

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

LETÍCIA REIS CUNHA

A CARACTERÍSTICA DA ATEMPORALIDADE NAS TEORIAS CLÁSSICAS DAS
RELAÇÕES INTERNACIONAIS

BRASÍLIA

2023

LETÍCIA REIS CUNHA

A CARACTERÍSTICA DA ATEMPORALIDADE NAS TEORIAS CLÁSSICAS DAS
RELAÇÕES INTERNACIONAIS

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

Orientadora: Fernanda L. S. Medeiros

BRASÍLIA

2023

LETÍCIA REIS CUNHA

A CARACTERÍSTICA DA ATEMPORALIDADE NAS TEORIAS CLÁSSICAS DAS
RELAÇÕES INTERNACIONAIS

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

Orientadora: Fernanda L. S. Medeiros

BRASÍLIA, CIDADE MÊS 2023

BANCA AVALIADORA

Professor(a) Orientador(a)

Professor(a) Avaliador(a)

AGRADECIMENTOS

A Deus, pela vida. Aos meus pais, por serem minha fortaleza e me ajudarem a trilhar meu caminho; à minha irmã, por reconhecer minhas dificuldades e me ajudar a reunir coragem para enfrentá-las; ao Vincenzo, por sempre estar ao meu lado e acreditar em mim, quando eu não acreditei; às minhas amigas e companheiras de estudo, pela ajuda e companheirismo nas horas difíceis; e à minha orientadora, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos: meus mais sinceros agradecimentos.

A CARACTERÍSTICA DA ATEMPORALIDADE NAS TEORIAS CLÁSSICAS DAS RELAÇÕES INTERNACIONAIS

Letícia Reis Cunha¹

Resumo: Este estudo tem como objetivo investigar a relação entre as teorias clássicas das Relações Internacionais e a ciberguerra, avaliando sua capacidade de explicar as características únicas desse tipo de conflito. Serão analisadas as teorias existentes, estudos de casos de casos e suas respectivas conexões. A hipótese orientadora sugere que embora as teorias existentes possam fornecer *insights* relevantes, sua aplicação direta pode ter limitações. A metodologia inclui revisão bibliográfica, análise de casos e comparação entre teorias e características deste tipo de conflito. Os resultados esperados são uma compreensão aprofundada da ciberguerra nas relações internacionais, identificação de lacunas teóricas e estratégias de prevenção e resposta mais eficazes.

Palavras-chave: Relações Internacionais, ciberguerra, teorias clássicas, análise teórica, conflitos internacionais.

Abstract: This study aims to investigate the relationship between classical theories of International Relations and cyber warfare, evaluating their ability to explain the unique characteristics of this type of conflict. Existing theories will be analyzed, along with case studies of cyber warfare, and connections between them will be established. The guiding hypothesis suggests that while existing theories may provide relevant insights, their direct application may have limitations. The methodology includes a literature review, case analysis, and comparison between theories and the characteristics of this type of conflict. The expected outcomes are a deep understanding of cyber warfare in international relations, identification of theoretical gaps, and the development of more effective prevention and response strategies.

Keywords: International Relations, cyber warfare, classical theories, theoretical analysis, international conflicts

¹ Graduanda em Relações Internacionais no Centro Universitário de Brasília | reisleticia@sempreueb.com

SUMÁRIO

AGRADECIMENTOS	4
SUMÁRIO	6
INTRODUÇÃO	7
CAPÍTULO II.....	9
<i>2. Teorias das Relações Internacionais.....</i>	<i>9</i>
<i>2.1. Realismo</i>	<i>9</i>
<i>2.2. Liberalismo.....</i>	<i>13</i>
<i>2.3. Teoria da Interdependência Complexa</i>	<i>17</i>
<i>2.4. Teoria da Dissuasão.....</i>	<i>17</i>
CAPÍTULO III	19
<i>3.1. Ataques ao site do Ministério da Saúde, no Brasil.....</i>	<i>20</i>
<i>3.2. Ataques russos ao DNC.....</i>	<i>21</i>
<i>3.3. Stuxnet</i>	<i>22</i>
<i>3.4. Ataques às empresas energéticas da Ucrânia.....</i>	<i>23</i>
CONCLUSÃO.....	24
CONSIDERAÇÕES FINAIS.....	31
REFERÊNCIAS	34
LISTA DE CONCEITOS.....	37

INTRODUÇÃO

O que é 'tecnologia'? Conforme a definição do Dicionário Online de Português, 'tecnologia' abrange os conjuntos de instrumentos, métodos e técnicas que possibilitam a aplicação prática do conhecimento científico. Contudo, com o propósito deste trabalho, pretende-se adotar uma perspectiva em que 'tecnologia' seja sinônimo de inovação, representando uma maneira de transformar significativamente a sociedade - tanto em termos positivos quanto negativos.

Em uma linha do tempo, algumas inovações que foram de extrema importância para a humanidade são: o descobrimento do fogo, a roda, a caça e pesca, agricultura, a eletricidade, entre outros. Todas essas descobertas e invenções - fruto de pesquisas e descobrimentos em um campo científico - revolucionaram a vida humana. Da mesma forma, as novas ideias também trouxeram proveitos militares, à medida que a sociedade evoluiu. De início, as guerras eram entre animais e seres primitivos, para alimentação, com a utilização de pedras ou fogo. Após séculos, surgem tribos, as quais batalhavam entre si com o uso de arcos e flechas. E, após o surgimento de Estados primitivos, os conflitos passam a ser pelo poder e tomada de territórios.

E, dessa forma, à medida que a humanidade progride em pesquisas, reflexões, filosofia e outras disciplinas científicas, novas possibilidades de desenvolvimento de armamentos surgem, tais como a invenção da pólvora, a introdução das armas de fogo e, inclusive, o advento dos armamentos nucleares. Durante o surgimento de novas tecnologias - utilizadas para a guerra - outros grupos sociais ou nações pelejaram com a falta delas.

Similarmente a períodos anteriores, no contexto contemporâneo, a sociedade enfrenta um desafio crescente associado à emergência de uma nova forma de tecnologia militar: a cibernética. Assim como suas irmãs, a utilização de computadores como armas militares permanece restrita à minoria dos Estados, estando acessível somente às nações detentoras de tecnologias avançadas. Além disso, seu potencial de destruição ainda não é completamente compreendido, tendo em vista sua rara aparição no cenário internacional.

Tendo em vista a análise e o estudo de guerras, assim como suas inovações e novas formas bélicas, as Relações Internacionais e, mais especificamente, suas teorias, surgem com o objetivo de entender a origem e as motivações da guerra. Em 1919, após a Primeira Guerra Mundial, surge a disciplina das RI com o objetivo de estudar conflitos e impedir que tamanha tragédia, que causou demasiado sofrimento humano, voltasse a se repetir (JACKSON;

SØRENSEN, 2018). Assim, a disciplina foi desenvolvida para buscar respostas sobre o início da guerra e compreender as causas de sua continuidade, apesar da imensa destruição causada.

No entanto, apesar de seu pontapé inicial ter sido a segurança internacional, atualmente, as Relações Internacionais analisam não somente o comportamento dos países, mas todos os agentes que regem o respectivo cenário. Como exemplo, a disciplina estuda a política externa das nações e seus impactos para um mundo globalizado, a cooperação internacional entre os intermediários das RI e pautas sociais, como o feminismo, a colonização e a migração de refugiados.

A evolução da disciplina das Relações Internacionais está intrinsecamente ligada ao desenvolvimento das ideias, à revolução da tecnologia e à evolução das teorias, concomitantemente com a dinamicidade das inovações. Pontos importantes para a atualidade que influenciam o cenário internacional são a revolução nuclear e espacial, que impõe uma paz armada pautada no medo, e a revolução científica, que aumenta a interdependência entre as nações, acelerando a desigualdade entre os países industrializados e aqueles pautados em economia de setores primários e secundários. (CASTRO, 2012)

Este trabalho tem como foco a segurança internacional e as capacidades de atualização das teorias clássicas das Relações Internacionais em relação às novas formas de conflitos. Para tanto, foram utilizados textos teóricos, para a análise, além de pesquisas e coletas de dados, para a compilação de casos. Além disso, tendo em vista a temporalidade das teorias, serão analisadas apenas aquelas presentes no 1º Debate das Relações Internacionais, assim como teorias complementares, referentes aos estudos estratégicos de guerra. Por fim, busca-se responder se as teses apresentadas são adequadas para a análise dos casos e, caso contrário, quais são suas limitações. Com base nisso, as seguintes perguntas servem como orientação:

1. As teorias tradicionais têm a capacidade de analisar as novas formas de conflito digital, como a ciberguerra?
2. Como podemos aplicar de forma efetiva as teorias existentes para analisar os casos específicos de ataques cibernéticos?
3. Quais são as principais limitações das teorias atuais para compreender e abordar a complexidade dos conflitos digitais?
4. Quais atualizações e aprimoramentos seriam necessários nas teorias existentes para torná-las mais adequadas e relevantes no estudo dos ataques cibernéticos?

