e disparo de comentários automáticos. No início os ataques eram pouco sofisticados, mas ao longo dos dias eles foram evoluindo e em 30 de abril as infraestruturas críticas tornaram-se alvo. Perante a essa situação estrutura ficou propicia a escalada dos ataques. Um dos setores afetados foi o bancário, que ficou com o sistema inoperável por longos períodos, principalmente para pessoas que estavam fora do país. Diante disso foi necessário bloquear o acesso internacional da rede e os usuários externos à Estônia ficaram sem conexão aos sistemas e acessos (Pernik, 2018; Tikk; Kaska; Vihul, 2010).

Os hackers russos atingiram o objetivo pretendido. A Crise do Soldado de Bronze demonstrou como os ataques cibernéticos podem influenciar o comportamento da sociedade e impactar na opinião pública. A partir do ocorrido na Estônia em 2007 alguns militares reconheceram a possibilidade de ataques cibernéticos causarem efeitos psicológicos relevantes gerando desestabilidade que alteram processos de tomada de decisão mesmo que sem o uso da força. Assim, nessa ação houve uma coação das autoridades estonianas sem danos materiais ou perdas de vidas, dessa forma, não os ataques não foram contemplados por punição pelo uso da violência porque efetivamente ataques cibernéticos não são equivalentes ao uso convencional da força (Pernik, 2018; Haataja, 2017).

Entre 2008 e 2012 atos de hacktivistas chamaram atenção. As campanhas dos hacktivistas se tornaram questão de segurança nacional pois as intenções desses atores chocaram-se com a necessidade de classificação e controle de informações por parte dos Estados. O grupo *Anonymous* se destacou na internet realizando campanhas na internet relacionadas a causas políticas. As ações desse ator visavam expor alvos amplamente reconhecidos, geralmente Estados, através da divulgação de

informações confidenciais. Em alguns casos, o *Anonymous* lutava contra interferências na liberdade de informação e expressão. O grupo aproveitava-se de causas emergentes que representavam sentimento de revolta coletiva sem ter necessariamente a existência de um conflito para fortalecer o movimento de suas campanhas. Com isso diferentes governos conseguiram atribuir os perpetradores dos atos através de investigações com pessoal infiltrado nas campanhas, permitindo que as agências de segurança pudessem julgar e processar hackers pelos atos do *Anonymous* (Dunn Cavelty *et a*, 2015).

Há dificuldade de atribuição dos ataques cibernéticos. Existem suspeitas que os ataques cibernéticos disseminados nos países vizinhos da Rússia entre 2007 e 2017 tenham sido de autoria do Estado russo. O país é reconhecido por utilizar ferramentas e práticas coercitivas na região em torno do país, como ameaça de cortes de energia, persuasão de elites políticas e empresariais, atração do crime organizado, campanhas de *fake news*, propagandas e manipulação de minorias de populações de língua russa. Com base nas acusações sobre a Rússia, organizações internacionais, como a União Europeia (UE) e a OTAN, passaram a debater regiões que significavam zonas de conflito no ciberespaço. Esses espaços, conhecidos pela ambiguidade estratégica, possuem nuances que permitiriam, a depender da ameaça deferida, o uso da força. Essa atitude da UE e OTAN também foi importante para a Rússia, pois o país conseguiu aproveitar a lacuna existente na falta de normas do direito internacional para regular o ciberespaço no que se refere a questões como jurisdição, responsabilidade, definição de ataques cibernéticos. Diante disso, independente das suspeitas contra o Estado russo, todas as acusações foram negadas e as provas recolhidas não foram suficientes para provar o envolvimento do país nos ataques cibernéticos ocorridos na região (Pernik, 2018).

A Georgia foi alvo de ataques cibernéticos em 2008. A empreitada dos hackers contra a Georgia estava ligada ao conflito militar entre a Georgia e a Rússia, que acontecia naquele momento. A atividade, que atingiu cerca de 90% dos sites do governo e endereços do domínio .ge, incluiu uma série de outras ações como disparo de e-mails contendo spam e infecção de sites da web. As caraterísticas desses ataques foram parecidas com os incidentes da Estônia de 2007, em que os hackers distribuíam as mensagens para seus alvos em língua russa. Além disso, a Equipe de Resposta a Emergências Informáticas da Georgia identificou que os endereços de IP

e DNS rastreados responsáveis pelos ataques eram de propriedade do grupo de crime organizado *Russian Business Network* (RBN), do qual suspeitava-se conexões com o governo russo. A campanha lançada por esses hackers coletou informações sigilosas do aparato governamental e não governamental georgiano e esteve relacionado com o contexto geopolítico e estratégico mundial. Há suspeita de que os militares russos estivessem envolvidos nos ataques cibernéticos e as investigações indicam que os hackers têm relações com os serviços de segurança russos (Pernik, 2018).

As operações de espionagem cibernética contra a Ucrânia escalaram de forma inesperada. A Ucrânia não estava preparada para a onda de ataques que sofreria entre os anos de 2014 e 2017. Desde 2013, os ataques DDos e *defacements* começaram a aumentar, porém esses ataques foram ignorados. Inicialmente foram deteriorados os canais de e-mails e outros meios de transmissão de mensagens. Em seguida, foram disparadas chamadas e mensagens de texto em smartphones com propaganda e, na sequência, foi a vez das plataformas de notícias e meios de comunicação social, organizações do Estado, instituições bancárias e partidos políticos sofrerem com as ações dos hackers. Assim, foram iniciados os ataques cibernéticos contra a Ucrânia e a infraestrutura de cibersegurança do país era pouco desenvolvida (Pernik, 2018).

