UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO RELAÇÕES INTERNACIONAIS

Ana Clara Ferreira Leonetti

Efeitos de Hegemonia em Instituições Multilaterais: Um Estudo de Caso das Políticas de Cibersegurança da Organização dos Estados Americanos

Florianópolis

2025

Ana Clara Ferreira Leonetti

O Efeito da Hegemonia Estadunidense nas Instituições Multilaterais: Um Estudo de Caso das Políticas de Cibersegurança da Organização dos Estados Americanos

Trabalho de Conclusão de Curso submetido ao curso de Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharela em Relações Internacionais

Orientadora: Profa. Graciela de Conti Pagliari, Dra.
Coorientador: Prof. Gustavo Fornari Dall'Agnol, Dr.

Florianópolis

2025

Leonetti, Ana Clara Ferreira
Efeitos de Hegemonia em Instituições Multilaterais : Um Estudo de Caso das Políticas de Cibersegurança da Organização dos Estados Americanos / Ana Clara Ferreira Leonetti ; orientadora, Graciela De Conti Pagliari, coorientador, Gustavo Fornari Dall'Agnol, 2025.
88 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Graduação em Relações Internacionais, Florianópolis, 2025.

Inclui referências.

1. Relações Internacionais. 2. Organizações Internacionais. 3. Cibersegurança. 4. Hegemonia. 5. Estados Unidos. I. Pagliari, Graciela De Conti. II. Dall'Agnol, Gustavo Fornari. III. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. IV. Título.

Ana Clara Ferreira Leonetti

O Efeito da Hegemonia Estadunidense nas Instituições Multilaterais: Um Estudo de Caso das Políticas de Cibersegurança da Organização dos Estados Americanos

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Bacharela em Relações Internacionais e aprovado em sua forma final pelo Curso Relações Internacionais

Florianópolis, 02 de dezembro de 2025.

Banca examinadora

Profa. Graciela de Conti Pagliari, Dra.
Orientadora

Profa. Camila Feix Vidal Dra.
Universidade Federal de Santa Catarina

Guilherme Boscardin Espindola, Me.
Universidade Federal de Santa Catarina

Florianópolis, 2025.

AGRADECIMENTOS

Agradeço à minha família, amigos e a todas as pessoas queridas que estiveram ao meu lado lendo, escrevendo e pensando em companhia desde o início até aqui. Em especial dedico esse agradecimento à minha avó Vera, que, embora tenha partido deste mundo durante a produção deste trabalho, deixou para seus descendentes e amigos a memória de um grande exemplo de dedicação ao aprendizado, ao carinho e ao ensino, sempre em busca de um futuro melhor. A ela, o mérito de sempre me incentivar a ler não só as palavras, mas o mundo. De me ensinar a interpretar a vida com inteligência e sabedoria, sem se deixar levar por ideologias dominantes, mas sem nunca deixar a crítica encobrir o brilho da esperança.

RESUMO

Este trabalho investiga o efeito da hegemonia dos Estados Unidos (EUA) nas políticas de cibersegurança da Organização dos Estados Americanos (OEA). O estudo postula que as referidas políticas são influenciadas pelos EUA, na medida em que as instituições internacionais são cenários de reprodução das estruturas de poder vigentes no Sistema Internacional. A pesquisa adota o Realismo Ofensivo de John Mearsheimer como referencial teórico principal. Essa teoria postula que os Estados agem em um sistema anárquico, buscando incessantemente maximizar seu poder relativo e alcançar a hegemonia regional, sendo esta a maior garantia de segurança. O estudo considera o ciberespaço como uma nova e relevante arena para a manifestação dessas dinâmicas de poder e competição interestatal. A cibersegurança, definida como as ações políticas para salvaguardar o espaço digital, constitui um componente estratégico fundamental para a projeção e manutenção da hegemonia. A metodologia emprega um estudo de caso qualitativo exploratório, analisando a política de cibersegurança da OEA no período de 2015 a 2024. O objetivo é esclarecer como o fenômeno geral da influência hegemônica se manifesta na instituição regional. A análise empírica utiliza fontes primárias como os relatórios anuais da OEA e do Comitê Interamericano Contra o Terrorismo (CICTE), confrontando-os com documentos estratégicos de cibersegurança do Departamento de Defesa (DoD) e Estratégias Nacionais Cibernéticas dos EUA. O arcabouço teórico discute o desenvolvimento da OEA, sua transição para o conceito de segurança multidimensional no início do século XXI, e a evolução do enfoque de segurança estadunidense do anticomunismo para o antiterrorismo. Essa transição estratégica alinha a organização às prioridades de segurança dos EUA. A hegemonia se manifesta por meio de três vetores de maximização de poder: econômico, produtivo (discurso e normas) e material (tecnologia), todos utilizados para moldar a governança digital internacional.

Palavras-chave: cibersegurança; Estados Unidos da América; Organização dos Estados Americanos.

ABSTRACT

This study investigates the effect of United States (US) hegemony on the cybersecurity policies of the Organization of American States (OAS). It argues that these policies are influenced by the US insofar as international institutions operate as arenas for the reproduction of the prevailing power structures of the international system. The research adopts John Mearsheimer's Offensive Realism as its main theoretical framework. This theory posits that states act within an anarchic system, relentlessly seeking to maximize their relative power and achieve regional hegemony, which constitutes the highest guarantee of security. The study considers cyberspace as a new and significant arena for the manifestation of these dynamics of power and interstate competition. Cybersecurity, defined as the set of political actions aimed at safeguarding the digital domain, is thus a fundamental strategic component for the projection and maintenance of hegemony. The methodology employs an exploratory qualitative case study, analyzing OAS cybersecurity policy from 2015 to 2024. The aim is to clarify how the broader phenomenon of hegemonic influence manifests within the regional organization. The empirical analysis relies on primary sources such as annual reports from the OAS and the Inter-American Committee against Terrorism (CICTE), comparing them with cybersecurity strategic documents issued by the US Department of Defense (DoD) and US National Cyber Strategies. The theoretical framework discusses the development of the OAS, its transition to the concept of multidimensional security in the early twenty-first century, and the evolution of the US security approach from anti-communism to counterterrorism. This strategic shift aligns the organization with US security priorities. Hegemony manifests through three vectors of power maximization—economic, productive (discourse and norms), and material (technology)—all of which are employed to shape international digital governance.

.

Keywords: cybersecurity; United States of America; Organization of American States.

LISTA DE ABREVIATURAS E SIGLAS

CDMA	Conferência de Ministros da Defesa das Américas
CICTE	Comitê Interamericano contra o Terrorismo
CICAD	Comissão Interamericana para o Controle do Abuso de Drogas
CIJ	Comissão Jurídica Interamericana
CITEL	Comissão Interamericana de Telecomunicações
CSH	Conselho de Segurança Hemisférica
CSIRTS	Equipes de Resposta a Incidentes de Segurança Cibernética
DEIR	Departamento de Relações Internacionais
DLC	Departamento de Cooperação Jurídica
DoD	Departamento de Defesa dos Estados Unidos da América
DOITS	Departamento de Serviços de Informação e Tecnologia
DPI	Direitos de Propriedade Intelectual
EUA	Estados Unidos da América
GELAVEX	Grupo de Peritos para o Controle da Lavagem de Ativos e Financiamento do Terrorismo
JID	Junta Interamericana de Defesa
Mercosul	Mercado Comum do Sul
MFCS	Marco de Fortalecimento das Capacidades em Cibersegurança
OEA	Organização dos Estados Americanos
OTAN	Organização do Tratado do Atlântico Norte
PCCIP	Comissão Presidencial para a Proteção de Infraestruturas Críticas
PROSUL	Fórum para o Progresso da América do Sul
REMJA	Reunião de Ministros da Justiça e Outros Ministros ou Procuradores-Gerais das Américas
SSM	Secretaria de Segurança Multidimensional
TIAR	Tratado Interamericano de Assistência Recíproca

UNASUL	União de Nações Sul-Americanas
USCYBERCOM	Comando Cibernético dos EUA

SUMÁRIO

INTRODUÇÃO..... 11

1 HEGEMONIA E INSTITUIÇÕES..... 15

1.1 REALISMO OFENSIVO..... 15

1.2 CONTRAPONTOS AO REALISMO..... 21

1.2.1 O Institucionalismo da Teoria da Segurança Coletiva..... 22

1.2.2 Neoliberalismo e Institucionalismo Liberal..... 23

1.2.3 Instituições para a Teoria Crítica..... 25

1.3 DEFINIÇÕES TEÓRICAS..... 28

2 O DESENVOLVIMENTO HISTÓRICO DA OEA..... 32

2.1 ANTECEDENTES E FUNDAÇÃO..... 32

2.2 POLÍTICAS E ÓRGÃOS DE SEGURANÇA..... 36

2.3 ATUAÇÃO DOS EUA..... 41

3 CIBERSEGURANÇA..... 46

3.1 O CIBERESPAÇO E OS FUNDAMENTOS DE CIBERSEGURANÇA..... 46

3.2 CIBERSEGURANÇA, GEOPOLÍTICA E PODER NAS RI..... 51

3.3 POLÍTICAS DE CIBERSEGURANÇA E HEGEMONIA ESTADUNIDENSE.. 54

4 ESTUDO DE CASO..... 62

4.1 POLÍTICAS DE CIBERSEGURANÇA DA OEA DE 2015 A 2024..... 63

4.2 INTERESSES DOS EUA EM CIBERSEGURANÇA..... 71

4.3 MATERIALIZAÇÃO DOS INTERESSES DOS EUA NA OEA..... 74

5 CONSIDERAÇÕES FINAIS..... 80

REFERÊNCIAS..... 83

INTRODUÇÃO

O avanço das tecnologias digitais tem ampliado a importância da cibersegurança nas relações internacionais, tornando-a uma questão central nas estratégias de poder estatal. No tocante à relação entre cibernética e poder, Joseph S. Nye coloca que “O poder depende do contexto, e o rápido crescimento do ciberespaço é um novo contexto importante na política mundial” (Nye, 2011, p. 5, tradução nossa), ou seja, o meio cibernético consiste em uma nova e relevante arena de atuação das relações de poder entre Estados, e destarte, as políticas relacionadas à cibernética e especialmente à cibersegurança dos países influenciam diretamente na geopolítica internacional.

Nas Américas, a Organização dos Estados Americanos destaca-se como um fórum multilateral essencial para a formulação de políticas de cibersegurança, promovendo iniciativas de cooperação regional em resposta às crescentes ameaças digitais. No entanto, considerando a forte ligação entre a cibernética e a geopolítica, a análise dessas políticas exige uma perspectiva que avalie não apenas sua eficácia técnica, mas também o impacto das dinâmicas de poder regional sobre sua instituição, aplicação e funcionamento.

Inserida em um Sistema Internacional anárquico, a OEA, como outras organizações multilaterais, atua em um contexto onde a busca por poder e segurança molda as interações entre seus membros. Sob a perspectiva do Realismo Ofensivo, que enfatiza a busca pela maximização do poder material e a consolidação da hegemonia regional (MEARSHEIMER, 2001), as iniciativas de cibersegurança da OEA podem ser analisadas como elementos que refletem diretamente as capacidades hegemônicas dos Estados Unidos (EUA). Ao investigar como essas políticas corroboram com o controle e a influência estadunidense sobre os Estados da América Latina e Caribe, esta pesquisa busca elucidar o efeito da hegemonia estadunidense sobre o desenvolvimento das políticas de cibersegurança da OEA. A hipótese principal que guia este trabalho consiste na ideia de que as políticas de cibersegurança da OEA sofrem influência da hegemonia dos EUA, na medida em que instituições internacionais são cenários de reprodução das estruturas de poder vigentes no Sistema Internacional.

A escolha de tais objetos de pesquisa se dá por dois fatores principais. Primeiramente, por ser a área de domínio da potência hegemônica regional mais forte na atualidade, os EUA. O segundo motivo é ser a região onde a presente pesquisa é desenvolvida, de forma que há familiaridade com os fenômenos que permeiam o continente e sua realidade, convergindo em proximidade física, histórica e cultural entre o território estudado e a autoria do trabalho. Assim, combina-se relevância com afinidade.

Nesse sentido, surge a necessidade de estudar as políticas de cibersegurança da OEA não de forma neutra e isolada de seu contexto político e estratégico, mas considerando as implicações da balança de poder e da manutenção da hegemonia regional que paira no continente, a hegemonia estadunidense na criação das políticas de defesa (com foco na cibersegurança) da instituição. Frente a essa demanda, se apresenta a urgência de pesquisar como a abordagem de cibersegurança da Organização dos Estados Americanos emula essa dinâmica de poder presente, sustentando os interesses de hegemonia dos EUA. Estudar a segurança cibernética no continente americano por essa perspectiva fornece a possibilidade de entender as implicações da cibersegurança para a independência tecnológica e segurança da América Latina e os desafios a serem enfrentados nessa área progressivamente relevante nas Relações Internacionais.

Quanto à metodologia, este trabalho adota um estudo de caso qualitativo, definido por John Gerring como “um estudo aprofundado de uma única unidade onde a meta do acadêmico é elucidar características de uma classe ampliada do mesmo fenômeno” (Gerring, 2004, p. 341, tradução nossa). A unidade de análise é a política de cibersegurança da OEA, observada ao longo de um período delimitado de tempo: de 2015 a 2024. O fenômeno ampliado a ser elucidado se refere a como potências hegemônicas manifestam seus interesses em organizações internacionais e como estas refletem a estrutura de poder global. O estudo de caso se encaixa na categoria de exploratório, com a finalidade de esclarecer como um fenômeno geral ocorreu em um cenário particular.