CAPÍTULO II

2. Teorias das Relações Internacionais

Atualmente, toda ciência é pautada na utilização de alguma teoria, dentro de seu campo de pesquisa. Define-se ‘teoria’ como o “conjunto de regras, de leis sistematicamente organizadas, que servem de base a uma ciência” (DICIO, 2023). Apesar de completa, pode não ser a mais adequada para o propósito deste estudo. Portanto, considere, também, a seguinte definição “É o uso da observação para testar hipóteses sobre o mundo (teorias empíricas)” (SARFATI, 2011). Assim, incorporando ambas as definições, a teoria, para este trabalho, pode ser considerada como “o conjunto de regras, que servem de base a uma ciência, para testar hipóteses sobre o campo de estudos as quais elas se aplicam.”

As teorias das Relações Internacionais têm a finalidade de formular métodos e conceitos que permitem compreender a natureza e o funcionamento do sistema internacional, bem explicar mais importantes que moldam a política mundial.” (NOGUEIRA; MESSARI, 2005)

Entenderemos, assim, ‘Teoria das Relações Internacionais’ como o conjunto de regras, leis, sínteses e teses, utilizadas como base para a ciência das RI, com o objetivo de estudar e entender o campo internacional e suas variáveis, como a sociedade, a economia e, fundamentalmente, a guerra. As Teorias Clássicas, chamadas de Realismo e Liberalismo, surgiram originalmente para analisar a Primeira Guerra Mundial, conhecida, na época, como "A Grande Guerra", e para compreender suas implicações para os Estados. Essas teorias foram desenvolvidas com o objetivo de prevenir conflitos de grande magnitude e examinar as consequências desses conflitos nas relações entre os Estados.

2.1. Realismo

O Realismo foi a primeira teoria das Relações Internacionais criada para análise do comportamento dos Estados perante questões de segurança, sendo até hoje o princípio mais dominante entre analistas, pesquisadores e estudantes do campo. Os realistas clássicos possuem certas características comuns em suas análises das relações internacionais: (I) uma visão pessimista da natureza humana; (II) a crença de que os princípios do Estado são pautados na segurança; e (III) autopreservação.

O cenário internacional é baseado na chamada 'política de poder', na qual a nação mais forte detém maior influência política e é dominante perante as outras. Além disso, as RI são vistas como tipicamente conflituosas em razão da necessidade de defesa dos interesses estatais, frequentemente resultando em guerras entre os Estados. Por fim, há ceticismo quanto à cooperação internacional, pois acredita-se que estas ocorrem apenas quando há grande interesse de uma das partes, sem a possibilidade de cooperação mútua baseada na bondade das nações. (JACKSON; SØRENSEN, 2018)

Outrossim, o Realismo clássico postula que os interesses pessoais são baseados no próprio bem-estar, dentro de relações de competição entre os indivíduos. Portanto, os seres humanos buscam estar no topo de uma relação de poder, para evitarem ser explorados por aqueles que possam ser 'mais fortes'. Essa situação é considerada como um 'desejo pelo poder'. Assim, em um vínculo indivíduo-indivíduo, as pessoas buscam permanecer em um status quo de dominação em relação aos outros membros de sua sociedade.

Tal cenário também se aplica às relações Estado-Estado, dado que o objetivo de cada nação, dentro da perspectiva realista, é sobreviver ao cenário de anarquia internacional e, principalmente, evitar ser dominada por outro país – essa dominação pode ser tanto militar, quanto política, social ou cultural.

É considerado fundamental para a defesa dos interesses nacionais de um Estado evitar ser dominado por outros, pois aqueles que estão subjugados não têm a capacidade de impor ou mesmo defender seus próprios interesses diante da influência de terceiros. Toda essa situação é o cerne da política internacional. (MORGENTHAU, 1965;1985).

“A política é uma luta pelo poder sobre os homens e quaisquer que sejam seus objetivos finais, o poder é seu objetivo imediato e as formas de adquiri-lo, mantê-lo e demonstrá-lo determinam a técnica da ação política” (Morgenthau, 1965:195)

“Nesse sentido, a política internacional é retratada, sobretudo, como uma “política de poder”: uma arena de rivalidade, conflito e guerra entre Estados nos quais os mesmos problemas básicos de defender seu interesse nacional e garantir sua sobrevivência se repetem várias vezes” (Jackson; Sørensen, 2018).

Os realistas acreditam que o cenário internacional funciona dentro de um sistema anárquico, onde os Estados atuam de forma independente, com o objetivo primordial de garantir sua própria sobrevivência. Dentro dessa perspectiva, as nações são consideradas os principais atores na tomada de decisões nesse contexto, enquanto outros agentes, como ONGs, indivíduos ou organizações internacionais, são vistos como menos relevantes.

De acordo com a teoria realista, a anarquia implica na prevalência da lógica do mais forte, e, portanto, as necessidades e vontades dos Estados mais poderosos são estabelecidas em detrimento das de outros agentes. Assim, para assegurar a realização de seus interesses, os agentes - Estados - precisam 'vencer' um conflito implícito de dominação. (NOGUEIRA; MESSARI, 2005)

2.1.1. HANS J. MORGENTHAU

Hans J. Morgenthau (1904-1980), um dos principais teóricos do Realismo, em sua tese "Politics Among Nations: The Struggle for Power and Peace" (1948), descreve conceitos importantes para o entendimento do Realismo e sua compreensão do cenário internacional. Como primeiro ponto, Morgenthau afirma que a política realista, assim como a sociedade, é governada pela natureza humana - a qual possui caráter egoísta. Afirma-se, também, que a política realista alcança a política internacional através de 'interesses definidos em forma de poder' - que sugere que interesses de indivíduos e/ou grupos são pautados na busca pelo poder. Esses agentes atuam com o objetivo de obter maior controle sobre os outros, mesmo que isso implique prejudicar os interesses alheios. Assume-se que os estadistas, ao longo da história humana, trilham suas ações através deste interesse em forma de poder e, por isso, é possível mapear os passos que serão tomados.

Os Estados, governados por estadistas consumidos pelo interesse pelo poder, buscam também o domínio sobre os demais dentro de um contexto global. Dentro dessa conjuntura, podem ocorrer duas situações possíveis. 1) a união entre Estados para impedir a soberania de uma única nação, visando proteção nacional e garantia de segurança e sobrevivência de suas nações. 2) a busca pela hegemonia de uma ou de um pequeno grupo de Estados no cenário internacional, onde estes lutam pela dominação do quadro mundial. Na primeira hipótese, a aliança formada entre os países tem como objetivo proteger a soberania nacional e garantir a segurança e a sobrevivência de suas nações. Na segunda hipótese, há a possibilidade de alinhamento com os Estados hegemônicos, visando também a segurança e sobrevivência dos países, por meio da força e domínio do mais forte. Em ambos os casos, no entanto, os Estados buscam formas de sobrevivência dentro de um cenário anárquico.

Adicionalmente, Morgenthau argumenta que, dada a realidade tumultuosa em que os Estados estão inseridos, a busca pelo poder e a necessidade de sobrevivência inevitavelmente levam a conflitos internacionais. Embora a diplomacia seja eficaz na gestão de conflitos, em muitos casos, pode não ser suficiente para evitar seu surgimento. Além disso, a política externa

dos Estados é intrinsecamente influenciada por seus interesses nacionais, e os fatores domésticos desempenham um papel crucial na formação dessas políticas, podendo também afetar as relações entre os países. No entanto, o autor afirma que há a possibilidade de um equilíbrio entre a busca de poder e a busca pela paz, quando há a promoção da estabilidade internacional. (Morgenthau, 1948)

Por fim, o realista realiza, também, uma crítica às ideias da Teoria Liberalista, enfatizando que a política internacional e as ações dos agentes não serão pautadas em questões morais, tendo em vista a natureza humana. Morgenthau argumenta que a política internacional é mais motivada pela busca de interesses próprios e considerações pragmáticas, em vez de princípios éticos. (Morgenthau, 1948)

2.1.2. KENNETH WALTZ

Kenneth Waltz (1924-2013), em suas obras "Theory of International Politics" (1979) e "Man, the State, and War: A Theoretical Analysis" (1959), discute acerca da importância do sistema anárquico internacional para a relação entre os Estados. Devido à sua natureza "desorganizada", pode haver a criação de um ambiente de incerteza e competição, o que gera nos países a necessidade de autopreservação e manutenção de sua segurança. Waltz defende que, independentemente da característica política e pessoal dos governantes, ainda há, em seus planos de governo, a priorização da segurança nacional e a busca pela manutenção de uma estabilidade internacional.

Além disso, o realista defende a ideia da 'Balança de Poder' - quando um Estado se torna superior aos demais em termos bélicos, militares, tecnológicos e econômicos, ele pode se tornar hegemônico, o que pode limitar a capacidade de outros países de enfrentá-lo. - para a manutenção da paz dentro da comunidade internacional. A competição entre dois Estados dentro da Balança de Poder chama-se equilíbrio de poder e ocorre quando duas nações, igualmente poderosas, são incapazes de enfrentar-se em um conflito, devido à uma igualdade de poder.