Diversos setores da sociedade ucraniana sofreram com ataques e espionagem cibernética. Hackers russos foram identificados como os autores dos ataques à Ucrânia. Os domínios ucranianos, ativos a partir de 2010, estavam sendo espionados desde 2013 pelo grupo Gamaredon e Armageddon. As empresas de segurança do país descobriram que os principais alvos de vigilância eram os setores militares e a segurança nacional. Nos mesmos anos em que a Ucrânia sofreu com os ataques e espionagem de hackers, o sistema eleitoral também foi atingido. Assim, mesmo que as ações desses atores fossem pouco sofisticadas, as campanhas empreendidas a longo prazo acabaram afetando o país de forma generalizada (Pernik, 2018).

Ataques a infraestruturas críticas tornaram-se recorrentes na Ucrânia. Os ataques cibernéticos disseminados pelos hackers russos à Ucrânia adotaram características de maior poder destrutivo, atingindo o Estado intensamente. No ano de 2014, o malware *Black Energy* foi distribuído para seis empresas do ramo ferroviário do país e prejudicou sistemas de tecnologia da informação da região. Em 2015, ocorreram falhas de energia relacionadas a infecções aos sistemas do setor

elétrico do país. Em 2016, o foco foi os sistemas de tráfego aéreo do aeroporto de Kiev, capital da Ucrânia. Junto a esses ataques, o setor financeiro também foi atingido, os principais alvos foram o tesouro nacional e o fundo de pensões do Estado. Os ataques mais onerosos ao Estado ucraniano aconteceram em 2017. Eles desconectaram 10% dos computadores do país e gerou despesas que chegaram a 0,5% do PIB. Com isso, o Estado foi obrigado a revisar sua estratégia a longo prazo para planejar e tomar medidas cautelares contra os ataques cibernéticos nos setores de energia e finanças públicas (Pernik, 2018).

O comprometimento do processo eleitoral ucraniano foi um marco da ação dos hackers pró-Rússia. Há suspeitas de que as informações reveladas sobre as eleições do país tenham sido realizadas entre os hackers e o canal de televisão 1. Os grupos mais atuantes no período eleitoral foram o CyberBerkut, o Cyber Riot Novorossiya e o Green Dragon. O grupo CyberBerkut se destacou por um dos ataques cibernéticos mais graves, responsável por comprometer o Comitê Eleitoral Ucraniano. As ações dos hackers foram responsáveis por destruir dados dos sistemas das eleições. Além da destruição das infraestruturas eleitorais, o grupo também interveio no software responsável por divulgar o resultado das eleições na página do Comitê Eleitoral. Diante disso, investigações realizadas pela Equipe de Resposta a Emergências Informáticas da Ucrânia verificou a presença do serviço secreto russo em 2014, sugerindo que o governo do país estivesse envolvido nos ataques (Pernik, 2018).

4.3 CASOS DE ATAQUES CIBERNÉTICOS E PERSPECTIVAS ATUAIS

A partir de 2015, documentos sobre segurança cibernética foram elaborados e atualizados ao redor do mundo. Nos EUA, houve uma atualização da avaliação do impacto na privacidade para os *Enhanced Cybersecurity Services* (ECS)[26]. Esse documento reflete a *Executive Order* 13636[34] de 2013. As recomendações do ECS são:

1. Fornecer informações atualizadas sobre a retenção de indicadores;

[34] Em fevereiro de 2013, o presidente Barack Obama assinou a Ordem Executiva 13636, intitulada "Improving Critical Infrastructure Cybersecurity". Essa ordem visava aprimorar a segurança cibernética dos setores de infraestrutura crítica promovendo o compartilhamento de informações entre entidades do governo e do setor privado.

2. Refletir o estado atual dos testes e as proteções de qualidade de dados existentes;
3. Refletir a frequência atual das revisões de registros; e
4. Descrever como a análise subsequente das métricas de segurança cibernética pode levar ao desenvolvimento de novos indicadores.

Esse programa se refere a relações público e privadas, e é dividido em algumas áreas: todas as capacidades; contempla todos os domínios; e coleta de dados; que são mantidos sob o controle do *National Cibersecurity Protection System* (NCPS). Essas informações são excluídas quando se tornam vulneráveis ou quando se tornam desnecessárias ao departamento. Nesse sentido, esse é um dos documentos que buscam melhorar os processos administrativos internos dos EUA em temas relativos a cibersegurança (U.S. Department of Homeland Security, 2015).

Em novembro de 2022, foi aprovada uma nova legislação para o fortalecimento da segurança cibernética dos países da União Europeia. A Diretiva[35] 2022/2555 do Parlamento e do Conselho Europeu publicada em 14 de dezembro de 2022, é um ato legislativo que faz referência a medidas que garantam a cibersegurança na UE. Essa nova regulação altera o Regulamento nº 910°/2014 e a Diretiva 2018/1972 e revoga a Diretiva 2016/1148 (Diretiva NIS 2). Esse novo documento tem como objetivo responder as ameaças impostas pela inovação tecnológica e aumento da ocorrência de ataques cibernéticos. Com isso, ficou determinado que os Estados devem adotar estratégias nacionais de cibersegurança e que autoridades especializadas em gestão de crises de segurança cibernética devem compor as Equipes de Resposta a Incidentes de Segurança em Sistemas Computacionais (CSIRT) (Europe Union, 2023; Pingen, 2023).