A análise empírica será realizada através da investigação da relação causal entre as duas variáveis (políticas de cibersegurança da OEA e interesse hegemônico dos EUA) ao longo do tempo. As fontes primárias da Organização incluem os Relatórios Anuais da OEA publicados de 2015 a 2023; os Relatórios

Anuais do CICTE dos anos 2021 a 2023 e o documento "*2024 Cybersecurity Program*". A inclusão dos Relatórios do Comitê Interamericano contra o Terrorismo (CICTE) só foi feita a partir de 2021 devido a uma alteração no formato do Relatório Anual geral da organização que fez com que, nos documentos a partir daquele ano, as medidas de cibersegurança deixassem de ser detalhadas. A inclusão dos documentos do CICTE permite uma visão mais específica sobre as atividades de segurança cibernética da instituição nesse período. Já a utilização de um documento distinto para o ano de 2024 se deve à indisponibilidade, na data deste estudo, de um Relatório Anual geral ou específico do CICTE para o referido ano. Quanto à segunda variável, a identificação dos interesses dos Estados Unidos em cibersegurança será realizada por meio da análise dos seguintes documentos estratégicos: a Estratégia Cibernética do Departamento de Defesa (DoD) de 2015; a Estratégia Cibernética Nacional dos Estados Unidos de setembro de 2018, notável por ser a primeira estratégia cibernética completamente articulada em 15 anos; a Visão de Comando para o Comando Cibernético dos EUA (USCYBERCOM) de 2018; a Estratégia Nacional de Cibersegurança de março de 2023; e o Plano de Implementação da Estratégia Nacional de Cibersegurança (NCSIP) de maio de 2024.

Para amparar o desenvolvimento do estudo de caso, o primeiro capítulo é dedicado à realizar uma revisão bibliográfica a respeito da teoria adotada, o Realismo ofensivo. A partir de uma revisão conceitual focada em instituições internacionais, são apresentados os modos pelos quais a hegemonia se manifesta em seu funcionamento e estrutura, buscando construir uma base teórica robusta para a análise. Em seguida, são discutidas as principais abordagens institucionalistas, como o institucionalismo liberal, o institucionalismo da segurança coletiva e a teoria crítica. A partir dessa exposição, o trabalho adota e aprofunda a perspectiva do Realismo Ofensivo de John Mearsheimer como referencial teórico principal, considerando-a a mais adequada para compreender as dinâmicas de poder em contextos regionais marcados por assimetrias de poder, como o da OEA.

No segundo capítulo é desenvolvido o histórico da OEA, a partir de fontes secundárias e de fontes primárias extraídas do site oficial da instituição. É introduzido, então, o estudo específico da Organização dos Estados Americanos, desenvolvendo uma pesquisa historiográfica para analisar a influência da hegemonia nas instâncias multilaterais. O objetivo é compreender os marcos de sua

criação, a evolução institucional e o papel desempenhado pelos EUA em seu desenvolvimento. A seção aprofunda a análise da evolução das políticas de segurança da OEA, identificando as diretrizes adotadas, a transição para a segurança multidimensional e como elas se relacionam com a balança de poder em cada momento.

Posteriormente, o terceiro capítulo visa estabelecer as bases teóricas e conceituais essenciais para entender a cibersegurança como um elemento de poder e de manifestação hegemônica no cenário internacional. Inicialmente, serão definidas as noções de ciberespaço, ciberpoder e cibersegurança. Em seguida, o capítulo abordará o caráter político e estratégico da tecnologia, conectando-o à teoria realista e à hegemonia dos Estados Unidos. Será demonstrado como a cibersegurança se transforma em instrumento de poder e hegemonia, principalmente através da disseminação de doutrinas e terminologias para documentos de políticas em fóruns multilaterais.

Por fim, o último e quarto capítulo desenvolve o estudo de caso empírico, utilizando os documentos oficiais da OEA e as estratégias de cibersegurança dos EUA de 2015 a 2024. A primeira seção descreve as políticas da OEA no período, focando em suas ações de capacitação e apoio à criação de estratégias nacionais. A segunda seção apresenta os interesses de cibersegurança dos EUA, fundamentados em seus documentos estratégicos. Finalmente, a terceira seção estabelece a conexão entre os interesses norte-americanos e as diretrizes da OEA, examinando a concretização dessa influência. Além disso, desenvolve uma análise crítica sobre as limitações da atuação das instituições internacionais diante de interesses hegemônicos.

1 HEGEMONIA E INSTITUIÇÕES

Neste capítulo, será realizada uma revisão conceitual sobre as instituições internacionais e os modos pelos quais a hegemonia se manifesta em seu funcionamento e estrutura. O objetivo é construir uma base teórica robusta que sustente a análise proposta neste trabalho. Para tanto, serão discutidas as principais abordagens institucionalistas das Relações Internacionais, como o institucionalismo liberal, o institucionalismo da segurança coletiva e o institucionalismo da teoria crítica. A partir dessa exposição, busca-se não apenas apresentar o panorama do debate teórico, mas também evidenciar os pontos de convergência e divergência entre as escolas analisadas, com atenção especial à maneira como concebem a relação entre instituições e poder.

Haja vista a revisão teórico-conceitual realizada, o trabalho adota a perspectiva do Realismo Ofensivo como referencial teórico principal, por considerá-la a mais adequada para compreender as dinâmicas de poder que atravessam o funcionamento das instituições internacionais — especialmente em contextos regionais marcados por assimetrias de poder, como o da Organização dos Estados Americanos (OEA). O Realismo Ofensivo, ao enfatizar a centralidade da competição interestatal, a lógica da sobrevivência e a busca incessante pela maximização de poder, oferece instrumentos analíticos particularmente úteis para interpretar como potências hegemônicas utilizam instituições multilaterais para expandir e consolidar sua influência, mesmo sob o verniz da cooperação internacional.

1.1 REALISMO OFENSIVO

A teoria realista das relações internacionais é uma das teorias mais antigas da disciplina, mas o nome “realismo” é bastante recente nessa área, marcado pela publicação do livro “Vinte Anos de Crise, 1919-1939” de E. H. Carr[1], datado de 1939. Este livro caracteriza muito bem os princípios do pensamento realista, pois seu cerne consiste na crítica de Carr ao pensamento utópico popular aos cientistas da política internacional no pós-Primeira Guerra Mundial, os quais tendiam, segundo ele, a focar suas análises em como o sistema deveria funcionar e não em como ele

[1] Carr postulou alguns dos princípios da teoria realista, mas vale ressaltar que suas ideias seguem muitos princípios marxistas e esse aspecto não deve ser desconsiderado quando sua teoria é utilizada.

realmente funciona. Em oposição a essa utopia, Carr propôs uma ciência política centrada no pragmatismo e na observação empírica da realidade, o que caracteriza a teoria realista desde então até os seus posteriores desenvolvimentos e ramificações (Carr, 1939).

A partir da proposição de um estudo não idealista das relações internacionais, alguns postulados foram estabelecidos sobre o funcionamento do Sistema Internacional. Entre eles, o mais fundamental consiste na visão do SI como um sistema anárquico, em que os Estados são os atores de soberania máxima e não se submetem a nenhum líder comum (Waltz, 1979). Esse cenário de anarquia foi comparado por muitos teóricos ao estado de natureza tanto de Thomas Hobbes quanto de Jean-Jacques Rousseau, nos quais os indivíduos não se submetem a qualquer lei maior, e, portanto, são movidos somente pelo desejo de preservação de sua própria segurança (Diniz, 2005, p. 16).

Perante a observação dessa característica central do sistema de Estados, John Herz definiu em 1950 o chamado “dilema da segurança” no seu texto intitulado *“Idealist Internationalism and the Security Dilemma*”. Nele, Herz defende que grupos ou indivíduos que convivem em um sistema anárquico geralmente se sentem ameaçados pelos outros grupos ou indivíduos do mesmo sistema e têm como principal preocupação manter sua própria segurança. Para tal, eles tendem a buscar o acúmulo de poder cada vez maior como meio de afastar e mitigar possíveis ataques de outros atores. Como sequela, essa postura de maximização de poder por parte de alguns causa nos outros grupos ou indivíduos ainda mais insegurança, o que, por sua vez, reabastece a necessidade de buscar por cada vez mais poder, em um “ciclo vicioso de acumulação de segurança e poder” (Herz, 1950, p. 157).

Entretanto, a existência do dilema de segurança não resulta necessariamente em um cenário de competição caótica e destrutiva, pois é contrabalançada por um terceiro fenômeno central à tradição realista: a balança de poder. Kenneth N. Waltz, expoente do realismo estrutural — corrente do neorrealismo —, descreve esse mecanismo como a tendência dos Estados a buscar o equilíbrio na distribuição do poder internacional, motivados por seu objetivo fundamental de autopreservação. Assim, os próprios Estados atuam para conter a concentração excessiva de poder por parte de um ou poucos atores, uma vez que percebem tal desequilíbrio como ameaça direta à sua segurança (Diniz, 2005, p. 60). Essa dinâmica está intrinsecamente relacionada ao dilema de segurança, na

medida em que o mesmo acúmulo de capacidades que gera desconfiança e estimula a busca por mais poder também é o alvo das ações de contenção promovidas por outros Estados. Ou seja, enquanto os atores estatais buscam ampliar suas capacidades, também agem para limitar a acumulação de poder alheio, com o objetivo primário de garantir sua própria sobrevivência.

Nesta concepção, a configuração do Sistema Internacional consiste em uma estrutura onde seus integrantes agem individualmente e estrategicamente, o que é definido por Waltz como o princípio de “auto-ajuda”. Esse princípio define que os Estados são os responsáveis pela sua própria sobrevivência e agem para garanti-la mesmo que em detrimento da segurança dos outros, na medida em que não existe qualquer líder maior que detenha o uso da força e seja capaz de protegê-los. (Ibid., p. 48). De forma similar, John J. Mearsheimer, teórico do Realismo Ofensivo, coloca que, como qualquer Estado representa uma ameaça para os demais e, simultaneamente, não há qualquer autoridade que os proteja uns dos outros, os Estados não podem depender de alguém além de si mesmos para sobreviver: “Na política internacional, Deus ajuda aqueles que ajudam a si mesmos”[2] (Mearsheimer, 2001, p. 33, tradução nossa).

O Realismo Ofensivo, desenvolvido por Mearsheimer, segue todos os princípios da teoria geral já citados, mas ressalta a busca por maximização de poder motivada pela busca pela sobrevivência. Em outras palavras, a teoria postula que a busca pela sobrevivência determina um comportamento agressivo por parte dos Estados, os quais não se satisfazem com o balanceamento da distribuição de poder no mundo e por isso almejam, como objetivo último, ser o Estado mais poderoso entre todos os existentes. Em outras palavras, o Realismo Ofensivo defende que a melhor maneira de garantir a segurança é obter a hegemonia, a qual, para o Realismo Ofensivo, consiste na dominação do sistema. (Ibid., 2001, p. 40, tradução livre). Tal efeito é causado principalmente pela incerteza que o sistema anárquico causa nos atores estatais, característica que, em combinação com a incapacidade de prever as ações de outros Estados, causa o ciclo de insegurança já descrito, o que culmina em um sistema de Estados altamente competitivo, onde cada país é encorajado a se sobrepor aos outros em função da otimização de seu próprio poder e segurança (Ibid, 2001, p. 29).

---

[2]Texto original: *“God helps those who help themselves.”* (Mearsheimer, 2001, p. 33)

Contudo, a aspiração de se tornar o hegemon global é contida pelo que Mearsheimer chama de o “poder parador das águas”. Esse obstáculo provém da característica geográfica do globo terrestre de ser composto por continentes separados por grandes corpos de água. Assim, para dominar outro país, uma nação precisaria transpor esses grandes oceanos para avançar suas forças terrestres sobre os territórios alheios e consolidar uma suposta hegemonia. O problema principal é, então, que a transposição dessas águas tem um custo militar, financeiro e logístico muito grande, o que torna o desembarque anfíbio muito difícil e por isso, na grande maioria das vezes, essa forma de ataque não compensa para o Estado que a considera. Tendo em vista que o poder parador das águas compõe um limite físico para a dominação militar intercontinental completa, constata-se que o melhor cenário possível para que uma grande potência maximize sua segurança é se tornar uma hegemonia regional (Ibid., 2001, p. 41).

Isto posto, urge a importância do poder relativo como objeto de aspiração dos atores estatais. Sendo impossível alcançar o maior poder absoluto do sistema na grande maioria das vezes, a prioridade dos Estados se torna maximizar seu poder relativo. Para Mearsheimer, teóricos realistas acreditam que “o sistema internacional força as grandes potências a maximizar seu poder relativo porque essa é a maneira ideal de maximizar sua segurança" (Ibid., 2001, p. 21, tradução nossa)[3]. Por conseguinte, o que importa para um Estado não é apenas o quanto de poder ele possui, mas quanto possui em relação aos demais. A noção de poder relativo é, portanto, fundamental para entender a lógica da competição interestatal: um aumento de poder só é vantajoso se resultar em uma posição de vantagem frente a possíveis rivais. Retomando a premissa do dilema da segurança, cada incremento de poder obtido por um ator é percebido como uma ameaça por seus concorrentes, o que estimula uma lógica de soma zero: o ganho de um é necessariamente a perda de outro.

