Universidade do Estado do Pará

Centro de Ciências Naturais e Tecnologia
Curso de Bacharelado em Relações Internacionais
Trabalho de Conclusão de Curso

ISABELA DA NATIVIDADE VIANA

CIBERESPAÇO GLOBAL:

IMPLICAÇÕES PARA A SOBERANIA ESTATAL

BELÉM-PA

2024

ISABELA DA NATIVIDADE VIANA

CIBERESPAÇO GLOBAL:
IMPLICAÇÕES PARA A SOBERANIA ESTATAL

Trabalho de Conclusão de Curso de Graduação apresentado ao Centro de Ciências Naturais e Tecnologia da Universidade do estado do Pará como requisito para a obtenção do grau de Bacharelado em Relações Internacionais.

Orientador (a): Prof. Msc. José Cláudio Warken.

BELÉM-PA
2024

ISABELA DA NATIVIDADE VIANA

CIBERESPAÇO GLOBAL:
IMPLICAÇÕES PARA A SOBERANIA ESTATAL

Trabalho de Conclusão de Curso de Graduação apresentado ao Centro de Ciências Naturais e Tecnologia da Universidade do estado do Pará como requisito para a obtenção do grau de Bacharelado em Relações Internacionais.

Orientador (a): Prof. Msc. José Cláudio Warken.
Co-orientador (a): Prof. Msc. Alinne Flexa de Castro.

Banca Avaliadora:

Prof. Esp. Danielle Silva da Silva
Instituição: Universidade do Estado do Pará (UEPA)

Prof. Msc. Thainá Penha Baima Viana Corrêa Nunes Nogueira
Instituição: Universidade Federal de Uberlândia (UFU)

Apresentado em: 10/01/2024

BELÉM-PA
2024

RESUMO

VIANA, ISABELA DA NATIVIDADE. **CIBERESPAÇO GLOBAL:** IMPLICAÇÕES PARA A SOBERANIA ESTATAL. Orientador: José Claudio Walker. 2024. Trabalho de Conclusão de Curso (Relações Internacionais) – Universidade do Estado do Pará, Belém, 2024.

Resumo: Este trabalho apresenta uma análise das interações entre o espaço cibernético e as vulnerabilidades dos Estados, a fim de compreender como essa relação impacta a soberania estatal. O ciberespaço global constitui um ambiente digital conectado, transcendendo barreiras físicas e oferecendo uma liberdade virtual profundamente associada ao mundo real. Contudo, a descentralização inicial da internet e do ciberespaço gerou desafios de segurança. Esses desafios se manifestam especialmente por meio de ciberataques, expondo de forma significativa as vulnerabilidades dos Estados diante de outros atores nesse ambiente virtual. Assim, serão abordados em seções distintas: a conceituação da internet e do ciberespaço; a base teórica empregada na análise do ciberespaço, contemplando as correntes realista e neoliberal; a evolução do conceito de soberania; e por fim, sua nova configuração diante do advento do ciberespaço. A pesquisa é descritiva, adotando métodos dedutivos, abordagem interdisciplinar e natureza qualitativa. Em se tratando do procedimento técnico, faz-se o uso da pesquisa bibliográfica, utilizando-se dados secundários como livros, artigos científicos e dissertações. Dessa forma, conclui-se que a crescente independência das estruturas digitais torna os Estados mais vulneráveis a ataques cibernéticos, afetando diretamente sua soberania.

Palavras-chave: Cibersegurança. Soberania. Equilíbrio de Poder. Hard Power. Snowden. Stuxnet.

ABSTRACT

VIANA, ISABELA DA NATIVIDADE. **CIBERESPAÇO GLOBAL: IMPLICAÇÕES PARA A SOBERANIA ESTATAL.** Orientador: José Claudio Walker. 2024. Trabalho de Conclusão de Curso (Relações Internacionais) – Universidade do Estado do Pará, Belém, 2024.

Abstract: This paper presents an analysis of the interactions between cyberspace and the vulnerabilities of States, in order to understand how this relationship impacts state sovereignty. The global cyberspace constitutes a connected digital environment, transcending physical barriers and offering a virtual freedom deeply associated with the real world. However, the initial decentralization of the internet and cyberspace has created security challenges. These challenges are manifested especially through cyber-attacks, significantly exposing the vulnerabilities of states before other actors in this virtual environment. Thus, they will be addressed in different sections: the conceptualization of the internet and cyberspace; the theoretical basis used in the analysis of cyberspace, contemplating the realistic and neoliberal currents; the evolution of the concept of sovereignty; and finally, its new configuration before the advent of cyberspace. The research is descriptive, adopting deductive methods, interdisciplinary approach, and qualitative nature. In the case of the technical procedure, the bibliographic research is used, using secondary data such as books, scientific articles, and dissertations. Thus, it is concluded that the increasing independence of digital structures makes states more vulnerable to cyber-attacks, directly affecting their sovereignty.

Keywords: Cybersecurity. Sovereignty. Power Balance. Hard Power. Snowden. Stuxnet.

SUMÁRIO

CIBERESPAÇO GLOBAL:

IMPLICAÇÕES PARA A SOBERANIA ESTATAL

Isabela da Natividade Viana[1]

Msc. José Cláudio Warken[2]

Msc. Alinne Flexa de Castro[3]

Resumo: Este trabalho apresenta uma análise das interações entre o espaço cibernético e as vulnerabilidades dos Estados, a fim de compreender como essa relação impacta a soberania estatal. O ciberespaço global constitui um ambiente digital conectado, transcendendo barreiras físicas e oferecendo uma liberdade virtual profundamente associada ao mundo real. Contudo, a descentralização inicial da internet e do ciberespaço gerou desafios de segurança. Esses desafios se manifestam especialmente por meio de ciberataques, expondo de forma significativa as vulnerabilidades dos Estados diante de outros atores nesse ambiente virtual. Assim, serão abordados em seções distintas: a conceituação da internet e do ciberespaço; a base teórica empregada na análise do ciberespaço, contemplando as correntes realista e neoliberal; a evolução do conceito de soberania; e por fim, sua nova configuração diante do advento do ciberespaço. A pesquisa é descritiva, adotando métodos dedutivos, abordagem interdisciplinar e natureza qualitativa. Em se tratando do procedimento técnico, faz-se o uso da pesquisa bibliográfica, utilizando-se dados secundários como livros, artigos científicos e dissertações. Dessa forma, conclui-se que a crescente independência das estruturas digitais torna os Estados mais vulneráveis a ataques cibernéticos, afetando diretamente sua soberania.

Palavras-chave: Cibersegurança. Soberania. Equilíbrio de Poder. Hard Power. Snowden; Stuxnet.

Abstract: This paper presents an analysis of the interactions between cyberspace and the vulnerabilities of States, to understand how this relationship impacts state sovereignty. The global cyberspace constitutes a connected digital environment, transcending physical barriers and offering a virtual freedom deeply associated with the real world. However, the initial decentralization of the internet and cyberspace has created security challenges. These challenges are manifested especially through cyber-attacks, significantly exposing the vulnerabilities of states before other actors in this virtual environment. Thus, they will be addressed in different sections: the conceptualization of the internet and cyberspace; the theoretical basis used in the analysis of cyberspace, contemplating the realistic and neoliberal currents; the evolution of the concept of sovereignty; and finally, its new configuration before the advent of cyberspace. The research is descriptive, adopting deductive methods, interdisciplinary approach, and qualitative nature. In the case of the technical procedure, the bibliographic research is used, using secondary data such as books, scientific articles, and dissertations. Thus, it is concluded that the increasing independence of digital structures makes states more vulnerable to cyber-attacks, directly affecting their sovereignty.