Houve avanços com a aprovação da Diretiva 2016/1148. Essa legislação deu oportunidade para que a segurança cibernética fosse institucionalizada e regulada na UE nas suas divisões nacionais. Isso foi feito através da melhoria de estruturas nacionais de segurança de redes e sistemas informacionais por meio de capacidades nacionais por meio de medidas regulatórias que englobam as infraestruturas críticas identificadas pelos Estados-membros da organização. Além disso, a Diretiva contribuiu para a para a identificação dos pontos ineficazes em termos de segurança

[35] “Uma diretiva é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. No entanto, cabe a cada país organizar as suas próprias leis para alcançar esses objetivos” (União Europeia, 2023).

cibernética de cada país. Outra questão importante para legislação foi a identificação e eliminação da divergência entre legislações os Estados da UE. Houve a tentativa de garantir segurança jurídica em relação a gestão de riscos da cibersegurança em relação a instituições públicas e privadas na aplicação da lei fossem consideradas a partir da Diretiva da UE. Para isso ficou definido que na Diretiva para garantir quesitos de segurança e supervisão de leis nacionais, os Estados-membros ficam isentos das obrigações com a instituição (Europe Union, 2023).

Segundo a RAND Corporation*, think tank*[36], que realiza pesquisas que visam impactar a política global através de suas soluções, os setores de estratégia e segurança dos EUA. A organização e os documentos oficiais do Estado apontam como foco um novo planejamento de defesa. A partir de 2022 os setores estratégicos dos EUA passam a observar os países considerados potências próximas, atenuando o papel de grupos extremistas não estatais. No histórico norte americano, esses atores representaram grandes ameaças à segurança nacional e internacional por atividades que atingiram severamente o país e os países aliados. O impacto desses grupos ainda compele a segurança e defesa do Estado, enquanto outros atores também influenciam as relações das nações que dependem de infraestruturas conectadas em redes para manter o funcionamento de seus serviços (RAND, 2024; Mazarr; Frederick; Crane, 2022).

A atenção concentrada em potências próximas foi anunciada nos documentos de Estratégia de Segurança Nacional de 2017 e Estratégia de Defesa Nacional divulgado em 2018. Desde as publicações realizadas pelas instituições do Estado e governo norte americano, acontecimentos internacionais repercutiram a maneira como o país observam suas interações com o sistema e países como China e Rússia. Um dos fatores que influenciaram a maneira como os EUA começou a conduzir suas políticas estratégicas militares e de segurança, está na invasão da Rússia na Ucrânia. Isso formou uma estrutura que permitiu uma estratégia clara sobre como os setores de relações internacionais do país devem agir mediante a situações críticas. Com isso,

[36] Think tanks são instituições que desempenham um papel de advocacy para políticas públicas, além de terem a capacidade de explicar, mobilizar e articular os atores. Atuam em diversas áreas, como segurança internacional, globalização, governança, economia internacional, questões ambientais, informação e sociedade, redução de desigualdades e saúde. Produzem pesquisas, análises e recomendações que contribuem para um ambiente de conhecimento, permitindo, inclusive, que os formadores de políticas públicas tenham ferramentas para tomar decisões mais embasadas, além de ter um papel importante na disseminação de conhecimento à sociedade (Enap, 2024).

novos elementos foram incorporados e considerados relevantes para a formatação das ações e comportamento dos EUA (Mazarr; Frederick; Crane, 2022).

Um dos subtópicos da Estratégia de Segurança Nacional dos EUA foi a segurança no ciberespaço. O documento aponta a importância de redes seguras para a manutenção das atividades que atendem a sociedade civil e assuntos estratégicos do país. Além disso, demonstra preocupações com as vulnerabilidades a que estão expostos e afetam a qualidade e condução dos seus serviços, citando como exemplo a Rússia e os ataques realizados por esse país, que impõe preocupação e coage os cidadãos estadunidenses. Por essa razão o documento firma o trabalho com aliados externos para estabelecer melhorias no setor cibernético (Biden, 2022).

Para agilizar a respostas a ataques cibernéticos, o documento do governo dos EUA se compromete a desenvolver-se coletivamente. O alargamento das relações com outros países do mundo incorpora aos Estados Unidos a conexão com autoridades militares e a proibição de refúgio aos criminosos cibernéticos. Isso mostra que o país aposta no poder nacional na tentativa de barrar a atuação de atores estatais e não estatais no espaço cibernético. Assim, o país demonstra interesse direto em expandir suas capacidades no ciberespaço, estabelecendo regulações firmes para melhorar e aumentar a estabilidade nacional sobre o espaço cibernético (Biden, 2022).

O estudo "*Understanding a New Era of Strategic Competition*" publicado pela RAND *Corporation* em 2022, aponta cinco tendências estratégicas emergentes. Esses pontos focais da política internacional estão ligados ao sistema multipolar global, desafios da predominância do modelo neoliberal, a quarta Revolução Industrial, surgimento de info esferas vulneráveis e a crise das mudanças climáticas. Sobre o ciberespaço, a pesquisa mostra que o crescimento de redes vulneráveis deixa os países expostos a invasões e ataques cibernéticos. O empenho de diferentes atores nessa esfera está alinhado ao empreendimento em influenciar a opinião pública e outros temas referentes a política dos Estados. As estatísticas demonstram como esse tipo de intrusão se tornaram realidade para os países:

- Um estudo da Corporação Internacional de Dados estimou em 2019 que 41 bilhões de dispositivos estarão conectados a internet até 2025;
- Empresas públicas registraram aumento de ataques *ransoware*[37] em 350%;

[37] O ransomware é um tipo de malware que bloqueia os dados ou o dispositivo de uma vítima e ameaça mantê-los bloqueados (IBM, 2024).