No livro "The Spread of Nuclear Weapons: A Debate" (1955), Kenneth Waltz aborda a proliferação das armas nucleares, apresentando pontos positivos e negativos. Segundo a perspectiva realista, Waltz argumenta que a posse de armas nucleares pode ser benéfica para a estabilidade internacional, uma vez que os Estados seriam desestimulados a entrar em conflitos, devido à capacidade destrutiva desses armamentos. Além disso, o autor argumenta que os países que possuem armas nucleares são menos propensos a serem invadidos por outros Estados, o que aumentaria sua segurança no cenário internacional.

No entanto, Waltz também discute a possibilidade de uma perigosa "corrida armamentista", na qual alguns Estados buscam adquirir armas nucleares como uma suposta garantia de segurança e credibilidade. Ele aponta ainda o aumento dos riscos internacionais, como o surgimento de novas crises e conflitos nucleares, a escalada do armamentismo e a possibilidade de atores não estatais terem acesso a essas armas.

2.2. Liberalismo

A Teoria Liberalista edifica-se, sobretudo, após a Primeira Guerra Mundial como uma alternativa ao Realismo, sendo criticada por este último, principalmente devido à sua abordagem utópica. O Liberalismo acredita na possibilidade de se estabelecer Relações Internacionais baseadas em valores éticos e morais e contrapõe a ideia do Realismo acerca da natureza humana.

O Liberalismo busca inspiração nos pensamentos iluministas e de autores da época, tendo como sua principal preocupação, a liberdade individual. Os liberalistas, assim como os iluministas do século XVII, acreditam que o ser humano possui total capacidade, através do uso da razão, de definir seu destino de forma autônoma. Uma sociedade liberta discerne aquilo que é bom para um grupo ou indivíduo, devido à sua capacidade analítica. Tal princípio respalda-se, também, no Direito Natural à liberdade e à propriedade dentro de uma comunidade. Assim, em busca da própria liberdade, mesmo que partindo de motivos egoístas, os indivíduos buscarão o bem-estar da sociedade em que estão inseridos. Um exemplo para esta síntese é a teoria da *mão invisível*, de Adam Smith (1723-1790), publicada no livro de Nogueira e Messari:

A mão invisível: o mecanismo da competição fazia com que o desejo de melhorar as próprias condições de vida se tornasse em um agente benéfico para a sociedade ao contrapor o impulso de enriquecimento do indivíduo ao dos demais. Dessa competição, surge a mão invisível para equilibrar os preços das mercadorias em seus níveis "naturais".

Os liberais pensam, também, que as organizações políticas contribuem para o progresso social, servindo para o desenvolvimento do bem-estar comum da sociedade. Paralelamente, o Estado, para estes pensadores, é um mal necessário. De forma externa, seu propósito é a defesa dos interesses nacionais, além da proteção da nação de inovações e possíveis guerras. De forma interna, há a possibilidade do surgimento de governos autoritários, os quais limitariam a liberdade da comunidade. Dentro de um Estado tirano, a guerra é um pretexto para a restrição da livre expressão, de aumento dos gastos militares, concentração de poder etc. Assim, a Teoria Liberal entende a guerra como um motivo para a restrição da liberdade individual e coletiva,

além de colocar em risco os interesses nacionais. Portanto, há a necessidade da manutenção da paz no sistema internacional - seja por organizações internacionais ou tratados bi e multilaterais - para a defesa da população estatal.

Acerca da anarquia internacional que rege o comportamento dos Estados, ambas as teorias possuem opiniões similares. Assim como o realismo, os liberais acreditam que o sistema anárquico serve como justificativa para conflitos entre nações. Porém, ao contrário do Realismo, acredita-se que esta característica não é imutável e pode ser transformada em um sistema de Estados harmonioso e cooperativo, a partir do livre-comércio, a democracia e as instituições internacionais. (NOGUEIRA E MESSARI, 2005)

Um dos pontos de origem do liberalismo é a Conferência de Paris, pós-Primeira Guerra Mundial, com a finalidade de instituir uma nova ordem mundial e a apresentação dos Quatorze Pontos, por Woodrow Wilson (1856-1924). Dois dos principais pontos apresentados pelo ex-presidente estadunidense, necessários para a manutenção da paz entre os Estados, é, em primeiro lugar, a promoção da democracia e da autodeterminação dos povos, o qual entende que governos democráticos não entrarão em guerra. O segundo ponto é a necessidade da criação de uma organização institucional internacional, com o objetivo de regular e mediar as relações estatais. (WILSON, 1918). Este era objetivo da Liga das Nações, organização internacional criada na época.

Adicionalmente, Norman Angell (1872- 1967), um dos pensadores do liberalismo à época de sua criação, em seu livro 'A Grande Ilusão', onde a Ilusão é a ideia de muitos governantes de que a guerra será benéfica e lucrativa para o vencedor. De acordo com Angell, a modernidade e a tecnologia provocam a interdependência entre os Estados e, conseqüentemente, a diminuição da necessidade do uso da força.

2.2.1. JOSEPH NYE

Joseph Nye (1937) um cientista político norte-americano conhecido por suas contribuições para as Relações Internacionais com viés liberal. Em sua obra "Soft Power: The Means to Success in World Politics", de 2004, Nye discorre acerca dos conceitos de *Soft* e *Hard Power*, que caracterizam diferentes formas de interpretação da influência dos Estados sobre outros. Embora os caminhos adotados por cada um sejam diferentes, ambos visam alcançar um objetivo em comum: a capacidade de persuadir outros Estados a fazerem aquilo que desejamos. Em outras palavras, as duas teorias buscam a habilidade de influenciar os outros para que ajam de acordo com nossos interesses.

O conceito de *Hard Power*, segundo o autor, se refere à capacidade de influenciar outros Estados através do uso da força. Essa ideia pode estar associada a conflitos armados e à quebra de soberania de outras nações. No entanto, atualmente, o conceito de *Hard Power* está predominantemente associado à capacidade bélica e econômica de um Estado. Dessa forma, entende-se que um país com maior força militar e econômica será mais temido e, conseqüentemente, terá mais facilidade em impor suas influências e interesses sobre outros países.

Ao contrário de seu irmão, *Soft Power* é a capacidade de moldar os desejos de outros através de 3 possíveis fontes - cultura, valores políticos e política externa. Como exemplo, a indústria de filmes estadunidense exerce forte influência, principalmente, nos países latino-americanos. Em consequência, o modo de vida americano é extremamente almejado pelas populações dos países ocidentais.

“O que é Soft Power? É a habilidade de conseguir o que você deseja, através da atração, ao invés da coerção ou pagamentos. Surge da atratividade da cultura, ideais políticos e políticas públicas de um país.” (Joseph Nye; 2014, p. 9, tradução: autoral).

“Quando você consegue que os outros admirem seus ideais e desejem o que você deseja, você não precisa gastar tanto em paus e cenouras para movê-los em sua direção. A sedução é sempre mais eficaz do que a coerção, e muitos valores como democracia, direitos humanos e oportunidades individuais são profundamente sedutores.” (Joseph Nye; 2004, tradução: autoral).

O *Soft Power*, definido como “a capacidade para se conseguir o que se quer através da atração, em vez da coerção ou do pagamento” liga-se à teoria liberal, pois é através de uma interdependência estatal que ocorre uma atração para as questões internacionais; “...a sua cultura (em lugares onde é atraente para os outros), os seus valores políticos (quando fazem jus a eles em casa e no exterior) e as suas políticas externas (quando outros os veem como legítimo e como tendo autoridade moral)”. (NYE, 2002). É necessário que tenha, primordialmente, uma cooperação/interdependência pré-estabelecida para que o *Soft Power* possa agir com maior eficiência.

Existem outras variáveis a serem consideradas dentro desse problema. A Teoria de Soft e Hard Power, juntamente com outras teorias clássicas, não atribui importância a agentes além do Estado quando se trata dessa problemática. Ao examinar o fenômeno da ciberguerra, é crucial reconhecer outros agentes que desempenham um papel relevante em sua análise, como

grupos de hackers. Esses grupos, assim como os Estados, apresentam desafios significativos para as nações no contexto do ciberterrorismo.

Ademais, ao abordar o conceito de Hard Power, essa teoria considera a superioridade de uma nação com base na qualidade e quantidade de seu arsenal militar. Como ilustração, imagine um confronto entre dois grupos, em que uma parte possui milhões de arcos e flechas, enquanto a outra detém apenas centenas de armas de fogo. Apesar da discrepância numérica dos armamentos, aquele grupo que possui armas de fogo, de melhor qualidade e tecnologia, terá maior probabilidade de alcançar a vitória. No entanto, quando aplicamos essa situação ao domínio cibernético, essa ideia não se aplica. Na guerra tecnológica, a quantidade de "armas" - nesse caso, computadores - não é relevante, apenas a qualidade. Ou seja, apenas um indivíduo com equipamentos de alta qualidade é capaz de exercer poder destrutivo.