Keywords: Cybersecurit. Sovereignty. Power Balance. Hard Power. Snowden. Stuxnet.

[1]AUTORA - Bacharela em Relações Internacionais da Universidade do Estado do Pará (2024). Tv. Dr. Enéas Pinheiro, 2626, Marco, Belém - PA. CEP: 66095-015. E-mail: isabelaviana02@gmail.com

[2]ORIENTADOR - Mestre em Ciência Política por meio da Universidade Federal do Pará (2015). E-mail: jose.warken@uepa.br

[3]COORIENTADORA - Mestre em Estudos Estratégicos da Defesa e da Segurança por meio da Universidade Federal Fluminense (2022) e em Segurança Internacional e Defesa, pela Escola Superior de Guerra (2021). E-mail: alinnecastro@id.uff.br

1. INTRODUÇÃO

Os avanços da revolução da informação têm permeado todos os âmbitos do conhecimento, moldando a dinâmica social e influenciando as estruturas governamentais. Esse processo revolucionário impulsionou significativos progressos tecnológicos na computação, resultando na diminuição dos custos relativos à produção, transmissão e processamento de informações (Nye, 2010, *apud* Maier, 2016).

Nesse contexto, entre as décadas de 1970 e 1990, emergiram e se disseminaram mundialmente novas tecnologias da informação, sobretudo a internet. Esse avanço tecnológico expandiu-se de forma exponencial, transformando-se em uma ferramenta de uso militar, acadêmico e, mais importante, social, conectando globalmente as pessoas por meio da tecnologia da informação (Rê, 2021). Assim, as ferramentas tecnológicas estão cada vez mais inseridas na dinâmica dos atores internacionais e na sociedade em geral, estabelecendo um novo paradigma no qual o virtual se tornou essencial para a humanidade e o ciberespaço, uma nova realidade (Serrano, 2022).

Nessa nova realidade, a ascensão da globalização reconfigurou a noção e a aplicação da soberania. Esse fenômeno, ao diluir as fronteiras territoriais por onde a informação se difunde globalmente, desafia a aplicação tradicional do poder soberano. A interação entre indivíduos de diferentes nacionalidades enfraquece os limites dos Estados, dificultando a execução da soberania convencional, cuja delimitação é afetada por essa mudança (Mansur; Rocha, 2019).

O surgimento do ciberespaço amplia ainda mais essas questões acerca da soberania, sendo ele caracterizado como um campo virtual que seria composto pelos computadores e usuários que se conectam diariamente e interagiriam entre si, em uma rede mundial (Gibson, 1984). Esse ambiente, de natureza tecnológica, transcende as fronteiras convencionais, escapando às amarras físicas e políticas que determinam a autoridade de um Estado sobre territórios específicos. Surge então um espaço de fronteiras invisíveis, gerando uma reconfiguração nos conceitos clássicos de poder, domínio territorial e soberania (Rê, 2021).

Como resultado deste cenário, há o surgimento de novos tipos de vulnerabilidades do espaço cibernético, que são exploradas por todo tipo de atores, podendo ser bem ou mal-intencionados (Castro, 2020). De acordo com Galvão (2018), essas vulnerabilidades do Ciberespaço estão intrinsecamente ligadas às novas capacidades de poder provenientes dos instrumentos tecnológicos, dinâmica a qual propicia o aumento das ameaças cibernéticas, visto

que possibilita e intensifica as interferências estatais tanto na política externa quanto na segurança de diferentes nações.

Como consequência, as relações internacionais no ciberespaço se tornaram mais complexas. A ocorrência de grandes incidentes cibernéticos, validaram o sentimento de insegurança das nações (Rê, 2021), exemplificados no presente artigo com o caso *stuxnet* e o caso *snowden*. Esses eventos ilustram a conexão entre as vulnerabilidades no ambiente cibernético e a soberania nacional, representando, respectivamente, o primeiro incidente cibernético com impactos físicos e as práticas de espionagem dos Estados Unidos em escala global, afetando cidadãos, governos e empresas. Dessa forma, a complexidade presente no ciberespaço levanta questionamentos cruciais sobre a segurança e política internacionais. À vista disso, o presente trabalho de pesquisa está relacionado à linha de pesquisa da Segurança Internacional, Estudos da Paz e Defesa Nacional.

Esta pesquisa possui o objetivo geral analisar as interações entre o espaço cibernético e as vulnerabilidades dos Estados, e os objetivos específicos são: 1) Conceituar a internet e o ciberespaço. 2) Compreender o ciberespaço e suas vulnerabilidades a partir da teoria realista e neoliberal. 3) Compreender a evolução do conceito de soberania. 4) Analisar como a soberania tradicional é impactada pelo ciberespaço. Os objetivos estão alinhados para responder à seguinte pergunta: “Como o espaço cibernético amplifica as vulnerabilidades e de que maneira elas impactam a soberania dos Estados?”.

Por conseguinte, a pergunta desperta a hipótese de que a crescente independência e a complexidade das infraestruturas digitais aumentam as vulnerabilidades dos Estados a ataques cibernéticos, enfraquecendo a sua capacidade de exercer controle sobre seu “território” no campo virtual. Isso sugere que a amplificação das vulnerabilidades no ciberespaço impacta diretamente a soberania dos Estados, minando sua autoridade e controle sobre questões de segurança e política.

A relevância deste trabalho reside na sua abordagem de um tema crucial e contemporâneo: o impacto da revolução da informação, especialmente com a ascensão do ciberespaço, na reconfiguração da soberania estatal e nas relações internacionais. Os entornos da sociedade da informação são fenômenos recentes na sociedade moderna, tendo pouco mais de três décadas de existência. Dessa forma, apesar do rápido crescimento e disseminação global, ainda estamos nos estágios iniciais de compreensão de todos os reflexos e implicações desses avanços na conjuntura atual.

Essa dinâmica transformadora desafia noções profundamente enraizadas sobre o exercício do poder e a autoridade dos Estados, num contexto que ultrapassa as barreiras físicas e desafia a aplicação tradicional da soberania. As complexidades emergentes e as consequências dessa mudança são áreas de estudo cruciais para compreendermos e nos adaptarmos a uma era em constante evolução, onde a tecnologia molda significativamente o curso das relações globais.

Esta pesquisa adota uma abordagem descritiva para estabelecer relações entre as variáveis fundamentais do estudo; o ambiente cibernético e a soberania (Gil, 2002). Com uma natureza qualitativa, a análise baseia-se na interpretação de dados objetivos em conjunto com as teorias utilizadas, conforme Marconi e Lakatos (2003). Quanto ao método empregado, optou-se pela pesquisa bibliográfica, conceituada por Gil (2002) como aquela que se fundamenta em materiais já existentes, como livros, artigos científicos, publicações periódicas e relatórios. Dessa forma, para a construção da revisão de literatura do presente trabalho foram utilizados artigos, livros e dissertações que desenvolvem acerca das questões do ciberespaço, segurança cibernética, revolução informacional, soberania e os eventos ocorridos em 2013 de Edward Snowden e em 2010, com o caso *stuxnet*, sob viés conceitual, teórico e descritivo.