Toda essa dinâmica e o comportamento estatal resultante dela são transpostos para o âmbito da cooperação internacional. Nesse sentido, frente à estrutura composta pelo princípio da auto-ajuda, a formação de alianças cooperativas entre Estados não é impossível, mas é frágil. As alianças são dadas como apenas temporárias, vigentes somente enquanto convenientes para os países

[3] Texto original: *“the international system forces great powers to maximize their relative power because that is the optimal way to maximize their security”* (Mearsheimer, 2001, p.21)

envolvidos nela (Ibid., 2001, p. 33). Além disso, o realismo postula que as relações nas organizações internacionais são provenientes de acordos entre Estados e só se mantém enquanto houver consentimento por parte deles (Diniz, 2005, p. 51). Assim dizendo, por mais que exista a possibilidade de cooperação frente a acordos bilaterais, acordos multilaterais e instituições internacionais, qualquer resolução proveniente destes só é possível enquanto há Estados soberanos a conduzindo, de maneira que os Estados e suas intenções de auto preservação permanecem como condutoras das relações internacionais.

A participação dos atores do Sistema Internacional em instituições de cooperação ocorre apenas enquanto for do interesse individual de cada Estado e, em especial, das grandes potências. Dessa forma, essas instituições não exercem as funções de um governo internacional efetivo, mas são inteiramente dependentes da vontade e dos objetivos dos Estados (Mearsheimer, 1995, p. 9). As regras e políticas formuladas no âmbito dessas organizações refletem diretamente os interesses estatais, que por sua vez são moldados pela distribuição de poder no sistema, incluindo a busca pela maximização do poder para garantir a sobrevivência e a aspiração à hegemonia. Assim, as instituições funcionam apenas como palcos onde se desenrolam as relações de poder, nunca como atores autônomos capazes de alterar essa estrutura fundamental (Ibid., p. 13). Conforme explica Kenneth Waltz, o Sistema Internacional é caracterizado pela busca constante de equilíbrio entre os Estados (no caso de sua teoria, predominantemente pela construção de capacidades de defesa; mas é possível aplicar essa ideia também de acordo com o Realismo Ofensivo de Mearsheimer), que agem para conter o crescimento excessivo do poder de seus rivais, reforçando a dinâmica competitiva na qual as instituições internacionais servem como arenas para disputas hegemônicas e mecanismos de contenção (Waltz, 2001, p. 60). Dessa maneira, as instituições atuam tanto como espaços quanto como ferramentas no jogo do poder relativo, contribuindo para a manutenção e a disputa contínua pela hegemonia no Sistema Internacional.

À vista disso, o Realismo Ofensivo aponta que as instituições são bastante frágeis e não garantem nenhuma mudança estrutural no Sistema Internacional. Tal porque refletem as estruturas de poder vigentes, e acabam servindo mais como um instrumento de manutenção do que de contestação ou alteração da balança de poder que reina no mundo. Isso ocorre porque os mecanismos de imposição que

acontecem no Sistema Internacional anárquico também existem dentro das organizações internacionais, países com mais poder material tem mais influência e maior capacidade de coerção, e países com menos poder ainda são obrigados a fazer concessões quando ameaçados. (Dabler, et al., 2024, p. 2).

Mearsheimer, por sua vez, argumenta que o Sistema Internacional é regido pela competição entre os países e pela dinâmica da balança de poder até os dias atuais e rebate argumentos liberais de que a cooperação entre nações tem crescido ao ponto de tornar o realismo obsoleto e ultrapassado. O autor defende que, até o século atual, as relações interestatais são regidas pela insegurança perante os outros Estados e que, por isso, os atores do sistema estão sempre em busca de maximizar sua segurança por meio do poder . A partir de sua observação do mundo atual, descreve que os maiores Estados do globo ainda consideram e se preocupam com a balança de poder descrita pelo realismo e, assim, ainda são motivados a competirem entre si. Por esse motivo, o realismo continua sendo a teoria mais adequada para a análise do Sistema Internacional, pois parte da observação de características reais sobre seu funcionamento, garantindo ferramentas teóricas precisas para descrever e prever o comportamento dos Estados (Mearsheimer, 2025). Assim, o teórico reforça que

> Os Estados ainda temem uns aos outros e procuram ganhar poder às custas uns dos outros, porque a anarquia internacional – a força motriz do comportamento das grandes potências – não mudou com o fim da Guerra Fria, e há poucos sinais de que tal mudança seja provável tão cedo. Os Estados continuam a ser os principais atores na política mundial e ainda não há nenhum guarda noturno acima deles. (Mearsheimer, 2001, p. 361, tradução nossa) [4]

Portanto, o realismo permanece relevante para a análise de fenômenos geopolíticos internacionais até a atualidade. As relações interestatais, bem como as instituições que interferem nelas, podem ser compreendidas e avaliadas a partir dos postulados dessa teoria, que fornece uma compreensão objetiva sobre essa realidade e possibilita a análise crítica de todos os mecanismos que as contemplam. Assim, cabe utilizar do arcabouço teórico realista para explorar os conceitos abordados nessa seção, sejam eles hegemonia e instituições, e como eles

[4] Texto original: "*States still fear each other and seek to gain power at each other-s expense, because international anarchy — the driving force behind great-power behavior — did not change with the end of the Cold War, and there are few signs that such chance is likely any time soon. States remain the principal actors in world politics and there is still no night watchman standing above them."*

interagem entre si no Sistema Internacional. Definir hegemonia e instituições a partir do Realismo Ofensivo permite solidificar a base teórica para o desenvolvimento deste estudo de maneira pragmática, clara e prática. A partir de então, os conceitos poderão ser aplicados na investigação específica sobre a hegemonia dos Estados Unidos e seus efeitos na instituição internacional nomeada Organização dos Estados Americanos.

Todavia, não se pode ignorar a existência de outras teorias das relações que tratam de instituições e hegemonia. No texto *"False Promise of International Institutions*", Mearsheimer aponta três teorias institucionalistas principais além do realismo: o institucionalismo liberal, a teoria da segurança coletiva e a teoria crítica (Mearsheimer, 1995, p. 14). Cada uma delas aborda as instituições do Sistema Internacional a partir de fundações teóricas e ideológicas particulares, e todas as três entram em embate com as premissas realistas supracitadas. Não obstante, nenhuma dessas teorias é tão pragmática e sólida quanto o institucionalismo a partir do Realismo Ofensivo, argumento que será desenvolvido nas próximas seções deste capítulo. Na seção a seguir, serão descritas as três teorias divergentes propostas acima e seus contrapontos à teoria realista, para contrastá-la com elas e, adiante, reforçar a superioridade do Realismo Ofensivo no contexto e finalidade propostos neste trabalho.

1.2 CONTRAPONTOS AO REALISMO

Embora o presente trabalho se ancore predominantemente na matriz do Realismo Ofensivo para analisar o impacto da hierarquia de poder na política de cibersegurança da Organização dos Estados Americanos (OEA), é imperativo reconhecer as importantes contribuições de perspectivas teóricas alternativas. Estas abordagens fornecem contrapontos essenciais à visão pessimista e materialista do Realismo, que tende a ver as instituições apenas como reflexos da distribuição de poder. Em particular, o Neoliberalismo Institucional, ao focar na possibilidade de ganhos absolutos e na capacidade das instituições de reduzir os custos de transação e mitigar a anarquia, e o Construtivismo, ao enfatizar a natureza socialmente construída das ameaças, normas e identidades (cruciais no ciberespaço), oferecem explicações alternativas para a existência e atuação da OEA. Contudo, a escolha metodológica de privilegiar a lente realista de John Mearsheimer reside na sua capacidade de oferecer a explicação mais robusta e

parcimoniosa para o cerne da pesquisa: a persistência da assimetria de poder e a instrumentalização da OEA como um veículo que reforça a hegemonia regional dos Estados Unidos, ao invés de atuar primariamente como um agente de cooperação autônoma ou de transformação identitária. A presente seção visa, portanto, apresentar e discutir criticamente estas perspectivas, reforçando o argumento de que a lógica da competição e da sobrevivência, central ao Realismo, se mantém como a força motriz fundamental subjacente à agenda de cibersegurança no hemisfério.

1.2.1 O Institucionalismo da Teoria da Segurança Coletiva

Anterior ao estabelecimento da nomenclatura “realismo” para a teoria apresentada na seção anterior a partir da publicação de Carr (Diniz, 2005, p. 16) já era bem estabelecida a abordagem idealista e otimista sobre as interações interestatais: o liberalismo. A teoria liberal das Relações Internacionais ganhou respaldo a partir da atuação de Woodrow Wilson, presidente dos Estados Unidos durante o fim da Primeira Guerra Mundial. Wilson perseguia a missão de disseminar valores democráticos pelo mundo como forma de evitar a ocorrência de novas grandes guerras. Esse pensamento era embasado na noção liberal, inicialmente introduzida pelo inglês John Locke, de um ser humano racional capaz de cooperar, que, transposta para o Sistema Internacional, indicava que os Estados seriam capazes também de cooperar entre si, enquanto atores desse sistema. A crença na cooperatividade e colaboração interestatal levava à visão de que era favorável para a prevenção de novas guerras a criação de organizações que viabilizassem essa cooperação entre Estados. (Jackson e Sorensen, 2007, p. 65)

Nesse contexto, o presidente estadunidense defendia um institucionalismo baseado na ideia de segurança coletiva. Em detalhes, a teoria da segurança coletiva diz respeito à perspectiva de que é vantajoso para todos os Estados construir, juntos, um arranjo organizacional transparente para administrar as relações de poder entre nações (Claude, 1962, p. 95). Wilson, então, propunha que todos os países realizassem suas ações diplomáticas e militares com transparência e mediante a regulação de um organismo internacional universal (Jackson e Sorensen, 2007, p. 65). Foi essa doutrina que inspirou e embasou a criação da Liga das Nações após a Primeira Guerra Mundial como um mecanismo institucional de prevenção de um novo conflito com a mesma grande magnitude da Primeira Guerra

Mundial, a qual falhou perante a ascensão da Segunda Guerra Mundial e foi sucedida pela Organização das Nações Unidas (ONU) (Orakhelashvili, 2011, p. 15).

Considerando que a teoria da segurança coletiva almeja gerenciar as relações de poder entre Estados e conter os conflitos gerados pelas competições entre eles, não se pode negar que essa corrente teórica admite a existência da balança de poder do Sistema Internacional (Claude, 1962, p. 95). Apesar disso, a teoria se mantém abertamente crítica ao realismo das Relações Internacionais, entrando em embate com a ideia de que a competição interestatal é inevitável e a opondo com a premissa de que a superação do estado de auto-ajuda e a concretização da paz podem existir mediante o compromisso de cada Estado com a cooperação. Sendo assim, as instituições internacionais exercem um papel de suma importância para a segurança coletiva, pois são o meio condutor da cooperação, estabelecendo a rede de normas e regras que viabilizariam a transparência e colaboração entre os atores estatais do sistema (Mearsheimer, 1995, p. 29).

Portanto, para essa corrente teórica, o papel das instituições não é anular as relações de poder, mas sim administrá-las em prol da paz. Segundo Inis L. Claude, Jr., grande referência dessa teoria, "grupos humanos serão sempre capazes de causar danos uns aos outros [...] A gestão do poder é o verdadeiro problema"[5] (Claude, 1962, p.7, tradução nossa). Contudo, nem todos os princípios realistas são aceitos como verdades, visto que para que a proposta da segurança coletiva se concretize, é necessário que os Estados se distanciem do comportamento egoísta de sobrevivência. Para tal, devem renunciar o uso do poder militar para manter o status quo; devem equalizar seu interesse individual com o interesse geral; e devem confiar uns nos outros (Mearsheimer, 1995, p. 28-29). Com efeito, o sucesso das instituições alinhadas às premissas dadas pela teoria da segurança coletiva depende do consentimento dos Estados, ou seja, depende que os atores estatais estejam comprometidos com esse sistema individualmente independente de qualquer ideologia que não a busca pela paz mundial (Orakhelashvili, 2011, p. 7).

---

[5] Texto original: *“[...] human groups will always be capable of doing damage to each other [...] The management of power is the real issue”* .

1.2.2 Neoliberalismo e Institucionalismo Liberal

Sem embargo, após o fracasso da Liga das Nações e o desenrolar da Segunda Guerra Mundial, as acusações de idealismo sobre a teoria da segurança coletiva ganharam força, e os próprios teóricos liberais passaram a buscar alternativas mais palpáveis para justificar a promoção da cooperação entre Estados. Ainda partindo do princípio de que o ser humano é capaz de ceder seu interesse individual em prol do bem comum e da organização da sociedade, buscavam reformular as críticas ao realismo de maneira mais alinhada aos acontecimentos da época. Assim, surgiu nos anos 1950 o que pode ser chamado de neoliberalismo das Relações Internacionais (Jackson e Sorensen, 2007, p. 80).

O contexto desse período era preenchido pela diversificação das relações entre Estados, com a complexificação das trocas econômicas e financeiras e maior divisão internacional do trabalho. Segundo a lógica do liberalismo, frente a essa conjuntura as vantagens em manter boas relações com outros países se tornavam cada vez mais relevantes. Nos anos 1970, Robert Keohane e Joseph Nye se destacaram como os estudiosos que desenvolveram essa ideia com mais profundidade. A partir disso, eles desenvolveram a teoria da interdependência complexa, segundo a qual os Estados tendem a cooperar justamente para manterem suas relações de troca, das quais se tornaram dependentes com a globalização (Ibid, p. 80).