A teoria em discussão apresenta algumas limitações em seu funcionamento, pois há várias situações em que não pode ser aplicada. Sendo elas:

1. As atividades bélicas no âmbito da ciberguerra ocorrem principalmente de maneira secreta. Portanto, no que se refere às ações dos Estados, muitos governos optam por não divulgar sua capacidade tecnológica, o que pode levar a uma subestimação de seu poder de hard power. Além disso, uma vez que a ciberguerra ainda não é amplamente reconhecida ou ativamente combatida como uma forma de guerra, mesmo que a tecnologia seja reconhecida, há a possibilidade de ela ser considerada inferior em relação às formas bélicas tradicionais.
2. A teoria em questão não considera outros agentes além dos Estados como relevantes, deixando de abranger ações significativas de ciberterrorismo realizadas por grupos, empresas ou indivíduos.
3. A teoria não inclui a posse de tecnologia que exceda os critérios de qualidade e quantidade estabelecidos previamente. Portanto, no âmbito da aplicação da ciberguerra, é reconhecido que somente uma fonte de tecnologia de alta qualidade é pertinente para uma ação de guerra significativa. Em outras palavras, dentro do contexto da ciberguerra, é compreendido que apenas uma fonte que disponha de tecnologia de qualidade é capaz de exercer um impacto relevante durante um conflito, situação a qual não é reconhecida pela teoria de Hard Power como força bélica.

2.3. Teoria da Interdependência Complexa

A Teoria da Interdependência Complexa foi desenvolvida pelos cientistas políticos Joseph S. Nye e Robert O. Keohane, na obra “Poder e Interdependência”. Os autores iniciam a explicação sobre o tema com a citação de Jean-Jacques Rousseau, onde afirma-se que a solução para a paz é o isolamento e separação dos Estados. Porém, em um cenário globalizado, a reclusão de uma nação pode gerar, ao contrário da ideia descrita, pode desencadear problemas econômicos, sociais e comerciais.

Atualmente, a interligação entre as nações, sejam comerciais, sociais ou políticas, torna quase impossível a exclusão de algum país, dentro do cenário internacional. Dois ou mais Estados podem se interligar, não somente de forma econômica ou militar, como em outros séculos, mas de maneira social, política, ambiental, tecnológica, entre outros.

De acordo com os autores, a interdependência entre as nações torna cada vez mais difícil o uso da força, seja ela militar ou econômica, para a resolução de conflitos. Isso se deve ao fato de que as consequências de tais ações afetam não apenas a nação que impõe a situação, mas também todas as outras que possuem relações comerciais, políticas ou culturais com ela.

“A interdependência força-nos a compreender que os desafios atuais representam não só um dilema para nós em nosso próprio país, mas também um dilema comum para todos. O ambiente chama a atenção para esse fato de maneira contundente não existe essa coisa de clima estável para um país ou um continente menos que o clima seja estável para todos. A segurança climática é um patrimônio público mundial” (John Ashton, representante especial do Reino Unido para a mudança climática, 27 de setembro de 2000)

Portanto, entende-se a Teoria da Interdependência Complexa como a correlação entre as nações, de forma a diminuir as tensões entre Estados, devido à dependência entre estas.

2.4. Teoria da Dissuasão

O princípio da Dissuasão é descrito no livro "Introdução aos Estudos Estratégicos", de Augusto Teixeira e Antônio Silva, como o equilíbrio entre a persuasão e a força bruta, baseada na coerção. A dissuasão limita a ação dos agentes, de acordo com a ameaça de violência, com o objetivo de manutenção de um status quo. Ou seja, uma ameaça como "não ataque o meu aliado" será aceita, dependendo da força bélica do transmissor.

Sua criação data-se com o surgimento das armas nucleares, com o medo que pode ser gerado pela possibilidade de retaliação de tamanha amplitude. No entanto, diversos autores começaram a utilizar a dissuasão em suas análises, de forma a expandir o entendimento da teoria. Portanto, atualmente, há duas vertentes para o raciocínio: dissuasão nuclear e convencional.

A dissuasão nuclear, devido à sua capacidade de destruição, terá o maior poder de persuasão, graças ao medo que pode ser gerado. No entanto, ao mesmo tempo que sua capacidade de destruição é temida por sua vítima, também será temida por seu usuário. Atualmente, as armas nucleares têm a capacidade de aniquilar grande parte das nações vizinhas àquela que for vítima de sua grandiosidade.

Sobrepondo, a categoria convencional, analisada por Mearsheimer, na obra "Conventional Deterrence", entende que será levado em conta, para persuadir ou evitar conflitos, o cálculo político e racional da guerra - situação esta que não cabe à utilização de armas nucleares, considerando as consequências de seu uso. Portanto, o agente levará em conta os ganhos e perdas que terá caso entre em um conflito

“[...] a dissuasão se estabelece na interação direta entre os motivos (eminente polítics ou com méritos militares) de se ir à guerra e um cálculo racional dos riscos e cursos dessa ação militar, em todos os campos, inclusive no político: se tal cálculo é maior do lado dos riscos e dos custos e o agente não vai à guerra, a dissuasão teve sucesso (Mearsheimer, 1983)” (JÚNIOR; SILVA, 2020)

O exemplo citado na obra de Augusto e Antônio é a Guerra da Lagosta, entre o Brasil e a França, onde o governo francês renunciou ao conflito, devido à distância entre a costa brasileira e a França. Durante os anos iniciais dos anos 60, navios pesqueiros ilegais, oriundos da França, realizaram a captura de lagostas no litoral nordestino brasileiro. Foi emitida, pelo governo do Brasil, uma autorização válida, por 180 dias, à França, para a pesca. No entanto, após o período permitido, o Estado-Maior da Armada soube acerca do deslocamento de um navio de guerra francês, à costa brasileira e, em resposta, o Brasil mobilizou sua marinha e força aérea para uma preparação de guerra. Após conversações, com a interferência dos Estados Unidos e da ONU, as tropas foram retiradas. De forma lógica, o governo francês detinha uma superioridade militar considerável e acreditava que, devido a essa vantagem bélica, poderia intimidar o Brasil a recuar no conflito. No entanto, para o governo francês, a continuidade da

guerra se mostrava inviável devido à distância geográfica entre seu país e a região em questão. Assim, o poder de dissuasão foi menor aos riscos e custos para a nação francesa.

Entende-se, portanto, a Dissuasão como fator estratégico, que visa a utilização da força como forma de barganha. Diante de uma superioridade bélica, a influência pode ser efetiva, tendo em vista a necessidade de proteção nacional. No entanto, esta só será eficaz se menor que os riscos e custos para a nação detentora do poder.

CAPÍTULO III

O período final à Segunda Guerra Mundial e a Guerra Fria foi marcado pelo surgimento de diversas tecnologias e inovações que moldaram o século - a bomba nuclear, tecnologias espaciais, como satélites de reconhecimento, Mísseis Balísticos Intercontinentais, entre outros. Simultaneamente, o ciberespaço caracteriza-se como parte das relações estratégicas entre os Estados, deixando de ser, apenas, destinado às relações sociais da população e, principalmente, torna-se palco para projeção de poder (Valente, 2007, p.15-16).

Com base nessas considerações, emerge uma nova forma de influência, denominada "Software Power", que se caracteriza pela capacidade de invadir software ou hardware com a intenção de causar danos. Compreende-se que, ao lidar com computadores, existem possibilidades de falhas ocasionais ou desatualizações que podem resultar em interrupções no sistema. No entanto, esses aspectos não são abordados no escopo da análise em questão. (JÚNIOR; SILVA, 2020)

Na obra "Introdução aos Estudos Estratégicos", os autores sustentam que os princípios fundamentais das Relações Internacionais, como defesa nacional e segurança internacional, devem derivar de conceitos essenciais, a saber, território e soberania. No entanto, o emprego de tecnologias na guerra, - a ciberguerra - contradiz ambas as noções fundamentais, apesar de ainda requererem medidas de defesa nacional e segurança internacional. Consequentemente, torna-se evidente a exigência de estabelecer um novo paradigma analítico que englobe a ciberguerra, dada a incapacidade das noções fundamentais das Relações Internacionais de oferecer uma solução adequada para essa questão.

Para a realização deste trabalho, conforme mencionado anteriormente, será conduzida uma análise das teorias clássicas das Relações Internacionais, com o objetivo de avaliar sua capacidade de compreender e analisar a questão da Ciberguerra. Para tanto, serão apresentados quatro casos que envolvem a utilização de tecnologias computacionais como meios de guerra e/ou manipulações estatais.

É necessário, no entanto, antes de expor o uso da tecnologia como forma de conflito, entender que a guerra não será, somente, o uso de forças armadas e a destruição de uma nação. Apesar de esta ser a ideia mais comum, ‘guerra’ ou quaisquer tipos de conflito, principalmente em um mundo globalizado, será tudo aquilo que visa um ataque à uma nação ou população, independente do uso de violência física. A manipulação de mídia, principalmente dentro da crescente onda de *fake news*, com a tentativa de converter uma opinião pública, também pode ser considerada formas de ataques. Portanto, para este estudo, entenderemos ‘guerra’, não somente como a ideia tradicional de destruição, mas como toda ação que visa um ganho maior de um agente - seja ele um Estado ou agentes individuais - com o objetivo de prejudicar uma nação ou uma população e/ou grupo étnico e minoritário.