Por fim, conclui-se que o aumento da autonomia das infraestruturas digitais expõe os Estados a ataques cibernéticos, resultando em um impacto direto sobre a sua soberania. Isso porque, a habilidade de conduzir operações cibernéticas invasivas compromete a autonomia de uma nação, influenciando negativamente sua independência na tomada de decisões. Consequentemente, tais ataques não apenas representam ameaças à segurança, mas também abalam a autoridade e a governança de um Estado, tanto em âmbito interno quanto externo.

2. REVISÃO BIBLIOGRÁFICA

Neste segmento da pesquisa, buscando compreender as interações entre o espaço cibernético e as vulnerabilidades dos Estados, serão abordados primeiramente os conceitos de Internet e Ciberespaço, juntamente com o contexto em que ambos surgiram. Em seguida, serão examinadas as vulnerabilidades presentes nesse espaço cibernético, a partir da análise sistêmica do ciberespaço e da concepção de poder, delineados pela teoria realista e neoliberalista, respectivamente. Posteriormente, será explorada a questão da soberania, delineando a evolução do conceito desde uma perspectiva tradicional. Para concluir o arcabouço teórico, será analisada a soberania moderna, caracterizada pelas transformações decorrentes da globalização e do surgimento do ciberespaço.

2.1. Conceitualização da internet e do ciberespaço

Joseph Nye Jr. analisou a revolução da informação, descrevendo-a como a transição do pensamento "rico em poder" para "rico em informação", ressaltando a centralidade da informação como uma forma de poder. Além disso, Nye Jr. também discorre que a atual revolução da informação se baseia nos rápidos avanços tecnológicos em computadores, comunicações e softwares (Nye, 2010 apud Maier, 2016).

Desse modo, o que diferencia a presente revolução da informação das demais seriam as novas tecnologias da informação que se difundiram pelo mundo. De acordo com Castells (1999), estas novas ferramentas seriam para a terceira revolução, o que as novas fontes de energia foram para as revoluções industriais, tendo em vista que a distribuição de energia foi o elemento base para a sociedade industrial.

A revolução teve ligação, ainda, com o período da Guerra Fria, ocorrida entre 1947 e 1991, entre os Estados Unidos e União Soviética. Esse foi um momento de intensa competição, com a disposição de uma corrida armamentista e tecnológica entre as duas maiores potências mundiais da época. Esse embate foi responsável pelo grande desenvolvimento de equipamentos que contribuíram para o domínio político, militar e econômico de uma potência sobre a outra (Rê, 2021).

É neste contexto que surge a internet. Suas origens remontam ao projeto ARPANET, correspondente a uma rede de computadores montada pela agência estadunidense Advanced Research Projects Agency (ARPA) no ano de 1969. Criado pelo Departamento de Defesa dos Estados Unidos, o projeto tinha como objetivo alocar recursos de pesquisa com o propósito de conquistar uma vantagem tecnológica militar sobre a União Soviética (Castells, 2003).

Dessa forma, a criação da Internet foi resultado de uma convergência singular entre estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural (Castells, 1999). Essa fusão de elementos diversos não só deu origem à internet, mas também impulsionou sua expansão global exponencial, conectando o mundo através da tecnologia da informação.

Entretanto, embora sua formulação inicial tenha ocorrido no período da Guerra Fria, a internet global atual reflete as transformações dos anos 1990. Esse foi um período marcado pela supremacia global dos Estados Unidos após o declínio da União Soviética e antes da ascensão da China como potência mundial. Nesse contexto, compreende-se que a internet é uma instituição internacional que espelha o equilíbrio geopolítico de poder do momento de sua

criação, visto que a cultura e estrutura da internet refletiram este período de hegemonia estadunidense (Riordan, 2019).

No que se refere à conceituação da internet, é inegável a sua relação com aspectos técnicos, definidos por Gatto (2008, p. 57) como "a rede entre computadores que adota protocolos-padrão, essencialmente o TCP-IP, para transmissão de dados via pacote". Contudo, além desses aspectos técnicos, os fatores sociais, jurídicos, econômicos e culturais também desempenham papéis fundamentais nessa estrutura informacional.

Dentro desse contexto, emerge o conceito de "ciberespaço", um termo controverso e com diversas definições. Bauman (1999) aponta que, com as evoluções tecnológicas, as barreiras físicas deixam de ser um fator limitante da realidade, uma vez que há o surgimento da intitulada "nova liberdade", corporificada no "ciberespaço": um campo eletronicamente sustentado no qual os corpos não interessam, embora ele seja determinante para a vida dos corpos.

A origem do termo "ciberespaço" remonta a William Gibson, em sua obra "Neuromancer" de 1984, onde o autor descreve uma narrativa envolvendo interações homem/máquina em um mundo transformado por avanços tecnológicos e científicos. Esse ambiente virtual, segundo Gibson, é o local onde os indivíduos se conectam diariamente entre si. Em linhas gerais, Riordan (2019) descreve o ambiente cibernético como um espaço paralelo ao físico, porém intimamente relacionado, onde informações e equipamentos digitais interagem entre si.

A infraestrutura do ciberespaço transcende o ambiente virtual, ancorando-se no mundo físico, onde os usuários exercem controle sobre as tecnologias. Conforme expresso por Castells (1999, p. 69), "computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana". O ciberespaço, composto por informações e dispositivos digitais concebidos e desenvolvidos por seres humanos, é uma criação humana. Suas configurações e funcionamentos são determinados por decisões humanas, sejam elas de atores estatais ou não estatais. Nesse contexto, o espaço virtual se expande e evolui a cada novo dispositivo ou aplicativo digital, estabelecendo uma relação em que as ações no ciberespaço têm o potencial de influenciar o ambiente físico e vice-versa (Riordan, 2019).

Ademais, questões fundamentais ligadas às origens da internet e, consequentemente, do ciberespaço, emergem. Segundo Clarke e Knake (2010), os primeiros formuladores não visavam um controle governamental da internet, mas um sistema mais focado na

descentralização do que na segurança. Essa abordagem não apenas permitiu a expansão da rede, mas também perpetuou desafios e vulnerabilidades na área de segurança.

2.2. Realismo e Neoliberalismo: Abordagens ao ciberespaço

Para atingir o objetivo do estudo proposto e oferecer respostas à questão de pesquisa, é crucial revisitar os fundamentos e conceitos da escola realista na teoria das relações internacionais. Segundo Morgenthau (2003), a teoria realista é fundamentada em uma abordagem empírica, pragmática e objetiva dos fatos, enfatizando o Estado como o principal ator das dinâmicas internacionais. Seu propósito é conferir significado e estrutura a uma série de fenômenos que, sem essa teoria, permaneceriam desconexos e incompreensíveis.

Em suma, o realismo clássico delineado por Morgenthau se concentra nas relações competitivas e conflituosas entre Estados, onde a prioridade principal é assegurar a própria segurança. Nesse contexto, os Estados atuam primordialmente em prol de seus interesses nacionais, buscando obter poder, frequentemente definido em termos de capacidade militar, e impondo sua vontade sobre Estados considerados mais vulneráveis (Morgenthau, 2003).