- Aumento de 70% de ataques realizados contra sistemas específicos e empresariais.

E podem crescer ainda mais, o que eleva a preocupações dos países em suas atividades e atuação aos demais atores do sistema internacional no ciberespaço (Mazarr; Frederick; Crane, 2022).

Pode-se concluir que analisar e estipular ações para o ciberespaço são tarefas em avanço (Van Rens, 2019). O que separa a paz e a guerra são nuances entre elementos que separam e unem os Estados e por isso há constante movimento nas relações internas e externas aos países. Isso acontece por meio de manifestações contra governos, conflito entre adversários, desorganização e desmobilização interna, opinião pública e desinformação como instrumento de interferência e resistência. Essas ferramentas e meios de ação, usados por atores estatais e não estais são capazes de comprometer a manutenção de normas, leis, tratados e perturbar a ordem dos Estados a nível nacional e internacional (Shlyakhtunov, 2021). Por isso, a preocupação com a segurança cibernética está crescendo e tende a aumentar, em termos de políticas públicas com uma abordagem baseada em riscos que visam proteger os Estados contra ameaças no ciberespaço.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa utilizou elementos teóricos e práticos da geopolítica e das teorias das relações internacionais para explicar a dinâmica do espaço cibernético, argumentando como a política estatal pode influenciar a ação de atores não estatais nesse ambiente. Assim foi traçado o histórico das relações, destacando a atuação de hackers russos contra Estônia, Geórgia e Ucrânia desde 2007, analisando o comportamento desses hackers e investigando o envolvimento de atores estatais. Todo esse levantamento foi contextualizado à luz da Guerra entre Rússia e Ucrânia, proporcionando uma nova perspectiva para compreender a geopolítica.

Esta abordagem das relações internacionais é objeto de discussão por alguns estudiosos, considerando que o conflito é eminente e esperado, podendo desencadear uma série de comportamentos. Tanto em situações de convergência de interesses quanto em momentos de divergência, a interação estatal pode resultar em interdependência, cooperação, constrangimento ou guerra. Em contextos de conflito direto, todos os atores do sistema internacional, segundo a lógica realista, enfrentam pressões externas que moldam o comportamento de diversos grupos sociais.

As teorias das relações internacionais adotadas para analisar os fenômenos de diferentes atores neste trabalho respondem à questão sobre a relação entre geopolítica, segurança cibernética e atores não estatais. O levantamento bibliográfico observa que tanto a teoria construtivista quanto a teoria realista oferecem abordagens que permitem compreender esses elementos sob diferentes perspectivas. Por esse motivo, uma das questões abordadas no texto é a discussão sobre a identidade no construtivismo, assim como suas relações que, na teoria realista, incidem diretamente com os interesses de uma nação e as questões securitárias.

Neste estudo, a análise da configuração geopolítica em meados de 2022 levanta uma questão fundamental abordada pelas teorias de relações internacionais, cujas respostas podem não ser suficientemente claras para compreender plenamente os determinantes do ciberespaço. Após o desencadeamento da Guerra da Ucrânia, observa-se que a geopolítica assume um papel central na segurança cibernética. Ao utilizar hackers como exemplo para ilustrar a atuação de atores não estatais no ciberespaço, fica evidente que mesmo quando o Estado não está diretamente envolvido de maneira oficial, as preocupações relacionadas à segurança estatal desempenham um papel significativo nas discussões. Em última análise, a

perspectiva adotada na análise do espaço e da segurança cibernética pode influenciar os avanços e as inferências obtidas, apontando para novas direções de pesquisa.

Autores construtivistas e realistas buscam explicar o avanço das atividades estatais e não estatais no ciberespaço, considerando o impacto da tecnologia nas relações internacionais. Alguns atores estatais expressam hostilidade a acordos que propõem normas para as tecnologias da informação, resultando em termos securitários devido à falta de regulação. A falta de regulação gera, nesse caso, um espaço com muitos desafios e incertezas. Vale ressaltar que países como Estados Unidos e a Rússia, não mostram forte engajamento na temática da segurança cibernética dentro das organizações internacionais, o que poderia contribuir para a criação de políticas e práticas comuns com outros países, garantindo um ciberespaço normatizado. As políticas desses países sobre questões cibernéticas são centralizadas, dentro dos e para os próprios Estados, com a formulação de estratégias de segurança fortes e que validam o comportamento deles perante a um sistema observado por cima de muralhas securitárias e operações ultrassecretas. Isso fortalece discursos e comportamentos agressivos no domínio cibernético.

Essa abordagem não se limita ao comportamento no espaço cibernético; reflete também como os atores se mobilizam no sistema internacional. Por isso, na ótica da segurança, os Estados têm foco na defesa dos aparatos, recursos e indivíduos nacionais e, para manter seus mecanismos em pleno funcionamento e seguros, são elaborados planos de ação correspondentes às ambições políticas internas e externas aos Estados.

O comportamento dos Estados é fundamentado nos interesses nacionais e na projeção de poder no contexto internacional. Diversos mecanismos facilitam a interconexão entre as nações, incluindo organizações internacionais que servem como canais para negociação, formação de alianças e parcerias. Para que esses dispositivos funcionem adequadamente, é crucial assegurar o envolvimento ativo nas atividades promovidas entre as nações. No âmbito da segurança, existem restrições mais significativas sobre as ações de cada país em tais instituições. Por essa razão, alguns Estados optam por uma menor conformidade com as políticas vigentes no sistema internacional, buscando maior interação com as questões nacionais para proteger suas estruturas políticas, econômicas e sociais. Dessa forma, buscam dissociar seu papel e imagem de outros países.