Os casos apresentados têm como objetivo abordar situações de conflito envolvendo diferentes atores, incluindo ações entre Estados, ações que afetam diretamente os indivíduos e as empresas, bem como o envolvimento de grupos distintos da sociedade civil. Entende-se, portanto, que esses casos são amplos suficiente para garantir uma análise global que compreende diversos agentes das relações internacionais.

3.1. Ataques ao site do Ministério da Saúde, no Brasil

Ao final de 2021, o site do Ministério da Saúde e o aplicativo ConecteSUS sofreram diversos ataques, - de autores não identificados - os quais impediam os usuários de acessarem suas informações. No mesmo período, ocorria a emissão de certificados de vacinação contra a Covid-19, tendo em vista que era, ainda, período de pandemia. Tais comprovantes eram utilizados para a autorização de viagens internacionais e/ou a entrada em algum estabelecimento, pela população brasileira. Além disso, por tratar-se de um sistema oficial do governo, informações pessoais e sigilosas estavam à mercê dos invasores. (GZH; 2021)

Supõe-se que o ataque ao Ministério da Saúde tenha sido através de um *Ransomware*, um *malware* ou ‘vírus’ de software que pode bloquear o computador, - ou, nesse caso, um sistema - por meio de criptografia, e tem o objetivo de reter dados pessoais das vítimas, podendo exigir por uma forma de resgate. (KASPERSKY, Ransomware: definição, prevenção e remoção; 2018).

De acordo com o Ministro da Saúde da época, Marcelo Queiroga, confirmou que tal ação foi um ataque cibernético, além de afirmar que “os dados não serão perdidos”. "Uma atitude criminosa, né, de um hacker. Está sendo investigada pela Polícia Federal e pelo Gabinete de Segurança Institucional. Hoje, o empenho total é para esses dados estarem disponíveis no

mais curto prazo possível. Está sendo investigado e, assim que tiver alguém culpado, será exemplarmente punido", afirmou Queiroga, em entrevista para a GloboNews. (Uol, 2021)

A situação provocou agitação na população brasileira, tendo em vista que, sem a emissão dos comprovantes de vacinação, a locomoção seria dificultada. Além disso, a sociedade estava receosa de que seus dados pessoais seriam vazados e/ou utilizados como forma de extorquir os indivíduos. Quando acessado, as plataformas exibiam a seguinte imagem

Figura 1 - Mensagem no site do Ministério da Saúde após ataque cibernético



Fonte: Ministério da Saúde

Este não seria o primeiro ataque hacker a um órgão brasileiro. Em novembro de 2020, o STJ também confirmou ter sido alvo de tais ações, onde foram forçados a suspender sessões e retirar o site do ar. Por fim, a Anvisa também sofreu com a onda de ataques cibernéticos, onde ocorreu a modificação estética da página da web (defacement), mas sem a alteração de dados ou demais impactos no sistema. (Uol, 201).

A autoria desses ataques foi declarada pelo Lapsus\$ Group, grupo hacker com ligações no Brasil (Folha; 2022) o qual afirmou que havia 50 terabytes de informações do sistema em sua posse e exigiam, para devolução, que fossem contatados pelos responsáveis. (CNN; 2021) Apesar de não ter sido causada por algum Estado, como comumente associado à ideia geral de guerra e ataques, tal questão gerou comoção social, além de afetar a vida da população brasileira durante o período.

3.2. Ataques russos ao DNC

Em 27 de julho de 2016, durante as eleições presidenciais dos Estados Unidos, foram vazados e-mails confidenciais do DNC, a fim de prejudicar a candidata Hillary Clinton. No mesmo dia, o procurador Robert S. Mueller III afirmou que diversos ataques hackers haviam sido proferidos às contas de e-mails da candidata e seus aliados. (Washington Post; 2016)

Ainda no mesmo ano, o presidente da época, Barack Obama, ordenou a saída de 35 diplomatas russos do país, além de negar acesso aos compostos de propriedade russa, além de aplicarem sanções para entidades. (Huffpost; 2016) No entanto, em 2017, o candidato eleito afirmou que tal situação era apenas uma reação do partido contrário, os democratas, à perda das eleições, além de rejeitar o relatório da inteligência americana. (The New York Times, 2017)

Em 2019, Mueller concluiu as investigações acerca do ataque e concluiu que houve interferência do Estado russo em prol da candidatura do ex-presidente Donald Trump. Em relatório, afirma-se que o presidente Vladimir Putin ordenou tal ação para prejudicar as chances da candidata Clinton. Foi ordenado a criação de diversas contas falsas em redes sociais, com o objetivo de gerar discursos de ódio e semear desconfiança no processo eleitoral dos Estados Unidos. Além disso, foram condenados, tanto indivíduos e organizações russas, quanto funcionários de campanha do presidente Trump, após comprovação de que estes se encontraram com o governo russo. No entanto, não se obteve provas suficientes para condenar Trump por corrupção, apesar de este ter se beneficiado das ações. (MUELLER, Robert S.; 2016)

Ao longo da história, grandes potências têm manipulado governos e nações para alcançar seus próprios interesses, seja por meio de guerras ou investimentos diretos. Contudo, com os avanços tecnológicos, a manipulação eleitoral e da opinião pública tornou-se uma ferramenta cada vez mais utilizada. Essa prática, considerada uma forma de guerra cibernética, permite que agentes estrangeiros influenciem o destino de um país sem o uso da força física. O exemplo mencionado ilustra como a tecnologia pode ser utilizada como forma de conquista de interesses nacionais, através da manipulação de massas, sem a necessidade de enfrentamento direto entre duas ou mais nações.

3.3. Stuxnet

O primeiro caso de ataques cibernéticos ocorreu em 2010, através do vírus Stuxnet. Apesar de já existirem diversos outros *malwares* na época, o episódio ficou conhecido por ter invadido sistemas do Irã e Índia. O Stuxnet utilizou brechas desconhecidas do sistema operacional Windows, tendo como alvos sistemas de controle de automação e monitoramento industrial. Apesar de não serem recomendados para uso nuclear, os governos iraniano e indiano

estavam utilizando a plataforma no monitoramento de suas usinas e, assim como outros usuários, estes computadores sofreram com os ataques cibernéticos.

Foi reportado que cerca de 12 complexos industriais foram infectados com o vírus e que este era capaz de interferir com a automação e configuração do sistema industrial, além de roubar dados do sistema. (G1; 2010) Além disso, o *worm* teria capacidade de assumir controle sobre o sistema das usinas, impedindo que estes fossem dirigidos pelos responsáveis. Os computadores das usinas não possuem conexão à internet e, portanto, precisam ter sido infectados através de hardwares, como USBs.

Em 2011, o embaixador russo Dmitry Rogozin, solicitou uma investigação acerca do vírus, tendo em vista que, este, por ter acesso ao sistema de controle das usinas, poderia ter gerado explosões termonucleares. No entanto, tal pedido foi questionado pelo especialista alemão em segurança, Ralph Langner, pois “o Stuxnet não tinha Bushehr como alvo.” Na verdade, a área afetada foi Natanz, que tem 7 mil centrífugas fazendo enriquecimento de urânio. “Em segundo lugar, mesmo neste caso, ele não conseguiria interagir com os sistemas do circuito primário circuito de água que fica em contato com a radioatividade.”

O vírus foi criado pelos governos estadunidense e israelense, em programa secreto denominado de “Jogos Olímpicos”, com a liderança da agência de Segurança Nacional dos EUA (NSA). O objetivo era desenvolver um vírus ou malware que, não somente infectasse softwares, mas danificasse a estrutura física do hardware. (Avast; 2022) A missão final do Stuxnet era impedir ou atrasar os estudos nucleares iranianos. O vírus foi classificado como o maior e mais caro esforço de desenvolvimento de malware da história. (BBC;2020).

3.4. Ataques às empresas energéticas da Ucrânia

Historicamente, há uma tensão entre a Ucrânia e a Rússia. Ambos os países emergiram do antigo Estado Eslovo, entre os séculos IV e VI, e, apesar de formarem duas nações distintas à época, permaneceram culturalmente, historicamente e linguisticamente próximas. Durante a existência da União Soviética, o Estado ucraniano foi parte do império, tendo conquistado sua independência apenas em 1991. No entanto, após a separação, a Rússia tenta a reconquista do território, ano após ano.