Esse princípio destaca que as interações entre as nações têm sido historicamente moldadas pelo chamado “interesse definido em termos de poder” que, em sua essência, está em conformidade com as intenções políticas, a fim de atender às necessidades nacionais e consolidar influência. Desse modo, de acordo com o autor “A política internacional, como toda política, consiste em uma luta pelo poder. Sejam quais forem os fins da política internacional, o poder constitui sempre o objetivo imediato” (Morgenthau, 2003, p. 49).

Dessa forma, para que seja compreensível a relação entre os Estados, é crucial analisar a dinâmica do equilíbrio de poder presente no cenário anárquico do sistema internacional, onde os atores atuam como entidades soberanas e independentes. De acordo com o autor: “A aspiração de poder por parte de várias nações, em que cada uma tenta manter ou alterar o status quo, leva necessariamente a uma configuração que é chamada de equilíbrio de poder, bem como a políticas que se destinam a preservar esse equilíbrio” (Morgenthau, 2003, p. 321).

Nesse contexto, o equilíbrio de poder e as políticas traçadas para mantê-lo não são apenas inevitáveis, mas também desempenham um papel crucial na estabilidade de uma sociedade composta por nações soberanas. Assim, todas as formas de equilíbrio se baseiam em duas premissas fundamentais: primeiro, que os elementos a serem equilibrados são essenciais para a sociedade ou têm o direito de existir; segundo, que na ausência de um estado de equilíbrio

entre esses elementos, um deles poderá prevalecer sobre os demais, desrespeitando seus interesses e direitos e, por fim, levando à sua destruição (Morgenthau, 2003).

Portanto, o propósito de todas essas formas de equilíbrio reside em preservar a estabilidade do sistema sem comprometer a diversidade e a integridade de seus elementos constituintes, impedindo que um deles se sobreponha aos demais. Assim, a existência de um equilíbrio se fez essencial para a manutenção da interdependência dos Estados. Contudo, essa estrutura de equilíbrio de poder e interdependência não foi capaz de eliminar a intervenção das externalidades ou das nações nos assuntos e interesses uns dos outros. Dessa forma, evidencia-se a presença de lacunas e vulnerabilidades na balança de poder (Morgenthau, 2003).

Sendo assim, é essencial examinar o equilíbrio de poder no contexto anárquico do sistema internacional. Dentro de suas fronteiras, os Estados detêm soberania, exercendo o monopólio da força e a autoridade máxima para aplicar leis e assegurar a segurança interna. No âmbito internacional, porém, não existe uma autoridade suprema à qual os Estados estejam subordinados. Esse cenário de ausência de poder central é conhecido como anarquia. (Morgenthau, 2003).

Isso permite a comparação com o ambiente anárquico do ciberespaço, possibilitando examinar paralelos quanto ao equilíbrio de poder e sua atuação neste domínio virtual de estrutura intangível. Nesse contexto, as vulnerabilidades estão intrinsecamente relacionadas às novas capacidades de poder provenientes dos avanços tecnológicos. Assim, a interligação entre vulnerabilidades e poder tecnológico amplia o potencial das ameaças cibernéticas para interferir significativamente nas políticas externas e na segurança de outras nações (Galvão, 2018).

Assim, à medida que as tecnologias evoluem, essas vulnerabilidades não apenas aumentam, mas também proporcionam meios mais sofisticados para ações de interferência por parte dos Estados, ampliando as possíveis repercussões e complexidades nas dinâmicas internacionais (Galvão, 2018). Isso evidencia a existência de lacunas e vulnerabilidades no equilíbrio de poder presente no ambiente virtual, de forma semelhante ao sistema internacional, porém acentuadas pelo poder tecnológico.

Considerando este novo contexto de ação, a dinâmica da balança de poder sofre uma alteração direta. Agora, a hegemonia no sistema internacional não é apenas medida pela capacidade militar, como propõe o realismo, ou pela potencialidade econômica. Ela passa a ser avaliada também pela posse de conhecimento e pelo avanço tecnológico dos Estados. Assim, a definição de poder e seus elementos se tornam igualmente essenciais ao discutir as questões de segurança e defesa internacionais (Galvão, 2018).

Nesse contexto, embora o realismo ofereça contribuições valiosas para uma avaliação sistêmica do ciberespaço, suas limitações são evidentes, uma vez que essa abordagem negligencia outros atores que desempenham papéis significativos na estrutura internacional. Organizações, empresas, instituições e indivíduos são minimizados, enquanto os Estados continuam enfatizados como os principais protagonistas das dinâmicas internacionais (Eriksson;Giacomello, 2006 apud Galvão, 2018).

O liberalismo, por outro lado, evidencia a influência dos atores domésticos nas ações dos Estados no âmbito internacional. A corrente admite desafios que vão além das questões oriundas da anarquia no âmbito internacional e, embora concorde com os realistas quanto à primazia dos Estados, o liberalismo reconhece a importância dos atores não-estatais na política internacional, observando o crescimento em quantidade e a capacidade de projeção de poder desses atores por meio da revolução da informação (Eriksson & Giacomello, 2006 *apud* Nye Jr., 2002 *apud* Galvão, 2018). Dessa forma, os próximos esclarecimentos se apoiarão principalmente no embasamento teórico fornecido por Joseph Nye Jr.

O ciberespaço se estabeleceu como um novo domínio significativo para a projeção e exercício de poder na política internacional. Essa ascensão trouxe uma série de incertezas quanto ao modo como o poder é exercido nesse novo espaço e, em particular, como ele influencia a segurança global e as relações entre os países (Rê, 2021).

Esse surgimento tem gerado uma série de ameaças de alcance global, como apontado pela União Internacional de Telecomunicações (UIT) em 2008, abrangendo sabotagem, vandalismo, negação de serviço, espionagem e outras violações. Tais ameaças evidenciam a potencial instabilidade decorrente de ataques cibernéticos ou do uso inadequado do ambiente virtual, impactando tanto a segurança nacional quanto a internacional (Rê, 2021).

As vulnerabilidades no ciberespaço, conforme apontado por Mandarino (2010), estão associadas aos princípios fundamentais que devem reger a informação, como confidencialidade, integridade, disponibilidade e autenticidade. Assim sendo, para abordar essas vulnerabilidades presentes no ciberespaço e potencializadas por ele, é indispensável versar acerca da definição de poder e seus aspectos.

Segundo Nye (2004), o poder se refere à posse de capacidades ou recursos que têm o potencial para influenciar ganhos nacionais, abarcando aspectos econômicos e sociais. Contudo, a posse desses recursos não garante necessariamente vantagens, visto que o poder é relativo e dinâmico. Dessa forma, é a maneira como essas habilidades serão utilizadas que determinará as vantagens ou desvantagens, no âmbito nacional e internacional.

Nesse sentido, destaca-se a influência no comportamento dos indivíduos. De acordo com Nye (2004), o poder pode se manifestar de diversas formas, inclusive sob forma de controle e coerção. Esse aspecto envolve a imposição de regras, nas quais o descumprimento pode acarretar punições através da força e da violência, caracterizando o que o autor denomina de "Hard Power".