A teoria da interdependência complexa é caracterizada pelo embate direto com a teoria realista, argumentando que os Estados não são os únicos atores do Sistema Internacional, o poder militar não se sobrepõe a outras formas de poder e que ele nem sequer é uma forma eficiente de fazer política internacional (Keohane e Nye, 1997, p. 20). Pelo contrário, nesse viés, o sistema de Estados conta com múltiplos canais de interação que vão além das relações interestatais tradicionais, incluindo vínculos diretos entre burocracias governamentais, atores não estatais e organizações transnacionais. Além disso, a agenda internacional é composta por diversos temas (como meio ambiente, economia e direitos humanos) que não seguem uma hierarquia fixa, de modo que a segurança militar deixa de ocupar posição privilegiada. Por fim, o uso da força militar torna-se improvável entre países interdependentes em contextos onde predominam vínculos complexos, sendo

ineficaz como instrumento de resolução de conflitos em muitas dessas situações (Ibid., p. 21).

É possível considerar que a visão neoliberal das instituições foi desenvolvida a partir da fundação teórica fornecida por Keohane e Nye, e que foi a partir daí que se consolidou o institucionalismo liberal. (Jackson e Sorensen, 2007, p. 80). A teoria coloca os Estados como atores de interesses auto-centrados, assim como o realismo, mas aponta que a cooperação pode sim ocorrer quando os interesses comuns se sobrepõem aos interesses conflitantes entre países. Todavia, somente a existência de interesses comuns não garante o alinhamento entre atores estatais, pois o aspecto de incerteza presente no Sistema Internacional pode inibir a confiança entre Estados e minar as possibilidades de acordos e alianças. Com efeito, é para reduzir essa incerteza e limitar as assimetrias que as instituições devem existir e atuar (Keohane, 1984, p. 12). Ademais, citando o argumento realista de que a presença de um hegemon no Sistema Internacional contribui para a regulação do comportamento dos países do mundo e estabiliza a balança de poder, Keohane menciona o conceito de cooperação hegemônica, argumentando que as instituições podem ser complementadas pela atuação de países hegemônicos, os quais são capazes de promover a ordem e instituir regras no sistema (Ibid., p. 15).

Em suma, o institucionalismo liberal defende a ideia de que a cooperação é possível quando há interesses comuns entre Estados, e cada um deles aceita abrir mão de sua própria liberdade de ação — mesmo frente à incerteza — ao contar que os outros países seguirão o mesmo caminho. A teoria opera segundo a concepção de que Estados são capazes de confiar uns nos outros, e que as instituições internacionais são instrumentos que existem justamente para facilitar essa interação (Mearsheimer, 1995, p. 15-16).

1.2.3 Instituições para a Teoria Crítica

Para além das teorias desenvolvidas especificamente considerando a área das Relações internacionais, existem teorias que surgiram como áreas relacionadas à política em geral, ou à política nacional, que são transpostas para o sistema de Estados. Esse é o caso da teoria crítica, cuja aplicação específica nas R.I. vem depois de sua formulação inicial e é marcada principalmente pelos escritos de Robert Cox, que transpõe os conceitos do cientista político italiano Antonio Gramsci para o Sistema Internacional (Ibid., p. 40). Gramsci, por sua vez, não estuda

especialmente o âmbito interestatal, mas foca na política interna. Ele define os modos de funcionamento das sociedades e dos governos a partir das ideias de Marx e de suas observações empíricas. (Cox, 1983, p.125)

Desse modo, para Gramsci, as relações sociais fundamentais precedem as relações internacionais e as moldam (Gramsci *apud* Cox, 1983, p. 133). As relações internacionais, por essa lógica, são modificadas organicamente pelas inovações orgânicas na estrutura social – vale ressaltar, que ao usar o termo "orgânico", o autor se refere a mudanças relativamente permanentes a longo prazo, em oposição ao termo "conjuntural" (Cox, op. cit., p. 120). Ou seja, na teoria gramsciana as mudanças nas relações de poder interestatais, traduzidas em mudanças no campo estratégico-militar e na balança geopolítica mundial, são produto das mudanças fundamentais nas relações sociais internas ao Estado (Ibid., p. 133).

Para efeito de análise, a implicação principal dessa colocação é que as relações entre a estrutura e a superestrutura de cada governo se sobrepõem às relações entre esse governo e outros países. Isso significa que o Estado não pode ser compreendido apenas como uma unidade racional e fixa no Sistema Internacional, mas como parte de um bloco histórico específico, no qual interagem forças materiais (estrutura) e ideacionais (superestrutura). A estrutura corresponde às forças produtivas e às relações sociais fundamentais, enquanto a superestrutura é formada pelas instituições, ideologias e práticas discursivas que dão coerência e legitimidade à dominação dentro de um determinado contexto histórico (Ibid., p. 134).

Nesse sentido, a hegemonia, tanto para Gramsci quanto para Cox, não se reduz à dominação coercitiva, mas envolve a construção de um consenso ativo que legitima determinada ordem social. Gramsci compreende a hegemonia como a capacidade de uma classe ou grupo dirigente de universalizar seus interesses particulares por meio da direção moral e intelectual da sociedade, consolidando um consenso que se manifesta nas instituições, nas ideologias e nas práticas culturais. Ao transpor esse conceito para o Sistema Internacional, Cox entende a hegemonia como a articulação entre forças materiais, ideias e instituições que estabilizam uma ordem mundial específica. Como destaca Cox (1983, p. 133), o movimento em direção à hegemonia é descrito por Gramsci como uma "passagem da estrutura à esfera das superestruturas complexas", ou seja, o momento em que os interesses

específicos de uma classe se convertem em ideologias e instituições com aparência universal. A hegemonia, nessa perspectiva, é sempre histórica, situada e construída, sendo resultado da interação entre as estruturas sociais internas aos Estados e as configurações globais de poder. Assim, as instituições internacionais passam a ser vistas não como árbitros neutros entre Estados soberanos, mas como mecanismos que reproduzem e legitimam determinada forma de dominação global, enraizada nas relações sociais hegemônicas de um dado bloco histórico (Cox, 1983, p. 137-139).

Cox enfatiza ainda que, em continuidade aos argumentos supracitados, uma hegemonia mundial se origina como uma extensão da hegemonia nacional, ou seja, das estruturas sociais e políticas consolidadas internamente por uma classe dominante. Essa hegemonia se projeta internacionalmente por meio da difusão de instituições econômicas, sociais e culturais, gerando um padrão de emulação nos países periféricos. Essa expansão se dá muitas vezes como uma “revolução passiva”, isto é, sem ruptura estrutural, mas por meio da adaptação subordinada às diretrizes da hegemonia dominante (Cox, 1983, p. 137).

Não obstante, cabe destacar que Gramsci não desconsidera a centralidade do Estado nas relações internacionais. Pelo contrário, para ele a entidade básica do Sistema Internacional é sim o Estado: o espaço onde os conflitos sociais ocorrem e onde as hegemonias sociais podem ser construídas (Ibid., p. 133). Todavia, essa perspectiva não contradiz a premissa de que as interações entre países são fundamentadas por relações sociais essenciais, uma vez que os conflitos entre Estados sempre refletem correlações originadas no âmbito doméstico. Seguindo essa perspectiva, o discurso tem papel fundamental na consolidação da hegemonia. Ele é o meio pelo qual a superestrutura produz consenso em torno de determinadas ideias, naturalizando as relações de poder existentes. Gramsci destaca que a hegemonia é tanto coerção quanto consentimento, e é no plano da cultura e da ideologia que se conquista a adesão das classes subalternas (Cox, 1981, p. 139).

As instituições internacionais, nesse sentido, não são entidades neutras voltadas exclusivamente à cooperação ou à estabilidade sistêmica. Elas operam como instrumentos da hegemonia, pois cristalizam uma determinada correlação de forças sociais e disseminam normas que refletem os interesses do bloco hegemônico, representando as seguintes características:

> (1) as instituições incorporam as regras que facilitam a expansão das ordens mundiais hegemônicas; (2) elas próprias são produto da ordem mundial hegemônica; (3) elas legitimam ideologicamente as normas da ordem mundial; (4) elas cooptam as elites dos países periféricos; e (5) elas absorvem ideias contra-hegemônicas. (Cox, 1983, p. 138, tradução nossa).[6]

Em suma, a compreensão crítica das instituições internacionais exige o reconhecimento de sua inserção em um bloco histórico global, no qual as relações sociais fundamentais determinadas por fatores como a forma de produção, a organização do trabalho e a estrutura de classes atravessam as fronteiras estatais e informam tanto a política doméstica quanto a política externa. O discurso, ao naturalizar certas hierarquias e formas de organização, é o elo entre a superestrutura interna e a superestrutura internacional, possibilitando que formas de dominação locais sejam projetadas e reproduzidas no plano global.

1.3 DEFINIÇÕES TEÓRICAS

Feita essa breve explanação acerca das principais correntes que relacionam hegemonia e instituições, neste trabalho, opta-se pela perspectiva do realismo, especificamente do Realismo Ofensivo. Julga-se que dessa maneira a instrumentalização pode ser melhor observada no objeto de estudo escolhido, que trata de instituições no plano regional. A hegemonia regional em questão, os Estados Unidos, utiliza a OEA para promover seus interesses regionais, potencializando sua posição e influência no continente

Conforme observado e descrito acima, são diversas as teorias da política internacional/relações internacionais que definem as funções das instituições e seu papel no Sistema Internacional. Por esse motivo, não se pode definir o que são essas instituições internacionais e qual seu lugar no mundo sem especificar qual corrente teórica é utilizada para tal definição. Os pontos de vista e opiniões sobre o tema são múltiplos, e apresentam argumentações complexas a partir de visões ontológicas variadas. Sendo assim, somente a partir de uma investigação completa sobre essa gama de perspectivas é possível escolher uma linha de estudo para seguir e defender essa escolha.

---

[6] *(1) the institutions embody the rules which facilitate the expansion of hegemonic world orders; (2) they are themselves the product of the hegemonic world order; (3) they ideologically legitimate the norms of the world order; (4) they co-opt the elites from peripheral countries; and (5) they absorb counterhegemonic ideas.*

Realizado o processo de análise das teorias institucionalistas em sua variedade, é possível constatar que, embora todas apresentem teses concisas e pertinentes, nem todas as perspectivas colocadas condizem com uma visão pragmática a respeito das Relações Internacionais. Os aspectos destacados na seção anterior sobre o institucionalismo da segurança coletiva e o institucionalismo liberal elucidam que ambas as teorias partem do princípio de que a cooperação é possível e os conflitos internacionais são reguláveis por meio de alianças e meios legais promovidos por instituições. No entanto, a ideia de subordinar a competição interestatal à normas é utópica no Sistema Internacional anárquico em que predominam as relações de poder (Mearsheimer, 2025).

Isso se confirma a partir da observação de que mesmo as argumentações liberais partem de princípios realistas, como a busca pela sobrevivência e a balança de poder; tanto Claude como Keohane aderem à noção de que as relações de poder são centrais nos assuntos geopolíticos (Claude, 1962; Keohane, 1984). O diferencial do liberalismo é que a teoria busca superar o dilema da segurança e promover a paz defendendo a centralidade da cooperação em detrimento da busca pela sobrevivência. Contudo, observa-se que é inevitável que as tomadas de decisão dos Estados sejam feitas por quaisquer interesses que não a garantia de sua própria existência, e, por conseguinte, a cooperação sempre ocupará um papel secundário (Mearsheimer, 2025).

Nesse cenário, a cooperação não deixa de ser possível, mas só dura enquanto for condizente com os interesses individuais de cada potência envolvida, isto é, está sempre ofuscada pela competição por segurança e pela possibilidade de guerra (Ibid., p. 15). Essa perspectiva crítica em relação à efetividade autônoma das instituições encontra respaldo em análises como a Waltz, que demonstra como instituições internacionais não são forças independentes com agência própria, mas sim criações moldadas pelas potências que as fundam e sustentam. Embora institucionalistas aleguem que, uma vez criadas, as instituições ganham vida própria e seguem operando independentemente dos interesses dos Estados que as criaram, o realismo aponta que as instituições seguem servindo à estrutura internacional vigente e se adaptam à balança de poder dominante (Waltz, 2000, p. 208).

O exemplo da OTAN, amplamente utilizado tanto por institucionalistas quanto por realistas, ilustra esse embate interpretativo. Enquanto teóricos liberais como

Keohane e Martin veem a sobrevivência e expansão da OTAN como evidência da força das instituições multilaterais, Waltz aponta que o verdadeiro motor por trás da longevidade da organização é o interesse dos Estados Unidos em manter sua influência sobre as decisões de segurança europeias. A organização, segundo ele, é sobretudo “um veículo para aplicação do poder Americano e de sua visão para a ordem securitária na Europa” (Waltz, 2000, p. 208, tradução nossa). É possível que a OEA sirva ao mesmo propósito, ocupando o papel de ferramenta de manutenção da hegemonia regional dos EUA no continente americano. Portanto, o instrumental teórico realista, ao tratar exatamente desse tipo de relação entre Estados, instituições e relações de poder, fornece meios eficientes para a análise dessa hipótese.

Waltz apresenta também que os Estados mais fracos, por sua vez, têm dificuldades em criar instituições que sirvam a seus próprios objetivos, sobretudo no campo da segurança (Ibid., p. 209). No caso da OEA na América, é evidente que os EUA se sobrepõem militarmente e economicamente aos demais países da região, em especial às nações da América Latina e Caribe. Trata-se de um cenário onde a preponderância das relações de poder é inegável e, de acordo com o realismo, supõe-se que a cooperação é submetida aos interesses de maximização de poder do Estado dominante: os Estados Unidos.