Estados Unidos e Rússia preservam suas imagens, ideias e propostas alinhadas à política interna, usando-a como expressão de poder para o resto do mundo. Esses dois Estados, assim como as outras nações, dependem de negociações e transações com outros países, mas trabalham em uma linha tênue entre cooperação e interesses nacionais, especialmente quando o tópico é segurança. Esse comportamento reflete constante alerta, remanescente da Guerra Fria. Logo, é possível ver que, apesar dos assuntos e movimentos internacionais, esses países ainda são capazes de elaborar estratégias de sobrevivência, recordando as teorias de guerra do realismo nas relações internacionais.

Ao longo da análise, os Estados estiveram no centro das preocupações. São eles os provocadores das ações de hackers, sejam vinculados a Estados ou não. Portanto, a geopolítica se mostra presente nas mais diferentes instâncias e circunstâncias, pois as operações de um Estado em qualquer domínio se fazem importante a partir do momento em que estamos em um sistema organizado do ponto de vista político, em territórios com fronteiras. Essa delimitação espacial, crucial na geopolítica convencional, torna-se um ponto de debate ao ser transferida para o ciberespaço, onde as mesmas regras e controle não podem ser aplicados.

Conclui-se, portanto, que há uma tendência à centralidade do poder dos Estados, tanto na geopolítica convencional quanto nas relações entre os espaços tradicionais e o ciberespaço. Esta centralidade foi evidenciada no cenário de guerra atual, demonstrando que o Estado influencia a atuação dos atores não estatais no ciberespaço. Logo, se em algum momento acreditou-se que o conflito não ocuparia mais o espaço cinético, essa não é mais uma hipótese válida.

REFERÊNCIAS

ADLER, Emanuel. **O construtivismo no estudo das relações internacionais**. Lua Nova. N.47, 1999, p. 201-246.

ALMÄNG, Jan. War, vagueness, and hybrid war. **Defence Studies**, [S.L.], v. 19, n. 2, p. 189-204, 2 abr. 2019. Informa UK Limited. http://dx.doi.org/10.1080/14702436.2019.1597631.

AYRES PINTO, Danielle Jacon. **O smart power como um novo projeto de poder na esfera internacional: uma análise do Brasil e sua inserção internacional nos governos de Fernando Henrique Cardoso e Luiz Inácio Lula da Silva**. 2016. 1 recurso online (352 p.). Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Filosofia e Ciências Humanas, Campinas, SP. Disponível em: http://www.repositorio.unicamp.br/handle/REPOSIP/305057. Acesso em: 30 jul. 2021.

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, 2020.

BAEZNER, Marie; CORDEY, Sean. Influence Operations and Other Conflict Trends. In: DUNN CAVELTY, Myriam; WENGER, Andreas (ed.). **Cyber Security Politics**: socio-technological transformations and polical fragmentation. New York: Routledge, 2022. p. 17-31.

BHATT, Gita. **A Deeper Look at Forces Fragmenting Our World—and How to Respond**. 2022. Disponível em: https://blogs.imf.org/2022/06/02/a-more-fragmented-world/. Acesso em: 24 jun. 2022.

BIDEN, Joseph. National Security Strategy. **The White House**. 2022.

BIJOS, Leila; DE OLIVEIRA, Jackeline Nunes. A legitimidade da guerra nos Estados fracassados. **Revista do Mestrado em Direito da UCB**, v. 5, n. 2, 2011.

BILAL, Arsalan. **Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote**. NATO Review. 2021. Disponível em: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threatscomplexity-and-trust-as-the-antidote/index.html. Acesso em: 02 mai 2022.

CHOUCRI, Nazli; GOLDSMITH, Daniel. Lost in cyberspace: harnessing the internet, international relations, and global security. **Bulletin Of The Atomic Scientists**, [S.L.], v. 68, n. 2, p. 70-77, mar. 2012. Informa UK Limited. http://dx.doi.org/10.1177/0096340212438696.

CHUKWUERE, Joshua Ebere. Internet of Things (IoT) Cybersecurity Challenges and Mitigation Mechanisms. **Khazanah Sosial**, [S.L.], v. 4, n. 2, p. 235-240, 16 abr. 2022. Sunan Gunung Djati State Islamic University of Bandung. http://dx.doi.org/10.15575/ks.v4i2.17638.

CISCO. **O que é um roteador?** Disponível em: https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/networking/what-is-a-router.html. Acesso em: 15 abr. 2023a.

CISCO. **Understanding TCP/IP**. Disponível em: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/linked/tcpip.htm#:~:text=The%20name%20TCP%2FIP%20refers,the%20Internet%20Protocol%20(IP). Acesso em: 15 mar. 2023b.

CISCO. **What Is a LAN?** 2023. Disponível em: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html. Acesso em: 20 mar. 2023c.

CROWTHER, Glenn Alexander. The cyber domain. **The cyber defense review**, v. 2, n. 3, p. 63-78, 2017.

DEPARTMENT OF DEFENSE. **Joint Publication 1-02**: Department of Defense Dictionary of Military and Associated Terms. Washington, DC: Joint Chiefs of Staff, 2010.

DIAS, Cláudia Augusto. Hipertexto: evolução histórica e efeitos sociais. **Ciência da informação**, v. 28, p. 269-277, 1999.

DUNN CAVELTY, Myriam *et al*. STRATEGIC TREND 2015: Key Developments in Global Affairs. **Center for Security Studies**. 2015.