Dessa forma, as características singulares do ciberespaço possibilitam diversas formas de gerar Hard Power no ciberespaço, resultando na amplificação das vulnerabilidades. Por meio de ciberataques, emergem amplas categorias, como a ciberguerra, ciberterrorismo, ciberespionagem e cibercrime. Esses conceitos se assemelham, pois compartilham a característica essencial de atacar sistemas e servidores de internet. A diferenciação, no entanto, reside na natureza do ataque (Riordan, 2019).

Na guerra cibernética, atores estatais visam computadores estrangeiros, buscando danificar sistemas para gerar efeitos no mundo físico ou preparar terreno para futuros ataques. Já no ciberterrorismo, grupos não estatais interrompem sistemas computacionais com o intuito de causar danos ou gerar impactos no mundo real (Riordan, 2019).

Já no cibercrime, criminosos invadem sistemas para obter ganhos financeiros ilegais, que variam desde roubo direto até extorsão de informações para chantagear empresas ou solicitar resgates. Por fim, na ciberespionagem, tanto atores estatais quanto não estatais penetram nos sistemas para roubar informações, abrangendo desde dados pessoais até propriedade intelectual e informações sobre capacidades e intenções (Riordan, 2019).

Além disso, faz-se importante pontuar o poder dentro do ciberespaço. Nesse novo panorama, surge o chamado poder cibernético, definido como a capacidade de controlar ou dominar os recursos existentes no ambiente digital com um propósito específico. Esse poder não é apenas derivado do Estado e de seus interesses nacionais, mas também de outros atores, sejam eles civis, organizações ou empresas (Nye, 2010).

Entretanto, os Estados e seus governos continuam mantendo uma influência predominante tanto no cenário internacional quanto no virtual. Essa predominância dos atores estatais é resultado do controle territorial, da infraestrutura interna e dos maiores recursos financeiros disponíveis, elementos cruciais para sustentar a soberania estatal no ciberespaço. Entretanto, apesar da considerável capacidade de influência, os Estados também enfrentam vulnerabilidades devido à sua natureza híbrida, uma vez que esse ambiente virtual tem suas bases vinculadas a territórios físicos (Nye, 2010).

Nesse sentido, Nye (2010) enfatiza que os objetivos, vantagens e influências decorrentes do poder cibernético podem ocorrer tanto na camada física quanto na camada virtual desse espaço. Isso implica que ataques na camada física, como o bombardeamento de cabos e servidores, podem ter impactos na camada virtual, assim como ataques originados do ambiente interno do ciberespaço podem causar danos materiais na camada física.

Além disso, Nye (2012) destaca ainda que os custos para se operar no espaço cibernético são baixos. Essa acessibilidade, aliada à possibilidade de permanecer anônimo, faz com que diferentes atores possam utilizar esse domínio para alcançar seus objetivos, facilitando-se assim ataques diretos aos Estados. Nesse sentido, o desafio relacionado à atribuição se dá devido à alta complexidade e imprecisão do espaço cibernético, o que torna difícil identificar os responsáveis por um ciberataque.

Desse modo, tal dificuldade pode levar à construção de desconfianças entre os atores no campo internacional e a uma divisão entre grandes e pequenos poderes no ciberespaço, resultando em potenciais instabilidades globais (Nye, 2017). Dessa forma, o ciberespaço se torna um ambiente no qual as vulnerabilidades dos Estados são expostas significativamente, seja perante outras nações, empresas, organizações não governamentais, opinião pública ou até mesmo indivíduos (Portela, 2018).

2.3. A Evolução do Conceito de Soberania

Para melhor compreender sobre a soberania até a sua mais recente crise com a emergência do espaço cibernético, é essencial desenvolver primeiramente acerca da evolução e construção do seu conceito tradicional e os contextos que a moldaram com o passar das décadas. A soberania clássica teve seus primeiros esboços traçados por Jean Bodin (1530-1596), figura crucial no estabelecimento dos alicerces da soberania. O francês compreendia que a soberania se tratava do poder permanente e absoluto do soberano em promulgar leis, estando suas ações restritas apenas pelas leis naturais e divinas (Gatto, 2008).

Todavia, a consolidação histórica e diplomática do conceito de soberania adquiriu forma apenas em 1648, através dos Tratados de Vestfália. Além de encerrar a Guerra dos Trinta Anos[4] entre as potências europeias, esses tratados reconheceram a legitimidade e a autoridade dos

[4]A Guerra dos Trinta Anos (1618-1648) começou como uma guerra civil na Alemanha entre regiões pró e contra o poder imperial, mas logo se tornou um conflito internacional. Católicos, liderados pelos Habsburgos e apoiados pela Espanha, confrontaram uma coalizão protestante formada por estados alemães, Holanda, Dinamarca, Suécia e até mesmo a França católica.

Estados sobre seus territórios, configurando um marco simbólico que sinalizou o avanço progressivo da soberania territorial (Nunes, 2001).

Após isso, foram registradas influências de diferentes correntes de pensamento, como o iluminismo, quando o poder monárquico foi contestado. Dessa forma, após o século XVIII, houve uma alteração na concepção de soberania, influenciada pela Revolução Francesa (1789)[5], com o pensamento de Jean-Jacques Rousseau. Segundo sua visão, a soberania é popular ou nacional, pertencendo ao povo, compreendido como um corpo político ou comunidade de cidadãos. A soberania é considerada inalienável e indivisível, devendo ser exercida por meio da vontade geral (Martins, 2014).

Posteriormente, uma nova transformação no conceito de soberania ocorreu em decorrência da Primeira Guerra Mundial[6] (1914-1918), levando-a do antigo sistema westfaliano, centrado no uso da força e na soberania política, para um novo sistema legal fundamentado na sistematização normativa e no conceito de soberania jurídica. Essa reconfiguração é evidenciada no Pacto da Sociedade das Nações de 1919, o qual estabeleceu a soberania como princípio da não-intervenção em assuntos domésticos dos países envolvidos (Mansur; Rocha, 2019).

Na Segunda Guerra Mundial[7] (1939-1945), entretanto, foram implementados esforços para extinguir o Pacto da Sociedade das Nações de 1919, o que culminou na fundação da Organização das Nações Unidas (ONU) em 1945. Com o estabelecimento da ONU, não apenas houve uma reiteração do princípio de não intervenção nos assuntos internos dos Estados, mas também houve o reconhecimento mais enfático da igualdade entre as nações no que diz respeito a sua soberania (Mansur; Rocha, 2019).

Sendo assim, segundo Mansur e Rocha (2019), a concepção tradicional de soberania é caracterizada por ser um poder coercitivo, exclusivo, constante e inerente ao Estado. Este poder

[5]A Revolução Francesa (1789-1799), um período intenso de agitação política e social na França, foi marcado pelo fim dos privilégios da aristocracia e do Antigo Regime. A monarquia absolutista que havia governado por séculos entrou em colapso em um curto período de três anos.

[6]A Primeira Guerra Mundial (1914-1918), também chamada de a Grande Guerra, foi um conflito bélico de ordem global centrado na Europa, entre os países da Tríplice Aliança e a Tríplice Entente, sendo esta última a vitoriosa. A Tríplice Aliança foi formada pela Alemanha, Áustria-Hungria e Itália, e a Tríplice Entente, por França, Inglaterra e Rússia.