A relevância da teoria realista para esta análise se intensifica quando Keohane e Martin, ao responderem às críticas de Mearsheimer ao institucionalismo liberal, admitem que os efeitos das instituições dependem das realidades de poder e interesse, ou seja, exatamente o que os realistas vêm sustentando (Keohane e Martin, 1995). Como apontado anteriormente, tal reconhecimento demonstra que o institucionalismo liberal, longe de ser uma alternativa ao realismo, parte de suas mesmas bases estruturais e retorna inevitavelmente a conclusões realistas: *“*O institucionalismo liberal, como afirma Mearsheimer, ‘não é mais uma alternativa clara ao realismo, mas, de fato, foi engolido por ele’.*”* (Waltz, 2000, p. 211, tradução nossa.

A criação e manutenção de instituições, portanto, não estão afastadas das capacidades e intenções dos Estados majoritários que as originaram. A própria permanência de estruturas como Bretton Woods ilustra isso com clareza: essas instituições só persistem enquanto forem percebidas como úteis para os interesses de seus criadores (Ibid., p. 213). Como sintetiza Stephen Krasner, citado por Waltz,

“a natureza dos arranjos internacionais é melhor explicada pela distribuição de capacidades de poder nacionais do que por esforços para resolver falhas de mercado” (Ibid.).

Nesse sentido, ao adotar a perspectiva do Realismo Ofensivo neste trabalho, considera-se que as instituições internacionais, como a OEA, operam principalmente como instrumentos da potência hegemônica regional — os Estados Unidos — para preservar e expandir sua influência estratégica. A institucionalização da cibersegurança no âmbito da OEA, assim, pode ser interpretada como uma extensão da lógica realista: não uma arena neutra de cooperação, mas um espaço estruturado para manutenção da ordem desejada por quem detém os meios de moldá-la.

2 O DESENVOLVIMENTO HISTÓRICO DA OEA

Com base nos critérios previamente estabelecidos para a análise das instituições internacionais e das dinâmicas de poder que se desenrolam em seu interior, este capítulo introduz o estudo específico da Organização dos Estados Americanos (OEA), com o objetivo de aprofundar a investigação sobre a influência da hegemonia nas instâncias multilaterais. A escolha da OEA como objeto de análise se justifica por seu papel central como uma das principais plataformas de cooperação política e securitária no continente americano, além de sua longevidade e relevância histórica na consolidação de normas, diretrizes e práticas institucionais na região.

Neste sentido, o capítulo desenvolve uma pesquisa de caráter historiográfico acerca da OEA, com base em fontes institucionais e acadêmicas primárias e secundárias, a fim de levantar os elementos necessários para a análise crítica da organização ao longo do tempo. O intuito é compreender não apenas os marcos históricos de sua criação e evolução institucional, mas também os arranjos internos, o papel desempenhado pelos Estados membros — em especial os Estados Unidos — e os mecanismos de financiamento que sustentam suas atividades. A trajetória da OEA será, portanto, analisada como um reflexo das disputas e assimetrias de poder presentes no sistema interamericano.

2.1 ANTECEDENTES E FUNDAÇÃO

A Organização dos Estados Americanos foi fundada em 1948, pós-Segunda Guerra Mundial e pré-Guerra Fria. Não obstante, existem diversos fatores políticos e históricos que antecedem essa fundação que influenciaram diretamente no modo como ela se deu e nos seus objetivos. A organização é produto de um longo processo de desenvolvimento da cooperação entre os países ocidentais, o qual foi marcado pela construção gradual de um aparato institucional de negociações e normas, como agências de cooperação, conferências regionais e acordos multilaterais (Herz, 2011, p. 28). Sendo assim, é importante avaliar quais foram esses antecedentes para construir uma síntese clara da trajetória da OEA no Sistema Internacional.

As origens da cooperação entre os Estados do continente americano se dão a partir do século XIX, quando o movimento do Pan-Americanismo ganhava

visibilidade, ideal que se manifestou em diferentes vertentes ao longo da história, com destaque para o bolivarianismo e o monroísmo (Gaviao, 2018). O bolivarianismo se define a partir da atividade de Simón Bolívar (presidente da então República de Bolivar, atual Bolívia), o qual, perante as rupturas dos países americanos com os países europeus, propunha uma confederação dos Estados hispano-americanos para proteger as novas independências da intervenção colonizadora. Esse desejo se materializou no Congresso do Panamá, em 1826, quando foram firmados acordos de segurança e cooperação econômica na região, introduzindo a ideia de segurança coletiva intra-regional para as Américas independentes (Galerani, 2011). A confederação proposta incluía uma "lei comum" e um "Congresso Geral Permanente" com representação igualitária, funcionando também como uma aliança militar. Contudo, o Congresso do Panamá não obteve qualquer sucesso considerável, visto que o tratado não foi ratificado por todos os signatários e poucos participantes realmente compareceram na ocasião (Prado e Pellegrino, 2014).

Na tese "Do Pan-Americanismo ao Sul-Americanismo: as Identidades Supranacionais no Continente Americano em Três Tempos (1826, 1960 e 2008)", o autor Leandro Gavião apresenta quatro principais razões para o insucesso do bolivarianismo: os desafios geográficos, a falta de percepção de ganhos coletivos, a fragilidade dos Estados recém-independentes e a exclusão do Brasil (Gavião, 2018). Apesar de seu insucesso imediato, o bolivarianismo tornou-se um referencial simbólico para a identidade latino-americana e para futuras iniciativas de integração.

A vertente estadunidense do Pan-Americanismo, o monroísmo, foi enunciada em 1823 com a Doutrina Monroe, um esforço conjunto do presidente James Monroe e de seu secretário de Estado, John Quincy Adams. Inicialmente, a Doutrina defendia a independência dos novos Estados americanos contra a intervenção europeia, similarmente ao bolivarianismo. Mas em seu discurso os EUA assumiam responsabilidades especiais pelo hemisfério, se colocando em posição de mentor do continente e já manifestando interesses de dominação sobre a região (Ibid.). A América Hispânica, a princípio, via a Doutrina Monroe como uma salvaguarda de suas independências recém-conquistadas.

Entretanto, após a Guerra de Secessão (1861-1865), os Estados Unidos cresceram em poder econômico-industrial e bélico, emergindo como uma grande potência internacional, assim sua política externa para o continente assumiu uma

postura progressivamente imperialista, tendo como antecedente ideológico a noção do Destino Manifesto de 1845 — não uma política oficial, mas uma crença amplamente difundida que justificava a expansão territorial norte-americana. Essa perspectiva refletia interesses de maximização de poder regional e garantia da segurança, com os EUA impulsionando suas próprias vias de expansão de controle sobre seus vizinhos, resultando em intervenções militares e econômicas. Com efeito, no final do século XIX, as intenções estadunidenses sobre a América Latina passaram a apresentar um teor diferente, muito mais intervencionista

Nesse contexto, os EUA iniciaram as Conferências Pan-Americanas a partir de 1889, as quais resultaram na criação da União Internacional das Repúblicas Americanas, que viria a ser o embrião da atual OEA (Herz, 2011). Em 1910, em sua quarta conferência, a instituição passou a se chamar União Pan-Americana. No entanto, a crescente instrumentalização do Pan-Americanismo pelos EUA para sustentar sua hegemonia continental, somada à incoerência entre o discurso da solidariedade e as práticas intervencionistas, levou a um desgaste dessa ideia de identidade, gerando um sentimento de alteridade entre intelectuais e políticos latino-americanos, que passaram a ver os Estados Unidos como uma “antítese da América Latina” (Id., 2018, p. 130-131).

No decorrer do século XX, os parâmetros de cooperação no continente não permaneceram estáticos, mas passaram por alterações e adaptações ao cenário internacional de cada período. Diversos novos órgãos regionais foram criados ao longo da primeira metade do centenário, como a Comissão Interamericana de Comunicação Elétrica (1923), o Instituto Interamericano de Geografia e História (1928), e a Comissão Interamericana pelas Mulheres (1928). Posteriormente, a Segunda Guerra Mundial reforçou a necessidade de solidariedade hemisférica, levando à realização de consultas e assinatura de acordos. A disputa por influência entre EUA e Alemanha no continente foi claramente vencida por Washington no início dos anos 1940, permitindo a institucionalização da posição da América nos assuntos mundiais (Herz, 2011, p. 34).

A Conferência Interamericana sobre Problemas da Guerra e da Paz, realizada no México em 1945 (Conferência de Chapultepec), foi um marco importante. Os EUA, apesar ocupados com a criação da Organização das Nações Unidas (ONU) e a nova ordem econômica mundial de Bretton Woods, não podiam ignorar as demandas dos países latinos, que haviam sido aliados leais durante a

guerra (Neto, 2015, p.4). Assim, sob pressão do México e da Argentina, ocorreu a conferência, que buscou coordenar o sistema interamericano com organismos internacionais, propor um sistema de defesa interamericano independente da ONU, criar um programa de ajuda econômica para a América Latina no pós-guerra e trazer a Argentina de volta à cooperação (Ibid., 2015).

Nessa época, a ascensão da Guerra Fria marcou uma nova mudança de paradigma para as relações entre os países americanos. Os EUA deixavam para trás a abordagem da Boa Vizinhança própria das décadas anteriores e adotavam uma política de contenção do comunismo, com disposição para intervir na América Latina caso julgassem necessário (Herz, 2011). Frente a esse cenário, foi realizada a Conferência do Rio de Janeiro em 1947, com o fim de assinar o Tratado Interamericano de Assistência Recíproca (TIAR). Apesar de o processo decisório do TIAR ter considerado interesses do México, Brasil e Argentina, a maior delegação presente na negociação era a dos EUA, o qual estava empenhado em fazer valer seus interesses de intervenção e combate à influência soviética. Esses interesses foram, em grande medida, consolidados, mas o verdadeiro poder estadunidense sobre o continente só se consolidou institucionalmente face à posterior criação da OEA. (Neto, 2015, p. 7).

Isto posto, fundada em 9 de maio de 1948 em Bogotá, Colômbia, por 21 ministros das relações exteriores das Américas, com a assinatura da Carta da Organização dos Estados Americanos, a OEA foi criada não apenas para promover a integração e cooperação, mas como parte da estratégia dos EUA para conter o avanço do comunismo no hemisfério ocidental (Herz, 2011). Sua estrutura institucional básica é composta pela Assembleia Geral, que é o órgão supremo que define as políticas e mandatos da organização com um voto por Estado, e a Secretaria Geral, que executa as funções atribuídas pela Carta da OEA e outros tratados, sendo liderada por um Secretário Geral eleito pela Assembleia Geral (Seoane, 2023). Cabe pontuar que a Carta foi reformada pelo Protocolo de Buenos Aires em 1967, pelo Protocolo de Cartagena de Índias em 1985, pelo Protocolo de Washington em 1992 e pelo Protocolo de Managuá em 1993.

Segundo esse instrumento fundador, os propósitos gerais da organização são alcançar uma ordem de paz e justiça, promover a solidariedade, intensificar a colaboração e defender a soberania, integridade territorial e independência dos Estados americanos (OEA, 1993). Dentro da ONU, a OEA atua como um organismo

regional e não possui faculdades que a autorizem a intervir em assuntos de jurisdição interna dos Estados membros. Ainda segundo a Carta da OEA, a organização busca consolidar um regime de liberdade individual e justiça social, fundado no respeito aos direitos essenciais do Homem, dentro do quadro das instituições democráticas (Ibid., 1993). Observa-se, portanto, que os fins da instituição descritos em sua documentação oficial se alinham à tradição diplomática da América Latina, focada em solução pacífica de conflitos, princípios de não agressão e segurança coletiva. Todavia, este trabalho questiona tais inclinações a partir das políticas de defesa desenvolvidas pela organização, analisando se elas realmente são condizentes com a soberania, integridade territorial e independência dos Estados. Dessa maneira, avalia-se em que medida os princípios associados à ideia de segurança coletiva são deturpados pela balança de poder e pelos interesses realistas dos Estados, especialmente da potência hegemônica da região: os Estados Unidos.

De acordo com a revisão teórica exposta no primeiro capítulo deste estudo, os princípios realistas concernem o poder militar como um protagonista das relações de poder, conjecturando que a sobrevivência é o fim máximo dos Estados. Juntamente com a ideia de que as instituições são palco para o desenrolar dessas mesmas relações de poder, isso resulta em uma importância destacada das políticas de defesa desenvolvidas pelas organizações multilaterais, as quais ilustram com precisão os interesses de seus membros. Aplicada à OEA, essa perspectiva sugere que suas ações em matéria de segurança podem refletir mais os interesses da potência hegemônica do que um compromisso genuíno com a soberania e a igualdade entre os Estados membros. Diante disso, torna-se fundamental analisar a evolução das políticas de segurança da OEA, desde sua fundação até os dias atuais, a fim de compreender de que maneira tais políticas foram moldadas e quais interesses passaram a representar ao longo do tempo. A próxima seção se dedica, portanto, a examinar esse percurso, identificando as principais diretrizes adotadas pela organização, as transformações em sua agenda de segurança no decorrer das décadas e como elas se relacionam com o cenário político e a balança de poder em cada momento.