DUNN CAVELTY, Myriam; WENGER, Andreas. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. **Contemporary Security Policy**, v. 41, n. 1, p. 5-32, 2020.

ECKE, Michael. **Clausewitzian Cyber Strategy**. Tufts University, 2018.

EGLOFF, Florian**. Cybersecurity and non-state actors: a historical analogy with mercantile companies, privateers, and pirates.** 2018. Tese de Doutorado. University of Oxford.

EGLOFF, Florian J.; SMEETS, Max. Publicly attributing cyberattacks: a framework. **Journal Of Strategic Studies**, [S.L.], p. 1-32, 10 mar. 2021. Informa UK Limited. http://dx.doi.org/10.1080/01402390.2021.1895117.

ENAP. **Afinal, o que é um think tank e qual é a sua importância para políticas públicas no Brasil?** Disponível em: https://www.enap.gov.br/pt/acontece/noticias/afinal-o-que-e-um-think-tank-e-qual-e-a-sua-importancia-para-politicas-publicas-no-brasil. Acesso em: 11 jan. 2023.

EUROPE UNION. **Directive (EU) 2022/2555** of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Acesso em: 31 mai. 2023.

FERNANDES, H., 2016. As Novas Guerras: O Desafio da Guerra Híbrida. **Revista de Ciências Militares**, novembro de 2016 IV (2), p. 13-40.

FERREIRA, Marcos Alan S. V.; FRAMENTO, Rodrigo de Souza. Atores não-estatais violentos transnacionais na América do Sul. **Revista Brasileira de Segurança Pública**, [S.L.], v. 14, n. 1, p. 72-87, 10 nov. 2021. Revista Brasileira de Seguranca Publica. http://dx.doi.org/10.31060/rbsp.2020.v14.n1.1011.

FIERKE, Karin M. **Critical approaches to international security**. John Wiley & Sons, 2015.

FINNEMORE, Martha; SIKKINK, Kathryn. Taking stock: the constructivist research program in international relations and comparative politics. **Annual review of political science**, v. 4, n. 1, p. 391-416, 2001.

GALLAIS, Cecilia; FILIOL, Eric. Critical infrastructure: where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. **Journal of Information Warfare**, v. 16, n. 1, p. 64-87, 2017.

GE, Mouzhi; BANGUI, Hind; BUHNOVA, Barbora. Big data for internet of things: a survey. **Future generation computer systems**, v. 87, p. 601-614, 2018.

GLOWNIAK, Jerry. History, structure, and function of the Internet. In: **Seminars in nuclear medicine.** WB Saunders, 1998. p. 135-144.

GÓRKA, Marek. Cybersecurity Politics-Conceptualization of the Idea. **Polish Political Science Yearbook**, v. 50, p. 71-89, 2021.

HAATAJA, Samuli. The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. **Law, Innovation And Technology**, [S.L.], v. 9, n. 2, p. 159-189, 3 jul. 2017. Informa UK Limited. http://dx.doi.org/10.1080/17579961.2017.1377914.

HOWARD, Michael; PARET, Peter. Carl von Clausewitz. **On War**. 1989.

HURD, Ian. Constructivism. **The Oxford Handbook of International Relations**, [S.L.], p. 298-316, 2 set. 2009. Oxford University Press. http://dx.doi.org/10.1093/oxfordhb/9780199219322.003.0017.

IBM. **O que é ransomware?** Disponível em: https://www.ibm.com/br-pt/topics/ransomware. Acesso em: 11 jan. 2024.

IMF. International Monetary Fund. **Low Internet Access Driving Inequality**. 2020. Disponível em: https://www.imf.org/en/Blogs/Articles/2020/06/29/low-internet-access-driving-inequality. Acesso em: 01 mar. 2023.

INSTITUTE FOR STRATEGIC STUDIES. Strategic Trends 2012: Key Developments in Global Affairs. **Strategic Studies**. Londres: Routledge, 2012.

ISNARTI, Rika. A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. **Andalas Journal of International Studies** (AJIS), v. 5, n. 2, p. 151-165, 2016.

ITU. International Telecommunication Union. **Global Connectivity Report 2022**. Geneva, 2022a. Disponível em: https://www.itu.int/hub/publication/d-ind-global-01-2022/. Acesso em 28 fev. 2023.

ITU. International Telecommunication Union. **Harnessing IoT Global Development**. Geneva, 2016.

ITU. International Telecommunication Union. **Individuals using the Internet**. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Acesso em: 28 nov. 2022b.

ITU. International Telecommunication Union. **Mensuring digital development**: Facts and figures. Geneva, 2021.

JORDAN, Tim. **Cyberpower: the culture and politics of cyberspace and the Internet**. Routledge, 1999.

KHANDELWAL, Swati. **Hackers behind Dyre Malware Busted in Police Raid**. 2016. Disponível em: https://thehackernews.com/2016/02/hacking-dyre-malware.html. Acesso em: 15 jan. 2024.

KIM, Ji-Young. The impact of Internet use patterns on political engagement: A focus on online deliberation and virtual social capital. **Information Polity**, v. 11, n. 1, p. 35-49, 2006.

KUEHL, Dan. **From Cyberspace to Cyberpower: Defining the Problem**. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry Cyberpower and National Security. Washington, Estados Unidos: National Defense University Press, 2009.

KURBALIJA, Jovan. **Uma introdução à Governança da Internet**. Comitê Gestor da Internet no Brasil. Brasil, 2016.