[7]A Segunda Guerra Mundial (1939-1945) foi um conflito militar global que envolveu a maioria das nações do mundo, incluindo potências globais, alinhadas em duas alianças opostas: os Aliados, representados por países como Reino Unido, França, EUA e URSS, e o Eixo, liderado por nações como Itália, Alemanha e Japão. Nesse período de "guerra total", os países envolvidos concentraram todos os recursos econômicos, industriais e científicos em esforços bélicos, dissolvendo a fronteira entre recursos civis e militares.

é incumbido da tarefa de estabelecer uma ordem jurídica específica em um território delimitado, habitado por uma determinada população.

Essa soberania é considerada única e indivisível, impossível de ser transferida a terceiros, pois não existe na ausência do Estado. Ademais, essa capacidade de imposição interna é reconhecida e respeitada globalmente, não havendo nenhuma autoridade superior que sobreponha a soberania estatal, visto que ela um fator sociojurídico-político, a qual se relaciona com a autonomia das nações (Mansur; Rocha, 2019).

2.4. A Soberania no Ciberespaço

O advento da globalização trouxe modificações ao entendimento da soberania e aplicação do poder soberano. Isso porque a globalização é um processo que enfraquece os limites estatais, ao romper as fronteiras territoriais por onde a informação é transmitida pelo globo, possibilitando o contato entre indivíduos de diferentes nacionalidades e desafiando assim a aplicação da soberania tradicional, que tem a sua delimitação prejudicada (Mansur; Rocha, 2019).

A chegada do ciberespaço amplia ainda mais essa questão. Este ambiente, por sua natureza tecnológica, não se encaixa nas noções convencionais de fronteiras físicas e políticas em que um Estado exerce controle e autoridade estatal sobre uma região específica com limites definidos. Ao invés disso, esse cenário digital se estabelece como um espaço com fronteiras invisíveis. Dessa forma, “Essa natureza transfronteiriça faz com que emerjam novas percepções em relação a conceitos tradicionais de dimensões de poder, domínio territorial e soberania" (Rê, 2021).

Entretanto, embora o ciberespaço seja uma realidade abstrata, ele tem sua existência intrinsecamente ligada aos servidores localizados em espaços físicos, tornando-o uma entidade que não pode ser considerada exclusivamente virtual ou imaterial. Isso estabelece uma conexão vital entre o mundo virtual e a presença física dessas estruturas. Portanto, o controle desses servidores por parte de um país específico transcende a esfera tecnológica, tornando-se também uma pauta significativa no contexto das relações entre Estados, visto que pode ser interpretado como uma questão de soberania nacional (Khanna, 2018).

Nesse sentido, governos mal-intencionados e entidades têm explorado o domínio cibernético para atacar a infraestrutura global e ativos cibernéticos críticos. Essas ações podem resultar na interrupção de funções governamentais, perdas financeiras e até na destruição de

propriedades e equipamentos de defesa estratégicos. Ademais, podem gerar perdas de vidas humanas, destacando a seriedade desses ataques (Khanna, 2018).

Assim, revela-se a vulnerabilidade de uma sociedade interligada na era digital diante das ameaças cibernéticas, que, devido à sua abrangência multissetorial, podem afetar várias esferas de atuação, impactando um ou mais Estados. Isso se deve ao fato de que suas infraestruturas críticas, como sistemas de saúde, energia, instituições financeiras, abastecimento de água e portais de serviços públicos, entre outros, também operam no ciberespaço. Se sujeitas a ataques ou paralisações, os danos seriam severos e abrangeriam diversas áreas da sociedade (Rocha, 2022).

A pluralidade evidenciada pelo trecho demonstra a seriedade com que o assunto deve ser tratado pelos Estados. Os ataques cibernéticos têm o potencial de afetar a soberania estatal, visto que compromete a capacidade do país em assegurar a segurança, proteger interesses estratégicos e manter a estabilidade interna. Nesse sentido "o ciberespaço tem a capacidade de desafiar a soberania nacional, visto que pode questionar a habilidade do Estado em regular os movimentos e os fluxos de informações dentro de suas fronteiras nacionais" (Khanna, 2018).

As vulnerabilidades abordadas ficam evidentes através do grande incidente cibernético conhecido como Stuxnet, ocorrido em 2010, quando um *worm*[8] de computador contaminou as máquinas da instalação nuclear de Natanz, no Irã. Esse país, localizado no sudoeste da Ásia, ocupa uma posição estratégica entre o Sul, Centro e Oeste da Ásia, além de possuir amplas reservas de combustíveis fósseis, como gás natural e petróleo (Afary, Mostofi, Avary, 2022 apud Rocha, 2022).

A história da energia nuclear no Irã inicia com uma iniciativa dos EUA. Em 1953, o presidente Dwight Eisenhower expressou preocupação sobre o potencial bélico da tecnologia nuclear em seu discurso na Assembleia Geral da ONU. Com o intuito de evitar que mais nações usassem essa tecnologia para fins militares, Eisenhower propôs medidas visando transformar esse conhecimento em algo benéfico para a humanidade (Rocha, 2022).

Uma dessas medidas foi o acordo denominado "Átomos para a Paz", estabelecido em 1957 entre Eisenhower e o soberano iraniano, Mohammad Reza Pahlevi, com o objetivo de promover o uso pacífico da energia atômica. Por meio desse acordo, os EUA se comprometeram

[8]Worm é um tipo de programa de computador malicioso (malware) que se propaga e se replica automaticamente com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, explorando vulnerabilidades em sistemas operacionais ou softwares para acessá-lo, oferecendo mais riscos do que o vírus porque o seu programa é autônomo.

a disponibilizar conhecimento e tecnologia para o desenvolvimento de energia nuclear para fins pacíficos. No entanto, todo esse programa foi interrompido com a Revolução Islâmica de 1979[9]. Desde então, o governo iraniano tentou reativar o programa por vários anos, por meio de parcerias existentes e novas propostas, mas os EUA aplicaram pressão sobre esses países, frustrando os planos do Irã (Rocha, 2022).

Após extensas negociações, a Rússia concordou em encerrar o projeto nuclear inicial e construir dois novos reatores no Irã. Essa ação gerou preocupações nos EUA e Israel, que temiam que o conhecimento adquirido permitisse ao Irã fabricar armas nucleares. Desde a Revolução Islâmica em 1979, o Irã adotou uma postura firme diante de intervenções estrangeiras, e esta postura junto à falta de informações sobre seu programa nuclear alimentou a desconfiança dos EUA e da União Europeia sobre suas verdadeiras intenções (Lopes e Oliveira, 2014 apud Rocha, 2022).

Foi durante o governo de George Walker Bush nos EUA que uma medida foi tomada, com a proposta de uma intervenção de forma cibernética, atacando o Irã. Para isso, foi desenvolvido o worm de computador denominado Stuxnet, um código malicioso programado para atacar o Sistema de Supervisão e Aquisição de Dados (SCADA) da empresa Siemens, usado para gerenciar o funcionamento de equipamentos industriais, como os presentes nas centrífugas de enriquecimento de urânio no Irã. O complexo código malicioso explorou as vulnerabilidades presentes nas máquinas do programa nuclear do Irã, interferindo de maneira discreta e camuflada, o que dificultou sua detecção imediata. Esse *malware* tinha como objetivo prejudicar as centrífugas, mascarando-se como um simples problema de funcionamento aos técnicos (Lopes e Oliveira, 2014 apud Rocha, 2022).