Em 2016, hackers invadiram os sistemas de abastecimento de energia e interromperam o fornecimento para centenas de casas na Ucrânia, sendo o primeiro ataque cibernético envolvendo eletricidade. (Folha de São Paulo; 2016) Já em 2022, durante o início da atual

guerra Rússia e Ucrânia, o grupo Sandworm - também responsáveis pelo ataque de 2016 - tentou infiltrar-se nos servidores de energia ucranianos e realizar outro apagão. (Veja, 2022)

O vírus responsável pela invasão chama-se *BlackEnergy*, um Trojan utilizado para realizar ataques de negação de serviço, ou ataques DDOs, espionagem cibernética ou destruição de informações. À época, o presidente ucraniano, Petro Poroshenko, afirmou que a Rússia estaria tentando uma guerra cibernética contra o país. (G1; 2017)

O exemplo acima demonstra a utilização da tecnologia como arma cibernética, tanto para ferir uma população, quanto para a defesa de interesses nacionais sobre outro país. Como citado anteriormente, a ciberguerra é uma forma de conflito que não necessita de um confronto físico e bélico para alcançar seus objetivos.

CONCLUSÃO

A partir do observado nos capítulos anteriores, entende-se que as teorias de Relações Internacionais vêm com o objetivo de entender a questão de segurança nacional e as ações dos Estados em situações de conflitos, sejam eles guerras ou não - apesar de este não ser o seu único foco. Portanto, com o surgimento de uma nova forma de realizar ‘guerra’, diferente daquelas já conhecidas anteriormente, há a necessidade de descobrir se as teorias citadas ainda possuem a capacidade teórica de analisar completamente tal novidade. Os casos não serão analisados individualmente, mas sim como um conjunto de situações em que ocorreu guerra cibernética ou sua tentativa.

O Realismo clássico engloba a guerra cibernética no que diz respeito à necessidade do Estado de se preocupar com a proteção nacional. Os quatro casos citados afirmam como os governos ainda estão suscetíveis a ataques ou agressões cibernéticas. No entanto, a teoria não possui abrangência para uma guerra tecnológica, pois compreende apenas o conflito bélico físico, com a possibilidade de invasão com o uso de armas tradicionais. Assim, a teoria realista pode analisar o conflito, se desconsiderado que essa não entende a guerra tecnológica, por falta de atualização, e auxiliará o Estado apenas quanto à necessidade de proteção.

A Teoria da Interdependência Complexa pode ser considerada parcialmente correta, tendo em vista que a globalização e a interdependência dos Estados, quando algum agente entra em conflito, pode gerar impactos em outras nações. Um exemplo claro é o aumento do preço da gasolina no Brasil, devido ao conflito entre a Rússia e a Ucrânia, em consequência às sanções econômicas impostas pela União Europeia (BBC, 2022). No entanto, no caso da guerra cibernética, há a possibilidade de uma investida não gerar consequências visíveis para outras nações. Como no caso da invasão ao Ministério da Saúde que não gerou impactos em Estados

aliados ao Brasil, por exemplo. A vitória do ex-presidente Trump gerou consequências internacionais, diferentes de guerras físicas, de forma lenta e gradual, a longo prazo. Portanto, uma investida cibernética pode não desencadear um impacto negativo global visível e, assim, não seria completamente abrangente dentro da Teoria da Interdependência Complexa.

A Teoria da Dissuasão, como mencionado anteriormente, possui duas vertentes para análise, a nuclear e convencional. Aplicados aos casos mencionados, as guerras cibernéticas não podem ser enquadradas dentro do aspecto nuclear, por não se encaixarem dentro do conceito de armas nucleares. No entanto, podem possuir, também, tamanha capacidade de destruição, tendo em vista a possibilidade de invadir e controlar, não somente a vida privada de usuários da internet, como sistemas de governos, incluindo plataformas bélicas e materiais sigilosos.

De forma convencional, a guerra cibernética pode ser enquadrada como forma de persuasão, mas, devido sua recente aparição, pode não ser a principal forma bélica desejada e/ou temida. Portanto, uma ‘potência ciber-bélica’ pode não ter a mesma eficácia de persuasão que aquelas com formas militares tradicionais. No entanto, tendo em vista o aumento das buscas por tecnologia, transformando nações como o Japão em potências tecnológicas, a tendência é que esta nova forma de conflito seja cada vez mais procurada. Há, também, a possibilidade da criação de uma terceira via, dentro da teoria, para a contemplação da guerra tecnológica, visando suas peculiaridades dentre as outras formas bélicas já conhecidas, entendendo que sua influência pode ser menor que armas tradicionais, mas possuindo alto poder destrutivo.

Por fim, dentro do liberalismo, a teoria de *Soft* e *Hard Power* pode ser analisada da seguinte forma: a tecnologia usual, a qual sua atualização pode gerar inovações para a ciberguerra, é forma de influência cultural e econômica, mas não poderá analisar o conflito em questão. Já o *Hard Power* pode analisar a influência ‘ciber-bélica’ entre Estados. No entanto, tendo em vista que as ações de ciberguerra ainda são, em grande parte, sigilosas durante seu acontecimento, a notoriedade que as nações recebem será menor que aquela recebida através de uma guerra ou investimento bélico tradicional.

A teoria liberalista clássica não poderá ser analisada de forma total, tendo em vista que, esta analisa um mundo diferente daquele do Realismo, focando em questões de economia política internacional (IPE) e meio ambiente. Enquanto isso, sua antagonista está focada nas questões de segurança internacional, suas causas e condutas, e consequências da guerra - assuntos deste trabalho. (JERIS,1999)

Portanto, através das análises acima, as teorias mencionadas não seriam capazes de analisar o estilo de guerra em questão, tendo em vista que foram pensadas para conflitos físicos e tradicionais.

A seguir, apresenta-se um quadro comparativo que tem como objetivo fornecer uma representação visual da forma como cada teoria aborda a análise de cada caso mencionado anteriormente. Serão apresentados os fatores, se houver, que justifiquem a impossibilidade de utilizar essas teorias na análise. É importante ressaltar que as teorias serão analisadas de acordo com escopo disponível

Quadro Comparativo 01 - Capacidade analítica das Teorias das Relações Internacionais

Caso	Realismo Clássico	Liberalismo Clássico	Teoria da Interdependência Complexa	Teoria da Dissuasão	Soft and Hard Power
Ataques russos ao DNC	A teoria apresenta uma limitação na análise do caso em questão, uma vez que sua abrangência se restringe principalmente aos conflitos territoriais, deixando de considerar outros tipos de embate. Embora a teoria seja capaz de abordar a necessidade de proteção nacional diante de ameaças, ela não oferece informações mais abrangentes.	A teoria carece de abrangência para análise, uma vez que se concentra principalmente em questões econômicas e políticas internacionais.	A teoria em questão é parcialmente adequada para analisar o caso, uma vez que o evento gerou impactos em outros Estados, mesmo que estes não tenham sido imediatos.	A teoria em questão tem uma capacidade de análise parcial do caso, considerando a possibilidade de utilização da tecnologia em questão como forma de dissuasão no futuro, porém reconhece-se que esses armamentos não são tão efetivos em comparação com outras armas disponíveis. Além disso, considerando que o uso do software power como forma de conduzir guerras é uma prática relativamente recente, ainda não é considerado um meio bélico suficientemente poderoso para se enquadrar dentro da força dissuasória.	A teoria de Soft e Hard Power é parcialmente capaz de analisar o caso da ciberguerra. No entanto, apresenta limitações ao não considerar o sigilo das atividades bélicas cibernéticas, o que resulta em uma subestimação do poder de hard power dos Estados. Além disso, essa teoria não abrange outros agentes relevantes, como grupos de ciberterrorismo, e não reconhece o potencial da tecnologia como meio bélico significativo. Isso ocorre porque o uso do software power como forma de conduzir guerras é uma prática relativamente recente e ainda não é considerado suficientemente poderoso para se enquadrar no conceito de hard power.

Quadro Comparativo 02 - Capacidade analítica das Teorias das Relações Internacionais

Caso	Realismo Clássico	Liberalismo Clássico	Teoria da Interdependência Complexa	Teoria da Dissuasão	Soft and Hard Power
<p>Ataques às empresas energéticas da Ucrânia</p>	<p>A teoria apresenta uma limitação na análise do caso em questão, uma vez que sua abrangência se restringe principalmente aos conflitos territoriais, deixando de considerar outros tipos de embate. Embora a teoria seja capaz de abordar a necessidade de proteção nacional diante de ameaças, ela não oferece informações mais abrangentes.</p>	<p>A teoria carece de abrangência para análise, uma vez que se concentra principalmente em questões econômicas e políticas internacionais.</p>	<p>A teoria em questão não é adequada para analisar o caso, uma vez que o evento não gerou impactos diretos em outras nações, independente da integração entre os Estados.</p>	<p>A teoria em questão tem uma capacidade de análise parcial do caso, considerando a possibilidade de utilização da tecnologia em questão como forma de dissuasão no futuro, porém reconhece-se que esses armamentos não são tão efetivos em comparação com outras armas disponíveis. Além disso, considerando que o uso do software power como forma de conduzir guerras é uma prática relativamente recente, ainda não é considerado um meio bélico suficientemente poderoso para se enquadrar dentro da força dissuasória.</p>	<p>A teoria de Soft e Hard Power é parcialmente capaz de analisar o caso da ciberguerra. No entanto, apresenta limitações ao não considerar o sigilo das atividades bélicas cibernéticas, o que resulta em uma subestimação do poder de hard power dos Estados. Além disso, essa teoria não abrange outros agentes relevantes, como grupos de ciberterrorismo, e não reconhece o potencial da tecnologia como meio bélico significativo. Isso ocorre porque o uso do software power como forma de conduzir guerras é uma prática relativamente recente e ainda não é considerado suficientemente poderoso para se enquadrar no conceito de hard power.</p>