LAYNE, Christopher. The Unipolar Illusion: Why Great Powers will Rise. **International Security**, v. 17, n. 4, pp. 5-51, 1993.

LIEBETRAU, Tobias; CHRISTENSEN, Kristoffer Kjærgaard. The ontological politics of cyber security: emerging agencies, actors, sites, and spaces. **European Journal Of International Security**, [S.L.], v. 6, n. 1, p. 25-43, 2 set. 2020. Cambridge University Press (CUP). http://dx.doi.org/10.1017/eis.2020.10.

MACHADO, Jussara O. **Ciberguerra: conceitos, doutrinas, estratégias, operações, instituições e o caso dos Estados Unidos**. 2014. 126 f. Dissertação (Mestrado em Relações Internacionais) - Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2014.

MARTINS, Marco. O espaço: uma nova realidade para a segurança internacional. **Idn – Nação e Defesa**, Lisboa, v. 1, n. 133, p. 32-49, abr. 2012. Quadrimestral. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD133/NeD133.pdf. Acesso em: 10 ago. 2021.

MAYER, Jane. **How Russia Helped Swing the Election for Trump**. 2018. Disponível em: https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump. Acesso em: 11 jan. 2024.

MAZARR, Michael J.; FREDERICK, Bryan; CRANE, Yvonne K.. Understanding a New Era of Strategic Competition. **RAND Corporation**. Santa Monica, California, 2022. Disponível em: https://www.rand.org/pubs/research_reports/RRA290-4.html. Acesso em: 12 jan. 2024.

MUNCASTER, Phil. **Dyre Trojan Silenced After Moscow Raid**. 2016. Disponível em: https://www.infosecurity-magazine.com/news/dyre-trojan-silenced-after-moscow/. Acesso em: 15 jan. 2024.

MURPHY, Dennis M. **Attack or defend? Leveraging information and balancing risk in cyberspace**. ARMY WAR COLL CARLISLE BARRACKS PA INFORMATION IN WARFARE WORKING GROUP, 2010.

NOGUEIRA, Carolina Dantas. Segurança internacional e os atores sociais. In: 3° ENCONTRO NACIONAL ABRI 2001, 3., 2011, São Paulo. **Anais online.** Associação Brasileira de Relações Internacionais Instituto de Relações Internacionais - USP, Disponível em: http://www.proceedings.scielo.br/scielo.php?script=sci_arttext&pid=MSC0000000122011000100046&lng=en&nrm=abn. Acesso em: 03 jan. 2024.

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

NYE JR., Joseph, **The future of Power**. Nova Iorque: PublicAffairs, 2011.

OLIVEIRA, Maria Engel de. **ORKUT: O Impacto da Realidade da Infidelidade Virtual**. 2007. 103 f. Dissertação (Mestrado) - Curso de Piscologia, Puc Rio, Rio de Janeiro, 2007.

OLIVEIRA, Nucia Alexandra Silva de. História e Internet: conexões possíveis. **Revista Tempo e Argumento**, [S.L.], v. 06, n. 12, p. 23-53, 30 ago. 2014. Universidade Estadual de Santa Catarina. http://dx.doi.org/10.5965/2175180306122014023.

ONUF, Nicholas Greenwood. **World of our Making**. Columbia: University of South Carolina Press, 1989.

PERNIK, Piret. The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In: POPESCU, Nicu; SECRIERU, Stanislav (ed.). **Hacks, leaks and disruptions**: russian cyber strategies. 148. ed. Paris: Chaillot Papers, 2018. Cap. 5. p. 53-64.

PETERS, Anne *et al*. (Ed.). **Non-state actors as standard setters**. Cambridge University Press, 2009.

PINGEN, Anna. **Legislation to Strengthen Cybersecurity Across the Union:**: nis 2 directive. NIS 2 Directive. Disponível em: https://eucrim.eu/news/legislation-to-

strengthen-cybersecurity-across-the-union-nis-2-directive/. Acesso em: 31 maio 2023.

QURESHI, Waseem Ahmad. Fourth-and fifth-generation warfare: Technology and perceptions. **San Diego Int'l LJ,** v. 21, p. 187, 2019.

RAND. **About RAND**. Disponível em: https://www.rand.org/about.html. Acesso em: 12 jan. 2024.

REITER, Dan. **Exploring the Bargaining Model of War**. Perspectives on Politics, v. 1, n. 1, p. 27-43, 2003.

RID, Thomas; MCBURNEY, Peter. Cyber-Weapons. **The Rusi Journal**, [S.L.], v. 157, n. 1, p. 6-13, fev. 2012. Informa UK Limited. http://dx.doi.org/10.1080/03071847.2012.664354.

RUOHONEN, Jukka. **Do cyber capabilities and cyber power incentive international cooperation? arXiv**, 17 nov. 2020. *Preprint*. Disponível em: arXiv:2011.07212. Acesso em: 20 jan. 2024.

SACHDEVA, Monika *et al*. DDos Incidents and their Impact: a review. **The International Arab Journal of Information Technology.** Índia, p. 14-22. jan. 2010.

SEGAL, Adam. **The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age**. Hachette UK, 2016.

SHALLCROSS, Nicholas J. Social media and information operations in the 21st century. **Journal of Information Warfare**, v. 16, n. 1, p. 1-12, 2017.

SHAREVSKI, Filipo; KESSELL, Benjamin. **Fight Fire with Fire**: Hacktivists' Take on Social Media Misinformation. Social and Information Networks. 15 fev. 2023. *Preprint.* Disponível em: https://arxiv.org/abs/2302.07788. Acesso em: 20 jan. 2024

SHLYAKHTUNOV, Mikhail A. White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies. **International Journal of Advanced Computer Science and Applications**, v. 12, n. 8, 2021.