O caso *Stuxnet* foi o primeiro a, por meio de códigos maliciosos, causar danos físicos em algo, ao forçar o Irã a substituir mais de 900 centrífugas de enriquecimento de urânio. Anteriormente, os ataques eram restringindo a sites e serviços governamentais, gerando transtornos e impactos econômicos. Contudo, esse *worm* trouxe novas proporções ao prejudicar infraestruturas essenciais (Rocha, 2022).

Seu impacto não se resume apenas à sua estrutura complexa ou à mira no programa nuclear do Irã. O debate e a cobertura midiática em torno desse programa sempre geraram preocupações globais sobre o potencial bélico dessa tecnologia. O *stuxnet* revelou a

[9]A Revolução Islâmica foi um movimento político e social que ocorreu no Irã em 1979 e mudou radicalmente o Irã, passando de uma monarquia autocrática pró-Ocidente liderada pelo Xá Mohammad Reza Pahlevi para uma república islâmica teocrática liderada pelo aiatolá Ruhollah Khomeini.

complexidade desafiadora das questões cibernéticas (Rocha, 2022), evidenciando-se como os desafios desse campo podem afetar a soberania nacional. Ao conter os avanços do programa nuclear iraniano, ressaltou-se a vulnerabilidade dos Estados diante de ataques cibernéticos, mostrando como eventos virtuais podem ter consequências tangíveis e interferir na autonomia de uma nação.

Outro marco significativo que influenciou intensamente os debates sobre segurança cibernética até os dias atuais foi o caso *snowden*. Esse evento, ocorrido em 2013, acentuou a discussão sobre vigilância em massa ao revelar as práticas de espionagem dos Estados Unidos contra a políticos, empresas e cidadãos ao redor do mundo. Em junho de 2013, o jornalista estadunidense Glenn Greenwald começou a revelar, por meio do jornal britânico The Guardian, os primeiros documentos do que viria a ser o caso mais comprometedor sobre o sistema de vigilância internacional. Esses documentos foram fornecidos por Edward Snowden (Oppermann, 2014).

Snowden, ex-agente da Agência de Segurança Nacional (NSA), trabalhou como terceirizado da agência de 2009 a 2013. Durante esse período, teve acesso às informações sigilosas que revelavam a extensão da operação de vigilância da NSA. Após deixar o cargo, Snowden mudou-se para Hong Kong, na China, em 2013, de onde começou a expor as práticas de espionagem virtual presenciadas. Ele compartilhou essas informações com o jornalista norte-americano Glenn Greenwald e a documentarista Lauren Poitras (Carvalho, 2015).

Conforme revelado por Snowden, os Estados Unidos secretamente coletavam dados pessoais de inúmeros cidadãos de diferentes países, bem como informações da comunicação de governos estrangeiros. Entre os esquemas de espionagem, destaca-se o Programa de Vigilância (PRISM), responsável pelo monitoramento das telecomunicações e atividades cibernéticas. Este programa permitia à NSA coletar comunicações pessoais das maiores empresas de internet do mundo, incluindo Facebook, Google, Yahoo! e Skype (Greenwald, 2014).

A repercussão desse evento causou muitos problemas à diplomacia estadunidense, uma vez que seus representantes não negaram as espionagens, mas as justificaram como práticas necessárias no combate ao terrorismo. Apesar da justificativa, os alvos do ciberataque não eram somente os fundamentalistas islâmicos e os líderes de facções terroristas, mas também incluíam nações aliadas e até mesmo cidadãos norte-americanos (Carvalho, 2015).

Dessa forma, o referido caso de vigilância foi visto por muitos como uma violação escandalosa à Soberania dos países espionados, incluso no Brasil. Em setembro de 2013, a presidenta Dilma Rousseff, em seu discurso, pontuou que a espionagem dos EUA não era

apenas uma afronta às relações amistosas entre Estados aliados, como também uma grave violação do direito internacional, descartando a ideia de que a prática foi uma forma de combate ao terrorismo (Martins, 2014).

Considerando o conceito jurídico de soberania, que regula as relações entre Estados e destaca a legitimidade do poder político pela lei, observa-se que essa soberania é atribuída não a uma autoridade específica, mas ao Estado como uma entidade. Nessa perspectiva, em que a soberania está ligada à autonomia, a interferência clandestina de um Estado em outro pode ameaçar seriamente a estabilidade e violar essa autonomia (Martins, 2014).

Por exemplo, a prática da espionagem pode levar à obtenção sigilosa de informações cruciais, que, se usadas estrategicamente pelo Estado invasor, diminuiriam consideravelmente a capacidade de ação e reação do Estado alvo. Assim, a noção de uma sociedade estruturada em torno de um Estado independente reflete a soberania e a capacidade de autodeterminação, elementos que seriam gravemente comprometidos por essa prática abusiva (Martins, 2014).

Além disso, a natureza multinacional do ciberespaço desafia a aplicação da soberania tradicional, pois questiona a capacidade dos sistemas jurídicos nacionais em lidar com questões transnacionais presentes nesse espaço compartilhado. Essas ponderações são relevantes para a compreensão da soberania, já que a jurisdição reflete a soberania de cada Estado (Mansur; Rocha, 2019).

3. CONSIDERAÇÕES FINAIS

O objetivo deste estudo é analisar as interações entre o espaço cibernético e as vulnerabilidades dos Estados, respondendo à pergunta: "Como o espaço cibernético amplifica as vulnerabilidades e como elas afetam a soberania dos Estados?". Para alcançar esse propósito, foram delineados objetivos específicos. Inicialmente, busca-se conceituar o surgimento da internet e do ciberespaço, além de explorar seus conceitos. A partir da revolução da informação, impulsionada por avanços tecnológicos, surge a internet, em um contexto de Guerra Fria, resultado de uma convergência entre estratégia militar, cooperação científica e inovação contracultural, e o intitulado "ciberespaço" - um ambiente eletrônico que transcende as fronteiras físicas. No entanto, as origens descentralizadas da internet e do ciberespaço, destinadas a impulsionar sua expansão, também resultaram em desafios de segurança devido à sua natureza.

Além disso, realizou-se um embasamento teórico do ciberespaço a partir da corrente realista e neoliberalista. Para a análise sistêmica do espaço virtual, trabalhou-se o realismo

clássico de Morgenthau, no qual destaca a competição entre Estados e a busca pelo poder como objetivo primordial na política internacional. No contexto do sistema internacional anárquico, instituiu-se que o equilíbrio de poder é essencial para a estabilidade, mas não elimina as vulnerabilidades e lacunas que permitem a interferência entre Estados. Com isso, faz-se paralelos com o ambiente anárquico do ciberespaço, cuja vulnerabilidades são relacionadas e potencializadas pelos avanços tecnológicos. Nesse sentido, apesar das contribuições do realismo, sua limitação está na negligência de outros atores além dos Estados.