Quadro Comparativo 03 - Capacidade analítica das Teorias das Relações Internacionais

Caso	Realismo Clássico	Liberalismo Clássico	Teoria da Interdependência Complexa	Teoria da Dissuasão	Soft and Hard Power
Stuxnet	<p>A teoria apresenta uma limitação na análise do caso em questão, uma vez que sua abrangência se restringe principalmente aos conflitos territoriais, deixando de considerar outros tipos de embate. Embora a teoria seja capaz de abordar a necessidade de proteção nacional diante de ameaças, ela não oferece informações mais abrangentes.</p>	<p>A teoria carece de abrangência para análise, uma vez que se concentra principalmente em questões econômicas e políticas internacionais.</p>	<p>A teoria em questão é parcialmente adequada para analisar o caso, uma vez que o evento gerou impactos em outros Estados, mesmo que estes não tenham sido imediatos.</p>	<p>A teoria é capaz de analisar o caso, levando em consideração o potencial de poder que a tecnologia em questão pode exercer em uma situação de dissuasão. No entanto, considerando que o uso do software power como forma de conduzir guerras é uma prática relativamente recente, ainda não é considerado um meio bélico suficientemente poderoso quanto outros armamentos.</p>	<p>A teoria de Soft e Hard Power é parcialmente capaz de analisar o caso da ciberguerra. No entanto, apresenta limitações ao não considerar o sigilo das atividades bélicas cibernéticas, o que resulta em uma subestimação do poder de hard power dos Estados. Além disso, essa teoria não abrange outros agentes relevantes, como grupos de ciberterrorismo, e não reconhece o potencial da tecnologia como meio bélico significativo. Isso ocorre porque o uso do software power como forma de conduzir guerras é uma prática relativamente recente e ainda não é considerado suficientemente poderoso para se enquadrar no conceito de hard power.</p>

Quadro Comparativo 04 - Capacidade analítica das Teorias das Relações Internacionais

Caso	Realismo Clássico	Liberalismo Clássico	Teoria da Interdependência Complexa	Teoria da Dissuasão	Soft and Hard Power
<p>Ataques ao site do Ministério da Saúde, no Brasil</p>	<p>A teoria apresenta uma limitação na análise do caso em questão, uma vez que sua abrangência se restringe principalmente aos conflitos territoriais, deixando de considerar outros tipos de embate. Embora a teoria seja capaz de abordar a necessidade de proteção nacional diante de ameaças, ela não oferece informações mais abrangentes.</p>	<p>A teoria carece de abrangência para análise, uma vez que se concentra principalmente em questões econômicas e políticas internacionais.</p>	<p>A teoria em questão não é adequada para analisar o caso, uma vez que o evento não gerou impactos diretos em outras nações, independente da integração entre os Estados.</p>	<p>A teoria em questão não é adequada para analisar o caso, uma vez que este não credita uma relação entre Estados que possa levar à uma possível dissuasão. Além disso, considerando que o uso do software power como forma de conduzir guerras é uma prática relativamente recente, ainda não é considerado um meio bélico suficientemente poderoso para se enquadrar dentro da força dissuasória.</p>	<p>A teoria de Soft e Hard Power é parcialmente capaz de analisar o caso da ciber guerra. No entanto, apresenta limitações ao não considerar o sigilo das atividades bélicas cibernéticas, o que resulta em uma subestimação do poder de hard power dos Estados. Além disso, essa teoria não abrange outros agentes relevantes, como grupos de ciberterrorismo, e não reconhece o potencial da tecnologia como meio bélico significativo. Isso ocorre porque o uso do software power como forma de conduzir guerras é uma prática relativamente recente e ainda não é considerado suficientemente poderoso para se enquadrar no conceito de hard power.</p>

Percebe-se, portanto, que as Teorias apresentadas individualmente apresentam deficiências em compreender os casos de ciberguerra. Conforme mencionado anteriormente, no capítulo III e ao longo deste capítulo, torna-se evidente a necessidade de expandir ou criar uma área de estudo voltada para o ciberterrorismo. Compreende-se que as Teorias Clássicas estão limitadas às ações bélicas tradicionais, que resultam na destruição de cidades e na aniquilação de nações, assim como à guerra de fronteiras, que envolve conflitos físicos - ou a sua mera possibilidade, como ocorreu durante a Guerra Fria.

As Teorias clássicas falham em apresentar atemporalidade paralelamente ao surgimento de novas formas de conflito, os quais divergem da forma imaginada de guerra, quando produzidas. Apesar de sua importância para as análises das Relações Internacionais, as teses não possuem a capacidade, sem uma possível reformulação ou, até mesmo, a criação de uma nova tese teórica, de analisar uma situação de grande importância, com potencial destrutivo e de crescente incidência dentro do cenário internacional. Além disso, as teorias não atribuem importância a agentes além dos Estados ao analisar um cenário de conflito, deixando de considerar a relevância de ações significativas de ciberterrorismo.

CONSIDERAÇÕES FINAIS

Seriam as teorias clássicas das relações internacionais suficientes para compreender a ciberguerra? O objetivo principal deste trabalho era responder a essa pergunta, considerando a importância da tecnologia como um símbolo de inovação, com potencial tanto positivo quanto negativo para a transformação da sociedade. Ao longo da história, várias inovações tiveram um impacto significativo na humanidade, desde descobertas primordiais até avanços tecnológicos recentes. No contexto das Relações Internacionais, as teorias clássicas, como o Realismo e o Liberalismo, foram desenvolvidas para analisar os conflitos entre Estados e suas consequências.

No entanto, as teorias clássicas das Relações Internacionais mostraram-se inadequadas para uma compreensão abrangente da ciberguerra, que é uma forma emergente de conflito altamente relevante nos dias de hoje. Os conflitos eletrônicos apresentam desafios únicos, uma vez que suas ações ocorrem no espaço virtual, sem o uso direto da força física, e seus impactos podem não ser imediatamente perceptíveis. Além disso, essas ações podem ser realizadas por grupos além dos Estados, o que torna necessário considerar outros agentes como relevantes para esse tipo de situação.

As teorias clássicas, como o Realismo, o Liberalismo e a Teoria da Dissuasão, não foram originalmente concebidas para lidar com esse tipo de conflito, pois surgiram em um período em que a guerra por meio de softwares não era imaginada. Portanto, é necessário repensar ou desenvolver uma nova teoria capaz de analisar adequadamente a ciberguerra e suas implicações nas relações internacionais. Essa nova teoria deve levar em consideração a natureza sigilosa e sutil da ciberguerra, bem como suas consequências para a segurança nacional e a estabilidade global. Além disso, é essencial compreender como a ciberguerra se relaciona com outras formas de conflito, como o poder militar convencional e o poder econômico. Também é importante analisar novas formas de armamentos bélicos que não envolvem a destruição de fronteiras ou estruturas.

Portanto, é fundamental atualizar as teorias clássicas diante das novas formas de conflitos internacionais, especialmente os confrontos cibernéticos, a fim de obter uma compreensão abrangente e precisa das dinâmicas globais. A pesquisa, a análise teórica e a coleta de dados desempenham um papel crucial nesse processo, fornecendo uma base sólida para o desenvolvimento de uma nova teoria que aborde efetivamente a ciberguerra e suas implicações para a segurança internacional e a cooperação entre os Estados.

Além disso, considerando o surgimento de novos tipos de ataques e a importância do tema, é crucial que os Estados compreendam a relevância da ciberguerra e busquem formas de prevenção. Um exemplo é o Projeto de Lei no Brasil, denominado PL 2.630/2020, proposto pelo Senador Alessandro Vieira (CIDADANIA/SE) e intitulado Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Esse projeto estabelece diretrizes relacionadas à transparência das redes sociais e dos serviços de mensagens privadas, em especial no que diz respeito à responsabilidade dos provedores na luta contra a desinformação e no aumento da transparência na internet, incluindo a transparência em relação a conteúdos patrocinados e a atuação do poder público, além de estabelecer sanções para o descumprimento da lei.

O objetivo desse projeto é iniciar uma proteção nacional à população contra a disseminação de desinformação promovida pelas redes sociais, que muitas vezes têm fins lucrativos. Embora seja importante ressaltar que essa proposição não será suficiente para garantir uma proteção completa contra a ciberguerra, uma vez que esta não se limita apenas à propagação de notícias falsas, ela representa um marco inicial no reconhecimento dessa problemática - e não apenas pelo Brasil, mas também por outros países.