ŠTRUCL, Damjan. Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. **Contemporary Military Challenges/Sodobni Vojaški Izzivi**, v. 24, n. 2, p. 103-123, 2022.

TALLMANN, Helena. **Por que a discriminação contra as mulheres na internet deve preocupar a todos nós**. Disponível em: https://www.openglobalrights.org/why-online-discrimination-against-women-should-concern-us-all/?lang=Portuguese. Acesso em: 16 abr. 2023.

THE MOSCOW TIMES. **Russia Jails Hacking Ringleader for 14 Years**. 2022. Disponível em: https://www.themoscowtimes.com/2022/02/15/russia-jails-hacking-ringleader-for-14-years-a76380. Acesso em: 15 jan. 2024.

TIKK, Eneken; KASKA, Kadri; VIHUL, Liis. **International cyber incidents: Legal considerations**. Cooperative Cyber Defence of Excellence (CCD COE), 2010.

TSAGOURIAS, Nicholas. Non-state actors, ungoverned spaces and international responsibility for cyber acts. **Journal of Conflict and Security Law**, v. 21, n. 3, p. 455-474, 2016.

TSAKANYAN, V.T.. The role of cybersecurity in world politics. **Вестник Рудн.** Moscow, v. 17, n. 2, p. 339-348, 2017.

TULGA, Ahmet Yigitalp. Constructivism, Identity, and Discourse in Terrorism. **Journal of Politics and Policy**, v. 4, n. 2, 2022.

U.S. DEPARTMENT OF HOMELAND SECURITY. **A Guide to Critical Infrastructure Security and Resilience**. November 2019. CISA. Disponível em: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf. Acesso em: 20 mar. 2023.

US DEPARTMENT OF HOMELAND SECURITY. **Privacy Impact Assessment Update for the Enhanced Cybersecurity Services (ECS)**. Office of Cybersecurity and Communications. Department of Homeland Security, 2015. Disponível em: https://www.dhs.gov/sites/default/files/publications/privacy-pia-28-a-nppd-ecs-november2015.pdf. Acesso em: 24 mai. 2023.

UN. United Nations. **ITU**: 2.9 billion people still offline. 2021.

US DEPARTMENT OF JUSTICE. **Organizing for computer crime investigation and prosecution**. Washington, DC: U.S. Department of Justice, 1989. Disponível em: https://www.ncjrs.gov/pdffiles1/Digitization/118216NCJRS.pdf. Acesso em: 06 mar. 2023.

VAN RENS, Dominick. **Patriotic hackers or russian cyberwarfare?Analyzing Russian cyberattacks in Estonia and Georgia** (74 p.). Tese (mestrado). Erasmus School of Social and Behavioural Sciences, 2019. Disponível em: https://thesis.eur.nl/pub/50757. Acesso em: 15 jan. 2024.

WALTZ, Kenneth N. **Theory of International Politics**. New York: McGraw-Hill, 1979.

WALTZ, Kenneth N. **The Origins of War in Neorealist Theory**. Journal of Interdisciplinary History. v. 18, n. 4, 615-628, 1988.

WEBSTER, Aaron A. **Leveraging Cyberspace in Counterinsurgency Operations**. ARMY WAR COLL CARLISLE BARRACKS PA, 2010.

WENDT, Alexander. **Collective Identity Formation and the International State**. American Political Science Review, vol. 88, nº 2, junho de 1994, p. 384–96. DOI.org (Crossref). http://dx.doi.org/10.2307/2944711.

WENDT, Alexander; ESTRADA, Rodrigo Duque. A anarquia é o que os Estados fazem dela: a construção social da política de poder. **Monções: Revista de Relações Internacionais da UFGD**, v. 2, n. 3, p. 420-473, 2013.

WENDT, Alexander. Social Theory of International Politics. **Cambridge Studies in International Relations**. Cambridge: Cambridge University Press, 1999.

WENDT, Alexander. Why a World State is Inevitable. **European Journal Of International Relations**, [S.L.], v. 9, n. 4, p. 491-542, dez. 2003. SAGE Publications. http://dx.doi.org/10.1177/1354066103940001.

WHYTE, Christopher. Beyond tit-for-tat in cyberspace: political warfare and lateral sources of escalation online. **European Journal Of International Security**, [S.L.], v. 5, n. 2, p. 195-214, 19 maio 2020. Cambridge University Press (CUP). http://dx.doi.org/10.1017/eis.2020.2.

WHYTE, Christopher. On the future of order in cyberspace. **Strategic Studies Quarterly**, v. 9, n. 2, p. 69-77, 2015.

WILNER, Alex s. Cybersecurity and its discontents: artificial intelligence, the internet of things, and digital misinformation. **International Journal**: Canada's Journal of Global Policy Analysis, [S.L.], v. 73, n. 2, p. 308-316, jun. 2018. SAGE Publications. http://dx.doi.org/10.1177/0020702018782496.

ZENDELOVSKI, Goran; CVETKOVSKI, Sergej. The Pandemic of Fake News and Disinformation in the Age of Deglobalization. **Security Dialogues**, Faculty Of Philosophy – Institute For Security, Defence And Peace, Skopje, v. 12, n. 2, p. 131-140, fev. 2021.

ZHOU, Ian *et al*. Internet of Things 2.0: concepts, applications, and future directions. **Ieee Access**, [S.L.], v. 9, p. 70961-71012, 2021. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2021.3078549.