Diante disso, para explorar o conceito de poder e suas nuances, recorremos ao liberalismo, que destaca a relevância dos atores não-estatais. A ascensão do ciberespaço como um terreno de projeção de poder gerou incertezas quanto ao seu impacto na segurança global. No âmbito desse ambiente, o exercício de poder pode assumir diversas formas, desde controle até coerção, representando o "Hard Power" e ampliando as vulnerabilidades através de ciberataques. Nesta análise salientou-se que o poder cibernético não é exclusivo dos Estados que, apesar de manterem uma influência predominante, enfrentam vulnerabilidades devido à natureza híbrida do ciberespaço. Isso expõe as vulnerabilidades dos Estados no ciberespaço diante de nações, empresas, organizações e indivíduos.

Adicionalmente, foi abordada a evolução da soberania desde suas origens tradicionais até a presente crise no ciberespaço. Estabeleceu-se que a concepção tradicional de soberania é definida como um poder exclusivo e constante do Estado, responsável por estabelecer uma ordem jurídica em seu território. Reconhecida globalmente, essa soberania é considerada um elemento essencial para a autonomia das nações. Por fim, instituiu-se que a globalização e o ciberespaço desafiaram o conceito tradicional de soberania. Enquanto a globalização diminuiu as fronteiras territoriais, o ciberespaço desafia as noções convencionais de fronteiras estatais. Este ambiente virtual, embora invisível, está ligado a infraestruturas físicas, tornando-se uma questão essencial de soberania nacional. O uso mal-intencionado desse domínio levanta preocupações sobre a vulnerabilidade das sociedades digitais, e os casos de *stuxnet* e *snowden* ilustram essa interligação entre vulnerabilidades cibernéticas e soberania nacional, destacando como ataques virtuais comprometem o controle estatal e afetam a capacidade de governar.

Dessa forma, após a pesquisa e análise dos dados, foi possível confirmar a hipótese proposta: a crescente independência das estruturas digitais torna os Estados mais vulneráveis a ataques cibernéticos, afetando diretamente sua soberania. A capacidade de operações cibernéticas invasivas compromete a autonomia de uma nação, minando seu controle sobre redes, dados e sistemas críticos, e afetando a sua independência na tomada de decisões. Assim,

os ataques não apenas ameaçam a segurança, mas também a autoridade e a governança de um Estado, tanto interna quanto externamente. Isso redefine não apenas a segurança nacional, mas os próprios fundamentos da soberania estatal diante das crescentes vulnerabilidades no ciberespaço.

Para futuras pesquisas, considera-se relevante aprofundar a análise dos casos *stuxnet* e *snowden*, visando detalhar de forma mais abrangente os aspectos desses eventos e sua relevância para a segurança cibernética. Este artigo apenas tangenciou esses eventos, apresentando uma visão superficial de suas implicações. Explorar mais a fundo o impacto do *stuxnet* na infraestrutura crítica e as consequências do vazamento de informações por Edward Snowden oferecerá uma compreensão mais completa sobre os desafios e as nuances da cibersegurança em nosso cenário atual.

REFERÊNCIAS

BAUMAN, Zygmunt (2001). **Globalização: as consequências humanas**. Rio de Janeiro: Jorge Zahar Ed., 1999, p. 13-33.

CARVALHO, Y. C. S. A diplomacia midiática na sociedade em rede: uma análise do caso Snowden. In: **C@LEA – Cadernos de Aulas do LEA,** Ilhéus – BA, n. 4, p. 61-79, nov. 2015.

CASTELLS, Manuel. **A sociedade em rede:** a era da informação: economia, sociedade e cultura. 8. ed. São Paulo: Paz e Terra, p. 67-113, 1999.

CASTELLS, Manuel. Lições da História da Internet. (Org.). **A Galáxia da Internet:** Reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p. 13-33.

CLARKE, Richard A.; KNAKE, Robert K**. Cyber War: the next threat to national security and what to do about it.** Harpercollins USA, 2010.

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

GATTO, Raquel Fortes. **O impacto da governança da internet sob o prisma da soberania**. 2008. Dissertação de Mestrado. Pontifícia Universidade Católica de São Paulo.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo: Atlas, 2002. 175 p. ISBN 85-224-3169-8.

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

KHANNA, Pallavi. **State Sovereignty and Self-Defence in Cyberspace**. BRICS Law Journal, New Delhi, vol. 5 (4), p. 139-154, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, p. 311, 2003.

MARTINS, Alexandre de Oliveira. **Espionagem e soberania nacional:** dilemas de segurança e defesa no caso Brasil x EUA (2013). 2014. Trabalho de Conclusão de Curso.

MAIER, Friedrich. A REVOLUÇÃO DA INFORMAÇÃO E O PODER CIBERNÉTICO: UM MAPEAMENTO CONCEITUAL NA OBRA DE JOSEPH S. NYE JR. **Revista de Iniciação Científica da FFC-(Cessada)**, v. 14, n. 1, 2016.

MANSUR, Daniele Barbosa; ROCHA, Bruno Anunciação. Desafios do exercício da soberania no ciberespaço. **Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí**, Ijuí, RS, v. 1, n. 51, p. 21-33, jun./2019.

MANDARINO JR., Raphael. **Segurança e Defesa do Espaço Cibernético Brasileiro.** Recife: Cubzac, 2010.

MORGENTHAU, H. **A Política entre as Nações**. 2003. Disponível em: <http://funag.gov.br/loja/download/0179_politica_entre_as_nacoes.pdf>. Acesso em: 14 janeiro 2024.

NYE JR, Joseph S. **Deterrence and dissuasion in cyberspace**. International Security, p. 44-71, (2017).

NYE JR, Joseph S. Public diplomacy and soft power. **The annals of the American academy of political and social science**, v. 616, n. 1, p. 94-109, 2008.

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

NYE, Jr., Joseph S. **Soft power: the means to success in world politics. New** York: PublicAfffairs, 2004.

OPPERMANN, Daniel. O cenário de cibersegurança depois de Snowden e consequências no Brasil. **JANUS 2014-Metamorfoses da violência (1914-2014),** p. 148-149, 2014.

PORTELA, Lucas Soares. **Geopolítica do espaço cibernético e o poder**: o exercício da soberania por meio do controle. Revista Brasileira de Estudos de Defesa, v. 5, n. 1, 2018.

QUITERIO, Janaína. Princípios da governança na rede: as contribuições do NET mundial. **ComCiência**, Campinas, n. 158, May 2014. Available from <http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542014000400003&lng=en&nrm=iso>. access on 20 July 2023.

RÊ, Eduardo De. **Ciberespaço e segurança cibernética:** as estratégias cibernéticas de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil. Florianópolis, 2021.

RIORDAN, Shaun. **Cyberdiplomacy:** managing security and governance online. John Wiley & Sons, 2019.

ROCHA, Gabriela Cristina**. Caso Stuxnet:** os impactos do ataque cibernético ao programa nuclear do Irã com a primeira arma cibernética à segurança internacional (2009-2010). 2022. Trabalho de Conclusão de Curso.

SERRANO, Inês Isabel Baião. **Cibersegurança na União Europeia:** a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. 2022. Dissertação de Mestrado. Universidade de Évora.

Universidade do Estado do Pará
Centro de Ciências Naturais e Tecnologia
Curso de Bacharelado em Relações Internacionais
Tv. Enéas Pinheiro, n° 2626 - Marco
CEP: 66095-100 Belém - PA

www.uepa.br