Entende-se que é necessário ir além desse projeto e adotar abordagens mais abrangentes e multifacetadas para lidar com os desafios. Isso envolve a implementação de medidas de segurança cibernética mais robustas, o fortalecimento da cooperação internacional e o

desenvolvimento de estratégias de defesa avançadas. Essas ações visam proteger os sistemas de informação, a infraestrutura crítica e a privacidade dos cidadãos em face das ameaças cibernéticas em constante evolução.

Por fim, considerando que a ciberguerra é um problema de natureza internacional, envolvendo diversos atores globais, surge a necessidade de desenvolver ou renovar uma teoria capaz de analisar esses casos e fornecer formas de prevenção. Conforme demonstrado anteriormente, as teorias clássicas não são adequadas para enfrentar esse desafio e, portanto, é imprescindível buscar abordagens teóricas atualizadas. A criação ou renovação de uma teoria adequada à ciberguerra é crucial para enfrentar os desafios e as ameaças emergentes nesse campo. Isso permitiria uma compreensão mais abrangente e precisa do problema, bem como a formulação de estratégias e políticas eficazes para garantir a segurança e promover a estabilidade nacional.

REFERÊNCIAS

A implacável guerra secreta contra o programa nuclear do Irã - BBC News Brasil. BBC News Brasil. Disponível em: <<https://www.bbc.com/portuguese/internacional-55485951>>. Acesso em: 30 abr. 2023.

ANGELL, Norman. A Grande Ilusão, São Paulo: UnB, 2002.

Ataque de hackers derruba rede de energia da Ucrânia - 07/01/2016 - Mercado - Folha de S. Paulo. Uol.com.br. Disponível em: <<https://m.folha.uol.com.br/mercado/2016/01/1726880-ataque-de-hackers-derruba-rede-de-energia-da-ucrania.shtml>>. Acesso em: 30 abr. 2023.

AUGUSTO, Thaís. Sites da Saúde e ConecteSUS saem do ar após ataque hacker; PF é acionada. Uol.com.br. Disponível em: <<https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2021/12/10/ministerio-da-saude-diz-que-pf-investigara-ataque-hacker.htm>>. Acesso em: 30 abr. 2023.

BUXTON, Oliver. Stuxnet: o que é e como funciona? Stuxnet: o que é e como funciona? Disponível em: <<https://www.avast.com/pt-br/c-stuxnet#:~:text=O%20Stuxnet%20foi%20criado%20por,dos%20EUA%20e%20de%20Israel.>>>. Acesso em: 30 abr. 2023.

CASTRO, Thales. Teoria das Relações Internacionais. [S. l.: s. n.], 2012.

DA REDAÇÃO. Hackers ligados à Rússia atacam empresa de energia ucraniana. VEJA. Disponível em: <<https://veja.abril.com.br/mundo/hackers-ligados-a-russia-atacam-empresa-de-energia-ucraniana/>>. Acesso em: 30 abr. 2023.

DICIO. [S. l.: s. n.], 2023. Disponível em: <https://www.dicio.com.br/>. Acesso em: 10 abr. 2023.

Götz, E. & Staun, J. (2022). Why Russia attacked Ukraine: Strategic culture and radicalized narratives. Contemporary Security Policy, 43(3), 482-497. <https://doi.org/10.1080/13523260.2022.208263>

GZH. Site do Ministério da Saúde sofre ataque e sai do ar; app ConecteSUS também tem problemas | GZH. GZH. Disponível em: <<https://gauchazh.clicrbs.com.br/saude/noticia/2021/12/site-do-ministerio-da-saude-sofre-ataque-e-sai-do-ar-app-conectesus-tambem-tem-problemas-ckx02g02c00f8014cwczt0o3c.html>>. Acesso em: 30 abr. 2023.

HERNANDES, Raphael. Quem é e como opera o grupo hacker Lapsus\$ e sua ligação com o Brasil. Folha de S. Paulo. Disponível em: <<https://www1.folha.uol.com.br/tec/2022/04/grupo-hacker-lapsus-exporta-malandragem-brasileira.shtml>>. Acesso em: 30 abr. 2023.

JACKSON, ROBERT; SØRENSEN, GEORGE. Introdução às Relações Internacionais. [S. l.: s. n.], Zahar, 2018.

JERVIS, Robert. Realism, Neoliberalism, and Cooperation. *International Security*, v. 24, n. 1, p. 42-63, 1999.

JOÃO PONTES, Nogueira; MESSARI, Nizar. *Teoria das Relações Internacionais*. [S. l.: s. n.], Elsevier, 2005.

JÚNIOR, Augusto W. M. Teixeira; SILVA, Antonio Henrique Lucena. *Introdução aos Estudos Estratégicos*. Curitiba: InterSaberes, 2020.

KASPERSKY. BlackEnergy APT Attacks in Ukraine. www.kaspersky.com. Disponível em: <<https://www.kaspersky.com/resource-center/threats/blackenergy>>. Acesso em: 30 abr. 2023.

KASPERSKY. Ransomware: definição, prevenção e remoção. www.kaspersky.com.br. Disponível em: <<https://www.kaspersky.com.br/resource-center/threats/ransomware>>. Acesso em: 30 abr. 2023.

LEVINE, Sam. Top Congress Members Call for Investigation into Russian Interference in The Election. *HuffPost*. Disponível em: <https://www.huffpost.com/entry/chuck-schumer-russia-investigation_n_584c1f4de4b0e05aded4329f>. Acesso em: 30 abr. 2023.

MEARSHEIMER, J. J. nuclear weapons and Deterrence in Europe. *International Security*, v. 9, n. 3, p. 19-46, 1985.

MORGENTHAU, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. New York: Knopf, 1948.

MUELLER, Robert S. et al. Report on The Investigation into Russian Interference in the 2016 Presidential Election. Washington, D.C.: U.S. Department of Justice, 2019. Disponível em: <https://www.justice.gov/storage/report.pdf>. Acesso em: 30 abr. 2023.

Nye, J. S.; Keohane, R. O. *Power and interdependence: World politics in transition*. Little, Brown, 1977.

NYE, Joseph S. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2004.

POR QUE guerra na Ucrânia aumenta preço da gasolina e do diesel no Brasil: resumo. [S. l.], 11 mar. 2022. Disponível em: <https://www.bbc.com/portuguese/brasil-60711085>. Acesso em: 9 maio 2023.

SAGAN, Scott D.; WALTZ, Kenneth N. (eds.) *The Spread of nuclear weapons: A Debate*. New York: W.W. Norton, 1995

Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. *Tecnologia e Games*. Disponível em: <<https://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>>. Acesso em: 30 abr. 2023.

SARFATI, Gilberto. Teoria das Relações Internacionais. [S. l.]: Editora Saraiva, 2011.

SEGUNDO. Ucrânia tem segundo apagão elétrico causado por hackers | G1 - Tecnologia e Games - Segurança Digital. Disponível em: <<https://g1.globo.com/tecnologia/blog/seguranca-digital/post/ucrania-tem-segundo-apagao-eletrico-causado-por-hackers.html>>. Acesso em: 30 abr. 2023.

SENADO FEDERAL. Projeto de Lei nº 2.630, de 2020. Estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas. Brasília, DF, 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: 19 maio 2023.

SHLAPENTOKH, D. Putin and Ukraine: power and the construction of history. Demokratizatsiya: The Journal of Post-Soviet Democratization, v. 29, n. 1, p. 87-100, 2021.

THE FOURTEEN Points. [S. l.], 2022. Disponível em: <https://www.theworldwar.org/learn/peace/fourteen-points>. Acesso em: 17 abr. 2023.

Trump Links C.I.A. Reports on Russia to Democrats' Shame Over Election (Published 2016). The New York Times, 2023. Disponível em: <<https://www.nytimes.com/2016/12/11/us/politics/trump-russia-democrats.html>>. Acesso em: 30 abr. 2023.

VALENTE, L. Política externa na era da informação: o novo jogo de poder, as novas diplomacias e a mídia como instrumentos de Estado nas relações internacionais. Rio de Janeiro: Revan/UFF, 2007.

WALTZ, Kenneth N. Man, the State, and War: A Theoretical Analysis. New York: Columbia University Press, 1959.

WALTZ, Kenneth N. Theory of International Politics. Reading, MA: Addison-Wesley, 1979.

LISTA DE CONCEITOS

Hardware: Equipamento ou componente físico que integram algum sistema de tecnologia. Em situações de computadores, entende-se hardware como as peças que compõem para sua construção, como unidades de armazenamento (como HDs ou SSDs), placas-mãe e, até mesmo, dispositivos de entrada e saída (mouse, monitor, pen drives etc.).

Malware: Qualquer tipo de software malicioso, que tem objetivo de prejudicar ou explorar dispositivos, serviços ou redes alheias. Conhecidos popularmente como ‘vírus de computador’ e ‘worm’.

Software: Pode ser definido como programas, dados ou instruções que comandam o funcionamento de um computador ou eletrônico. Como exemplo, o sistema Windows é um software de computadores.