2.2 POLÍTICAS E ÓRGÃOS DE SEGURANÇA

Durante a Guerra Fria, a postura da OEA em relação à segurança foi predominantemente moldada pela agenda anticomunista dos EUA, refletindo a balança de poder bipolar global (Ziccardi, 2013). Como supracitado, a organização, juntamente com o TIAR, assinado em 1947, tornou-se um instrumento fundamental para a política externa da hegemonia americana na região, visando a contenção do "avanço soviético", especialmente na América Latina. A Doutrina Truman (1947) e o memorando NSC-68 (1950) estabeleceram a base para essa política de segurança, que identificava o bloco socialista como a principal ameaça internacional e legitimava ações como o apoio a regimes autoritários e a oposição a reformas sociais e econômicas consideradas influência comunista (Coelho, 2010). Ante essa conjuntura, os EUA incentivaram a militarização da região por meio de investimentos e estímulos destinados ao mercado de armas (Ibid., 2010).

Essa postura securitária adotada na Guerra Fria continuava um viés de "solidariedade hemisférica" e uma ideia de sistema interamericano de defesa instituídos na região desde a Segunda Guerra Mundial. Nesse contexto, em 1942 foi criada a Junta Interamericana de Defesa (JID), resultante de três Reuniões de Consulta dos Ministros das Relações Exteriores do Continente Americano, cujo objetivo principal era "o intercâmbio de opiniões e pontos de vista em matérias militares, para fomentar uma estreita colaboração entre as forças armadas dos Estados no Hemisfério" (JID apud Galerani, 2011, p. 3). A JID nunca possuiu mandato operacional, se limitando a sediar estudos e propostas sobre o sistema de defesa coletivo hemisférico. Com efeito, os países americanos resistiram à concessão à JID de uma dimensão política equiparável às alianças militares dos EUA com outras regiões do mundo, recusando-se a dar-lhe o papel operacional desejado por Washington, principalmente por conta da grande assimetria de poder observada entre eles e a potência norte-americana (Galerani, 2011).

Não obstante, a política estadunidense havia se modificado do não intervencionismo próprio do governo Roosevelt para o caráter intromissor da Doutrina Truman na condição de Guerra Fria, intensificando as pressões do país por realizar operações de defesa no continente. Com esse viés, os EUA passaram a estabelecer uma agenda de segurança para os Estados americanos, composta pelo anticomunismo e por medidas de intervenção explícitas, como: patrulhamento naval,

manutenção de linhas de comunicação, informação humana, entre outros (Silva Filho e Moraes, 2012). A criação do TIAR, em 1947, reforçou essa postura, bem como a fundação da OEA em 1948, conforme já mencionado.

Juntamente à aliança de colaboração bilateral entre os Estados Unidos e as nações da América Latina, abrangendo desde o treinamento de militares em várias áreas até a comercialização e o repasse gratuito de armamentos, o TIAR e a OEA passaram a compor os pilares do chamado sistema interamericano de defesa. Esse sistema se alinhava aos interesses estratégicos dos EUA, alinhamento consolidado com a declaração formal de uma incompatibilidade do comunismo com a herança democrática e cristã das Américas pela OEA em 1951, conformando-se plenamente ao clima de Guerra Fria (Ibid.). A própria organização passou a definir, então, o Sistema de Segurança Hemisférico a partir de três instrumentos principais: o TIAR, também conhecido como Tratado do Rio; a Carta da OEA; e o Tratado de Tlatelolco ou Tratado para a Proscrição das Armas Nucleares na América Latina e no Caribe. Esse último foi assinado por todos os países americanos, com exceção dos Estados Unidos e do Canadá, na década de 1990, e define a não proliferação de armas nucleares na América Latina (OEA, 1999).

Ao fim da Guerra, o sistema de defesa hemisférico se enfraqueceu, perdendo sua eficácia e legitimidade pela perspectiva da maioria dos países latino-americanos. Com a desmobilização dos aparatos de defesa e a expectativa de uma paz duradoura após o colapso do bloco soviético, surgiram novas dinâmicas no cenário internacional, e, por conseguinte, a OEA e o TIAR passaram a ser vistos como instrumentos obsoletos. Segundo Gonçalves, “O projeto de globalizar o capitalismo liberal sob a égide norte-americana forjou as condições para uma nova concepção de segurança internacional, transferindo-se o foco do Estado para o indivíduo” (Gonçalvez, 2011, p. 21). Entretanto, frente a esse novo quadro, emergiram desafios de segurança de natureza transnacional, que passaram a dominar a agenda, incluindo: crime organizado, terrorismo, desastres naturais e ameaças cibernéticas. Como resultado, a força armada terrestre e a mobilização de exércitos perderam a centralidade que antes possuíam, abrindo caminho para uma nova perspectiva de segurança internacional, mais ampla e com diferentes especificidades.

Para adaptar-se a essas prioridades, a OEA redefiniu seu papel e sua abordagem sobre assuntos de segurança, adotando o conceito de segurança

cooperativa nos anos 1990 e o conceito de segurança multidimensional nos anos 2000. O primeiro marco citado se deu ainda no século XX a partir de um cunho liberal, propondo que a paz é indivisível e exige um crescente envolvimento e cooperação interestatal, e definindo uma necessidade por essa segurança cooperativa (Guimarães, 2002). Ele se distanciou da ênfase na dissuasão e no castigo aos agressores, típicos da Guerra Fria, para sublinhar a prevenção de conflitos interestatais, o que foi realizado por meio da promoção de Medidas de Fomento da Confiança e Segurança (MFCS) e da reivindicação por transparência nas políticas de defesa (Ziccardi, 2013).

Em 1999, a Comissão de Segurança Hemisférica do Conselho Permanente (CSH) da OEA redefiniu o conceito de segurança e de suas apontadas novas ameaças, apontando que já não seria possível centralizar as discussões e as possibilidades de ação de defesa sobre ameaças entre Estados, como ocorria na década de 1940, quando a arquitetura de segurança americana passou a ser instituída. De acordo com o resumo da sessão da referida data,

> “Com a queda do muro de Berlim e a evolução de nossas sociedades no passado recente, os problemas de segurança se tornaram mais difusos. [...] As discussões incluíram não apenas as questões de segurança "graves" mais tradicionais, envolvendo as medidas de fortalecimento da confiança e da segurança, questões referentes à luta contra o terrorismo e o narcotráfico, mas também problemas "menos graves", como o papel dos militares na sociedade civil, as relações entre civis e militares, e outros correlatos. Assistimos a uma evolução dos problemas de "defesa" para os de "segurança". (OEA, 1999)

A partir de então, passou a ser considerada a criação um novo arcabouço de segurança para o hemisfério, capaz de englobar não somente discussões de defesa de cunho militar, mas também segurança pública e crimes transnacionais, envolvendo outros órgãos securitários, como o policial, por exemplo. Nesse sentido, o Canadá propôs, nessa mesma sessão, possíveis uniões entre as instituições de segurança já existentes, as quais eram a OEA, a JID, o Colégio Interamericano de Defesa (administrado pela JID), a Reunião Ministerial de Defesa das Américas e a Conferência de Chefes e Serviços, mas a proposta não foi acatada (Ibid.).

Em continuidade a essas discussões, surgiu o conceito de segurança multidimensional no início do século XXI, especialmente após os ataques de 11 de setembro de 2001, formalizado na Declaração sobre Segurança nas Américas de 2003. Um forte impulso para tal surgimento foi o início de um novo período de

tensões globais causado pelo ataque às Torres Gêmeas. Perante esse cenário, a administração estadunidense vigente — do presidente Bush (filho) — adotou a doutrina da “guerra preventiva” e a intenção de atuar unilateralmente quando necessário (Ibid.). Essa nova visão consolidou a ampliação do escopo da segurança para além das ameaças estritamente militares e centradas no Estado e a adoção de uma abordagem mais focada na proteção do ser humano enquanto indivíduo, além de que enfatizou a importância de ameaças domésticas e transnacionais. Em tempo, observa-se que a abordagem da segurança multidimensional não surgiu para substituir o conceito clássico de segurança, mas sim ampliá-lo (Thérien et. al., 2012).

A OEA, em contrapartida, reorganizou seu aparato institucional para comportar tal alteração no paradigma da segurança. Com esse fim, foi criada a Secretaria de Segurança Multidimensional (SSM) em 2005, dependente da Secretaria Geral da organização e dedicada a apoiar a CSH que, por sua vez, ocupava o cargo de principal órgão responsável pelas questões de segurança do continente. Subordinados à SSM, foram aos poucos fundados novos departamentos, comissões e comitês dedicados às emergências securitárias internacionais, como: a Comissão Interamericana para o Controle do Abuso de Drogas (CICAD); o Comitê Interamericano Contra o Terrorismo (CICTE); o Departamento de Segurança Pública; e o Departamento Contra o Crime Organizado Transnacional (DDOT) (OEA, 2025). Ademais, a JID, existente desde 1942, continuou a passar por transformações e foi finalmente incorporada oficialmente como entidade da OEA em 2006, acompanhando o cenário de mudanças e de maior atenção à variedade de fenômenos securitizados no novo século (Galeani, 2011).

Outros órgãos, grupos de trabalho e departamentos fazem parte de todo o arcabouço de estudos e planos de ação em segurança da OEA, alguns criados sob formas mais primitivas de administração da instituição e incorporados na complexidade hierárquica atual posteriormente. Entre eles estão o Grupo de Especialistas para o Controle de Lavagem de Dinheiro (GELAVEX) criado em 1990 e atuante como grupo de trabalho sob o escopo do DDOT desde 2016 (OEA, 2025); o Observatório Interamericano de Segurança, que é um banco de dados da organização; e as Conferências dos Ministros de Defesa das Américas (CDMA), atuante desde 1995.

Atualmente, grande parte das informações sobre as medidas e os órgãos de segurança e defesa da OEA podem ser encontradas no seu site oficial. Também é possível observar, pela plataforma digital, quais são os temas contemplados pela organização. Na aba “temas” da página inicial do site, estão colocadas três categorias de segurança: segurança cibernética; segurança multidimensional; e segurança pública. Outros dez temas são especificados na página específica da CSH: (i) ação contra minas; (ii) armas nucleares e educação para o desarmamento; (iii) combate ao tráfico ilícito de armas; (iv) combate ao tráfico de pessoas; (v) criminalidade organizada transnacional; (vi) fortalecimento da confiança e da segurança; (vii) prevenção da criminalidade e da violência; (viii) redução de desastres naturais; (ix) preocupações especiais de segurança dos pequenos Estados insulares; (x) tratamento das quadrilhas de delinquentes. Essa abordagem reflete claramente o alargamento da diversidade de tópicos securitizados pela OEA nas últimas décadas, seguindo a lógica das últimas declarações e conceitos desenvolvidos em sua alçada. A presença de uma categoria específica de cibersegurança no site oficial demonstra a importância dada a esse tópico e a urgência da própria instituição de tratá-lo como uma prioridade de segurança internacional.

Consubstanciando, o desenvolvimento das funcionalidades administrativas da OEA em matéria de segurança internacional se deu em consonância com as tendências do cenário político mundial. Nessa medida, é possível associar esse processo com os desenrolares da balança de poder da região, assim como é pertinente explorar quais os efeitos da influência dos movimentos geopolíticos predominantes de cada época na formação de todo esse aparato. Segundo o descrito desde o começo desta seção, os balanços da Segunda Guerra Mundial e da Guerra Fria moldaram muitas das decisões tomadas na OEA, e a influência dos EUA enquanto hegemonia regional foi constantemente notável. Portanto, a seção seguinte é dedicada a aprofundar a análise dessa relação.

2.3 ATUAÇÃO DOS EUA

É vasta a gama de bibliografias que apontam a instrumentalização da OEA a favor do interesse estadunidense na Guerra Fria. As questões adicionais a serem estudadas são se essa dinâmica se perpetua até os dias atuais e, em caso afirmativo, como se dá essa tendência.

Dentro da organização, o processo de tomada de decisão é baseado na definição clássica de soberania, na qual os Estados possuem direitos iguais. Assim, a distribuição real de poder não é expressa nos procedimentos formais, e os membros são tratados igualmente. Isso se reflete no fato de que o sistema de votos não possui pesos diferentes para cada país, ou seja, cada integrante tem direito a um voto que vale o mesmo que todos os votos dos demais. Para mais, não existe poder de veto na OEA; contudo, a cultura organizacional enfatiza a tomada de decisões por consenso, o que — apesar de reforçar a noção de igualdade entre os Estados e a restrição à intervenção em assuntos domésticos — pode bloquear a tomada de medidas e decisões (Herz, 2011). Especificamente para casos de agressão e medidas de retaliação contra o agressor, o texto final do TIAR adota o sistema de maioria qualificada (dois terços dos votos favoráveis) para as ações a serem decididas (Neto, 2015). Constata-se, portanto, que o funcionamento administrativo da OEA é aparentemente neutro e igualitário.

Mas para além dessa arquitetura institucional, a organização admite a participação de atores externos como empresas privadas, sociedade civil, organizações não-governamentais, especialistas e funcionários de agências de governo, principalmente de países da OTAN e dos EUA. Essa abertura nem sempre ocorre de forma proporcional para todos os países, com clara predominância de atores estadunidenses participando nas tomadas de decisões (Seoane, 2023). Um acontecimento que exemplifica essa atuação preponderante de atores ligados aos interesses estadunidenses foi a articulação entre o CICTE e forças sociais dos EUA e de Estados aliados, particularmente empresas de tecnologia com capacidade em cibersegurança, exemplos incluem a colaboração com Symantec, Trend, Micro e Microsoft. O CICTE também estabeleceu convênios de cooperação com outros atores, como o Banco Interamericano de Desenvolvimento (BID), o Fórum Econômico Mundial e a Universidade de Oxford. O denominador comum desses colaboradores não-estatais é que eles se associam a aliados ou organismos onde os EUA têm considerável influência financeira e política (Ibid., 2023). Ademais, funcionários de órgãos como o Departamento de Estado dos Estados Unidos e o FBI participam de eventos da OEA juntamente com acadêmicos e membros de organizações civis com sede no território da potência regional. Essa atuação contribui para a legitimação e institucionalização das preferências estadunidenses em novas agendas, como a cibersegurança, reproduzindo assim a lógica de

hegemonia regional dos EUA. Ainda que o contexto da Guerra Fria tenha se encerrado, estruturas criadas sob sua égide, como o Colégio Interamericano de Defesa (CID), permanecem ativas, operando como instrumentos da difusão ideológica e estratégica da potência hegemônica.

Nesse sentido, é possível afirmar que se a associação da OEA com as políticas anticomunistas dos EUA durante a Guerra Fria acabaram, não foi necessariamente porque a influência dos EUA diminuiu, mas porque a própria política estadunidense mudou de centro. Com o foco das políticas de segurança da OEA no combate ao terrorismo, é possível observar que a organização se manteve alinhada aos interesses estadunidenses. O alinhamento aos interesses dos EUA deixou de se manifestar no anticomunismo e no antagonismo extremo à URSS, mas ele não sumiu, e sim foi substituído pelo antiterrorismo a partir de 2001. Esse processo não ocorreu de forma repentina, mas pode ser descrito como gradual desde as décadas anteriores, se concretizando, evidentemente, perante a mudança de conjuntura descrita. Vale ressaltar o argumento reforçado por Arrighi (2007), que expõe como a Guerra ao Terror foi um projeto ideológico com o objetivo de viabilizar um novo conjunto de medidas intervencionistas promovidas pelos EUA no governo Bush do início do século XXI, veiculadas no projeto Novo Século Norte-Americano. Dessa forma, constata-se que a securitização focada no combate às práticas terroristas funcionava como um bode expiatório para a implementação de projetos de propagação da dominação estadunidense, em um contexto onde a credibilidade política norte-americana estava corroída em decorrência de sua derrota contra o Vietnã durante a Guerra Fria (Arrighi, 2007).

O caso do México ilustra com nitidez essa lógica. Apesar de tradicionalmente buscar um equilíbrio de poder com os EUA e defender a autodeterminação dos Estados de sua própria política interna sem intervenção de discussões em fóruns multilaterais, o país viu seus interesses estratégicos desconsiderados diante da imposição do conceito de segurança multidimensional na OEA descrito na seção anterior, cuja concepção, além de abraçar a ideia do antiterrorismo instrumentalizada a favor da dominação estadunidense, favorece a vigilância e intervenção em assuntos domésticos (Ziccardi, 2013). Tal postura da organização reforça a crítica realista de que instituições internacionais tendem a refletir os interesses das grandes potências, sendo moldadas conforme os objetivos de segurança e sobrevivência das hegemonias.

Como Ziccardi destaca, com o fim da Guerra Fria, os EUA realizaram uma transição para um enfoque mais pactuado em matéria de segurança regional, não por convicção normativa, mas por razões estratégicas: sem a ameaça soviética, não havia mais preocupação de que os países latino-americanos fossem cooptados por potências rivais extrarregionais (Ibid., 2015, p. 110). Assim, a adoção da abordagem baseada no conceito de segurança multilateral reuniu o útil ao agradável para a perspectiva norte-americana: era capaz de justificar — englobando a narrativa do combate ao terrorismo — uma securitização da região ditada por agentes e diretrizes estadunidenses, ao mesmo tempo em que a necessidade de manter um combate interestatal intenso para equilibrar a balança de poder havia diminuído com o encerramento da Guerra Fria e performar esse enfoque não traria um contraponto de enfraquecimento da sua hegemonia regional.

Portanto, a continuidade da influência estadunidense na OEA se manifesta tanto nas estruturas formais herdadas da Guerra Fria quanto na incorporação de novas agendas de segurança pautadas pelas prioridades estratégicas dos EUA. A cibersegurança é uma área emblemática dessa transição. Ainda que os países latino-americanos não tenham histórico significativo de ataques cibernéticos com motivação terrorista, a OEA passou a tratar o tema sob essa ótica, revelando uma clara importação das preferências normativas dos EUA (Seoane, 2023). Tal enquadramento não só mascara as reais vulnerabilidades da região, como também desloca a formulação de políticas para ambientes nos quais a influência de Washington é preponderante. Como conclui Seoane, “em todos os casos, é difícil encontrar a presença da voz de especialistas da América Latina, e menos ainda de vozes críticas” (Ibid., 2023, p. 106).

Essa assimetria não se resume à diferença de capacidades técnicas entre os Estados, mas se enraíza na forma como as ameaças cibernéticas são enquadradas politicamente. O modo como determinados eventos ou riscos digitais são reconhecidos como ameaças legítimas depende de processos institucionais que operam dentro de relações de poder. Segundo Cavelty (2024), esse enquadramento político consiste em uma prática de construção na qual determinadas narrativas ganham legitimidade e sustentam decisões políticas com base na percepção de risco. Reforçando o argumento desenvolvido neste trabalho até então, no caso da OEA, essa prática é fortemente influenciada pela agenda normativa dos EUA, que historicamente associa os riscos cibernéticos ao terrorismo, à criminalidade

transnacional e à instabilidade geopolítica. Mesmo na ausência de ataques cibernéticos com motivação terrorista na maioria dos países latino-americanos, a cibersegurança foi incorporada como prioridade institucional em resposta ao contexto global da “Guerra ao Terror”, adotando categorias e soluções construídas fora da realidade concreta da região (Seoane, 2023).

A formulação das políticas públicas nesse campo tende a reproduzir visões técnicas e estratégicas derivadas de atores centrais no Sistema Internacional. Nesse sentido, a política de cibersegurança pode ser compreendida como resultado de negociações em âmbitos nacional e internacional, que buscam delimitar as responsabilidades de atores estatais, econômicos e sociais, além de refletir os acordos ou divergências quanto aos meios empregados por esses agentes (Dunn Cavelty e Wenger, 2019). Ademais, diversos aspectos que definem as políticas de defesa decorrem das percepções, constantemente em transformação, de autoridades civis, militares e da própria sociedade de cada Estado (Maciel e Zaniboni, 2023). Ao assumir o enquadramento citado como legítimo e objetivo, a OEA contribui para institucionalizar uma hierarquia de conhecimentos e prioridades que replica a distribuição de poder no continente americano. Essa dinâmica será examinada com maior profundidade nos capítulos e seções a seguir, dedicados à análise dos documentos oficiais da OEA sobre políticas de cibersegurança, com o objetivo de compreender até que ponto elas refletem os interesses de hegemonia regional estadunidense nas Américas.

3 CIBERSEGURANÇA

Considerando que a cibersegurança é um elemento central deste trabalho, o presente capítulo tem como objetivo central construir uma base teórica e conceitual para a compreensão da segurança cibernética como um elemento de poder e de manifestação de hegemonia no Sistema Internacional, bem como compreender a importância das políticas de cibersegurança nas instituições multilaterais e as variáveis políticas por trás de suas formulações. Essa perspectiva complementa o Realismo Ofensivo ao compor a discussão sobre o papel da propagação de políticas de medidas de cibersegurança dentro da OEA na busca pela maximização e manutenção da hegemonia. De forma similar a como as instituições, para Mearsheimer (2001), representam cenários de reprodução da balança de poder mundial, o ciberespaço também é mais uma dimensão onde Estados disputam poder e buscam maximizar sua segurança — nesse caso, sua cibersegurança. Nesse sentido, a segurança cibernética não consiste somente em um campo técnico, mas em um componente estratégico fundamental das relações interestatais, profundamente entrelaçado com a competição por poder, com a manutenção da hegemonia regional dos EUA e com a forma como as instituições internacionais funcionam como palco para essas dinâmicas.

Sendo assim, a primeira seção deste capítulo se dedica a elaborar o campo conceitual, trazendo as definições de ciberespaço, ciberpoder e da cibersegurança em si, mostrando como esses termos se formaram historicamente e destacando o papel dos Estados Unidos nesse processo. A seção posterior, por sua vez, consiste na exploração do teor político da tecnologia e das relações entre cibernética, segurança e hegemonia, relacionando esses aspectos com a teoria realista. Por fim, a terceira seção trata como a cibersegurança se torna instrumento de poder e hegemonia por meio da exportação de doutrinas e terminologias para documentos de políticas de cibersegurança, amarrando todo o arcabouço teórico elaborado até então e preparando o leitor para entender a OEA no capítulo seguinte.

3.1 O CIBERESPAÇO E OS FUNDAMENTOS DE CIBERSEGURANÇA

Conforme discutido anteriormente, as relações de poder no Sistema Internacional são regidas pela busca da maior capacidade ofensiva que se possa obter, o que se traduz na busca das grandes potências pela hegemonia regional.

Essa dinâmica se manifesta em diversos campos das Relações Internacionais, contaminando desde aspectos sociais e culturais até questões militares e econômicas. No campo de segurança e defesa, as produções ligadas às forças armadas estadunidenses foram precursoras da divisão de setores de ação militares, segundo a qual são definidos quatro domínios tradicionais: a terra, o mar, o ar e o espaço; no entanto, com o advento das novas tecnologias ao longo do século XX e principalmente no século XXI, diversos teóricos apontam o surgimento de um quinto domínio: o ciberespaço (Nye, 2016).

A conceitualização do ciberespaço não é homogênea entre cientistas que tratam do assunto, é possível observar a existência de um espectro de interpretações que vai de definições técnicas a definições predominantemente teóricas, ou seja, há tanto conceitos centrados em aspectos informáticos sobre o campo eletromagnético quanto conceitos que consideram a interposição das camadas físicas e técnicas que trabalham conjuntamente para que o funcionamento do ciberespaço seja viabilizado (Medeiros e Goldoni, 2020). Todavia, quando se trata de teóricos ligados às Relações Internacionais e às Ciências Políticas, é notável uma predominância de definições que colocam o ciberespaço não somente como um meio de comunicação, mas como uma forma de criação, armazenamento, modificação e exploração de informação (Sheldon, 2011). No campo militar, as tecnologias de informação e comunicação permeiam as mais diversas operações e funções das Forças Armadas de muitos países do globo; nos EUA o ciberespaço está entrelaçado às funções militares de suas forças terrestre, aérea, marinha e espacial (Ibid., 2011).

Apesar de a dimensão de comunicação ser muito importante quando se trata do ciberespaço, é necessário considerar que esse meio não é puramente virtual, visto que ciberespaço não é sinônimo de Internet. Isso significa que o ciberespaço existe além da Internet, pois esta consiste em um domínio eletrônico e eletromagnético específico, enquanto o primeiro engloba uma grande rede de domínios operacionais baseados em computadores (Maciel e Zaniboni, 2023). Libicki (2009) propõe que o ciberespaço seja dividido em três camadas: física, sintática e semântica: a camada física compreende toda a infraestrutura necessária para o funcionamento do ciberespaço, como cabos e fios; a camada sintática diz respeito aos sistemas e protocolos que permitem a comunicação entre as máquinas; a camada semântica abrange as informações e códigos que constituem o próprio

propósito da existência dos computadores (Ibid., 2023). Compreender essa complexidade e as múltiplas dimensões do ciberespaço evidencia a importância de sua proteção. Em um contexto cada vez mais automatizado, as vulnerabilidades presentes nesse ambiente podem ser exploradas, configurando ameaças aos Estados e às suas infraestruturas, o que traz à tona o conceito e a função estratégica do ciberpoder.

A partir das considerações colocadas por Nye (2010), o ciberpoder pode ser definido como a capacidade de utilizar o ciberespaço e seus recursos informacionais para gerar vantagens estratégicas, influenciar eventos e alcançar objetivos políticos, econômicos ou militares. Ele se fundamenta no uso e controle de tecnologias e fluxos de informação eletrônica, envolvendo infraestrutura, redes, softwares, competências humanas e sistemas de comunicação, como internet, satélites, ondas de rádio e cabos de fibra óptica (Grassi e Ayres Pinto, 2022). Assim, o poder cibernético resulta da articulação entre tecnologia, organização e informação, permitindo que atores empreguem o domínio digital como instrumento de poder e influência no Sistema Internacional.

A partir disso, emerge a importância da cibersegurança no SI, a qual deve ter como função proteger atores que atuam no ciberespaço — ou são afetados por ele — dos possíveis riscos existentes nesse ambiente. Inicialmente, a noção de cibersegurança surgiu como uma reformulação moderna de práticas já existentes voltadas à proteção de sistemas e redes computacionais (Von Solms e Van Niekerk, 2013). Porém ao longo do tempo o conceito sofreu alterações e atualmente não existe consenso a seu respeito, uma vez que diferentes Estados e instituições divergem quanto à adoção de uma linguagem padronizada para descrevê-lo (Giles e Hagestad, 2013). Ademais, o entendimento do termo tem passado por constantes mudanças conforme o contexto tecnológico e político evolui.

Para a análise realizada neste estudo, cibersegurança será definida como as ações políticas adotadas por civis, militares, a indústria e o setor privado para salvaguardar o espaço digital (Solar, 2020). Com efeito, os objetivos centrais da segurança cibernética são assegurar a continuidade da sociedade da informação de uma nação; garantir e proteger os ativos de informação e as infraestruturas críticas no ciberespaço; e minimizar os riscos para os ativos do Estado e para os cidadãos (Grassi e Ayres Pinto, 2022). Academicamente, a cibersegurança “aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para

proteger o ambiente cibernético de um país e suas organizações" (Ibid., 2022) e trata de temas relacionados à segurança pública.

Embora o termo *cybersecurity* seja comumente usado de forma geral, abrangendo a *cyber defense* (defesa cibernética), conceitualmente há distinções baseadas na natureza da ameaça. Enquanto a cibersegurança é associada à dimensão da segurança pública, a defesa cibernética é comumente ligada à noção de guerra, à defesa dos interesses nacionais e à garantia da sobrevivência e soberania. No âmbito de fóruns regionais como a OEA, a temática é focada na segurança cibernética, tratando de delitos, crimes, ataques e terrorismo no ciberespaço, e a nomenclatura "defesa cibernética" não é tão utilizada (Gonzales e Portela, 2018).

Historicamente, a própria Internet foi desenvolvida nos Estados Unidos, em meios militares e com fins estratégicos para defesa. Consonantemente, o desenvolvimento da literatura relativa aos aspectos políticos da cibersegurança foi inicialmente exclusivo à *think tanks* e universidades militares dos EUA, os quais não pretendiam contribuir com o debate acadêmico e sim com os interesses militares norte-americanos. Por isso, "as questões que recebiam mais importância eram somente "quem (ou o que) representa o maior risco para uma nação/sociedade/força armada/ambiente de negócios crescentemente digitalizado" e "qual a melhor maneira de conter essa ameaça nova e em evolução"" (Dunn-Cavelty, 2024, tradução nossa). Esse foco trazido pela potência americana teve influência em como os assuntos cibernéticos foram tratados e formulados no campo das Relações Internacionais, direcionando os estudos da área para os aspectos militares e securitários.

Apesar de a Internet ter sido originada no contexto militar, ela se consolidou como uma rede predominantemente civil a partir do início da década de 1990. Ainda assim, as forças armadas mantiveram seu entendimento de que controlar o fluxo de dados e garantir vantagem informacional seria um fator determinante em contextos de guerra. Portanto, desde o surgimento dos primeiros computadores, o meio militar se interessou por empregar as tecnologias do ciberespaço para fins estratégicos. Segundo análise de Dunn Cavelty (2025), o momento em que essa preocupação ganhou centralidade nos EUA foi a Guerra do Golfo de 1991, que evidenciou o papel da tecnologia e da informação como componentes táticos decisivos. A partir desse episódio, surgiram intensos debates sobre o conceito de guerra da

informação e um aumento expressivo de estudos sobre a "*Revolution in Military Affairs (RMA)",* que vinculava a superioridade tecnológica à transformação das práticas de combate (Dunn Cavelty, 2025).

Para mais, nos anos iniciais de ascensão do ciberespaço como alvo de securitização, as ameaças eram causadas principalmente por indivíduos (os *hackers*), e grupos de interesse que agiam de forma independente. Contudo, conforme a problemática se expandiu pelo mundo, governos e forças armadas se envolveram cada vez mais, com atores estatais tomando a liderança do combate à ameaças digitais (Zheng, 2014). Frente a essa mudança, a problemática sobre o papel da cibernética em cenários e medidas de guerra se tornou cada vez mais relevante. Nos anos seguintes, o entendimento de guerra da informação deixou de se restringir a ações bélicas e passou a englobar a manipulação de sistemas informacionais de outros Estados em variados contextos, inclusive em tempos de paz. Em 1997, o Departamento de Defesa dos EUA e o Estado-Maior Conjunto adotaram o termo *information operations* em substituição a *information warfare,* refletindo uma ampliação conceitual. Essa nova terminologia incorporava tanto as operações de influência e propagando quanto as ofensivas contra redes de computadores, chamadas de *computer network operations (CNOs),* voltadas a comprometer infraestruturas inimigas, muitas vezes por meio de práticas equivalentes ao *hacking.* Essa diferenciação foi fundamental para o desenvolvimento posterior da doutrina e das capacidades cibernéticas que culminaram na criação do *US Cyber Command* em 2010 (Id., 2025).

A expansão do ciberespaço também trouxe uma vulnerabilidade inédita: a perda das fronteiras físicas como barreiras de proteção. Essa percepção levou estrategistas norte-americanos a popularizar um possível "Pearl Harbor eletrônico" (Schwartau, 1994, tradução nossa), que seria um ataque súbito e devastador que poderia paralisar o país em questão de minutos. Desde então, Estados considerados hostis e grupos terroristas passaram a ser apontados como principais ameaças nesse novo domínio e a possibilidade de uma ofensiva cibernética de grandes proporções se tornou elemento central das discussões sobre segurança nacional, influenciando o modo como os Estados Unidos e outros países passaram a estruturar suas políticas de defesa (Id., 2025).

Esse breve apanhado histórico a respeito da construção das percepções sobre o ciberespaço, ciberdefesa e cibersegurança nos EUA aponta para as

relações indissociáveis entre política e assuntos cibernéticos. Em suma, o ciberespaço proporciona um novo campo de análise sobre as Relações Internacionais, que deve ser multidisciplinar e minucioso, levando em conta aspectos estratégicos e geopolíticos ao tratar da segurança cibernética e da construção de políticas públicas nesse respeito.

3.2 CIBERSEGURANÇA, GEOPOLÍTICA E PODER NAS RI

Além de técnica, a cibersegurança também é uma questão profundamente política e estratégica. Embora parte significativa dos teóricos de RI aborde a temática cibernética majoritariamente a partir de uma perspectiva que pode ser caracterizada como ‘determinismo tecnológico’ — segundo a qual a tecnologia é um aspecto exógeno à construção do ciberespaço e definitivo em essência — existe uma alternativa a essa visão que estuda a tecnologia enquanto um produto social e político, moldado por interesses e, simultaneamente, capaz de reproduzi-los (Dunn-Cavelty e Wenger, 2019). Sob esse enfoque, a tecnologia não é neutra , ela reflete as intenções, valores e normas dos atores que a desenvolvem e controlam, funcionando, portanto, como uma arena em que as disputas de poder e as dinâmicas políticas do Sistema Internacional se materializam (Ibid., 2019).

Portanto, a lógica de competição existente entre países nos meios tradicionais das RI é transferida para o meio tecnológico e, destarte, Estados buscam maximizar seu poder e segurança também no ciberespaço. A partir da década de 2010, diversos episódios ilustram essa dinâmica, como o ataque com o vírus *Stuxnet* ao programa nuclear iraniano, as revelações de Edward Snowden sobre as práticas de vigilância global dos Estados Unidos e os ataques cibernéticos dirigidos contra a Estônia, a Geórgia e, mais recentemente, a Ucrânia. Esses eventos demonstram como o ciberespaço se tornou um campo de disputa geopolítica, onde a informação, a infraestrutura e o controle tecnológico se convertem em instrumentos de poder e influência.

Dunn Cavelty (2024) aponta duas tendências apresentadas no emprego de operações cibernéticas na política internacional: a normalização de ciber conflitos de “baixo-nível” (*low level*) e o aumento de campanhas cibernéticas ligadas ao encobrimento de envolvimento estatal nesse meio. Segundo a autora, essas propensões demonstram amadurecimento do uso da cibernética para propósitos políticos, traduzido tanto no aumento quantitativo dos ataques quanto em seu

aumento qualitativo, via crescente sofisticação técnica e estratégica. Dessa forma, o ciberpoder emerge como componente central da geopolítica contemporânea, revelando que as disputas por influência e segurança não se limitam mais ao território físico, mas se expandem para o domínio digital (Ayres Pinto et. al., 2024).

Nesse cenário, a infraestrutura digital assume valor de ativo estratégico e passa a representar uma forma de poder político. Para Sheldon (2011), o propósito estratégico do ciberpoder consiste na “habilidade, na paz e na guerra, de manipular percepções sobre o ambiente estratégico a favor de determinado ator, simultaneamente degradando a habilidade do adversário de compreender esse mesmo ambiente”. Em outras palavras, a detenção de infraestruturas de tecnologia e a capacidade de formulação de normas e discursos a respeito do meio tecnológico concede àqueles que as possuem capacidade estratégica sobre seus adversários. Essa capacidade se converte em poder político no Sistema Internacional anárquico, possibilitando meios de acumulação e manutenção de poder para além dos tradicionalmente estudados pelas Relações Internacionais.

Isso pode ocorrer de diversas formas, por coleta de inteligência e espionagem; subversão e manipulação de informações; apoio a operações militares; coerção; sabotagem de infraestruturas críticas; etc. A função mais disseminada do ciberpoder patrocinado pelo Estado é a espionagem, a qual tem um custo relativamente baixo em contraste com métodos tradicionais de inteligência humana e vigilância física (Dunn Cavelty, 2024); ela pode ser realizada por meio de extração de informações sensíveis, aproveitamento de dados, espionagem econômica e apoio à inteligência militar (Ayres Pinto et al, 2024). Além disso, o ciberespaço tornou-se uma ferramenta para construir consensos e moldar narrativas na política nacional e internacional, cuja função é moldar o comportamento do adversário de maneira favorável, frequentemente através de técnicas de guerra psicológica ou de informação (Id., 2024). Para mais, é recorrente a utilização de operações cibernéticas nas chamadas ‘guerras híbridas', quando são empregadas para projetar poder e obter influência sobre outros Estados (Rocha e Fonseca, 2019).

Com efeito, a conjuntura política observada no ciberespaço contém características condizentes com o sistema descrito pelos princípios da teoria realista, o que a torna propícia para analisar as relações de poder que se desenrolam em torno da cibersegurança. Anarquia, dilema de segurança, maximização de poder, preponderância de ataque e foco no Estado são aspectos

que evidenciam a relevância do realismo quando se estuda as disputas e assimetrias que permeiam o ambiente digital. A ausência de uma autoridade central capaz de regular o comportamento dos atores no ciberespaço cria um cenário de incerteza permanente, no qual as intenções e capacidades cibernéticas de cada Estado são ambíguas e difíceis de distinguir. Essa opacidade, segundo Rid e Buchanan (2014), intensifica o clássico dilema de segurança, pois diante da impossibilidade de determinar se as capacidades tecnológicas de um país possuem natureza ofensiva ou defensiva, as demais potências tendem a expandir seus próprios arsenais, alimentando o ciclo de competição e desconfiança que é descrito pela teoria realista.

Diante disso, o dilema de segurança se torna ainda mais agudo nesse domínio, uma vez que as ferramentas cibernéticas são, por definição, secretas e não verificáveis. Dessarte, qualquer ampliação de recursos, orçamentos ou pessoal em comandos cibernéticos — como o *US Cyber Command* — pode ser interpretada como um movimento ofensivo, independentemente de sua finalidade declarada (Craig e Valeriano, 2018). Em um contexto anárquico, essa incapacidade de sinalizar intenções pacíficas leva os Estados a buscarem segurança por meio da acumulação de poder, o que paradoxalmente aumenta a insegurança geral do sistema, reforçando a lógica da autoajuda típica do realismo descrita por autores como Mearsheimer (2001).

Craig e Valeriano (2018) colocam que, por tratar essencialmente de questões de poder e segurança, o realismo permanece uma estrutura teórica válida para compreender os conflitos cibernéticos. A corrida por capacidades ofensivas, a ausência de mecanismos de verificação e a sobreposição entre defesa e ataque fazem com que o comportamento dos Estados no ciberespaço reproduza, em larga medida, o padrão competitivo observado nos domínios tradicionais das RI. Por essa perspectiva, o desenvolvimento de capacidades cibernéticas não apenas responde a ameaças imediatas, mas constitui um instrumento estratégico de longo prazo para consolidar posições de poder e influência no Sistema Internacional.

Ao fim e ao cabo, o ciberespaço não rompe com as dinâmicas clássicas de rivalidade interestatal, na verdade, as reforça em um novo terreno. Consequentemente, a busca por supremacia tecnológica e informacional se soma às dimensões militar, econômica e diplomática da competição global, convertendo a infraestrutura digital em um dos principais vetores de poder político contemporâneo.

Nesse ambiente, destaca-se novamente que o domínio da cibersegurança representa não apenas uma vantagem operacional, mas também uma ferramenta de manutenção e projeção de hegemonia, capaz de moldar normas, comportamentos e dependências.

Compreendida a dimensão política da cibersegurança, resta entender como as estratégias e doutrinas nacionais, sobretudo dos Estados Unidos, moldam o Sistema Internacional e as organizações multilaterais.

3.3 POLÍTICAS DE CIBERSEGURANÇA E HEGEMONIA ESTADUNIDENSE

A maneira como as ameaças cibernéticas e os empregos de ciberpoder são percebidos e conceitualizados por cada país tem influência direta em como políticas de cibersegurança são formuladas em organizações multilaterais e, por conseguinte, afetam como os países que participam dessas organizações tratam questões de segurança cibernética em suas respectivas jurisdições. Buzan, quando desenvolve suas considerações sobre securitização na política internacional, defende que a delimitação das ameaças — que define como "*threat subject"* (Buzan et al., 1998) — é um aspecto essencial do processo político que define quais problemas devem ser securitizados e alvos de esforços estatais de mitigação. Isto posto, o Estado responsável por definir e especificar quais são as ameaças cibernéticas que devem ser apontadas e priorizadas na formulação de políticas de cibersegurança detém poder de direcionamento do processo de securitização do ciberespaço. Assim sendo, ao convencer com sucesso de que determinadas questões devem ser enquadradas como urgências em arenas políticas e sociais, é possível que um ator direcione medidas de segurança cibernética dentro de fóruns promotores de normas internacionais, as quais são seguidas por conjuntos consideráveis de países, propagando essa influência.

Ao analisar as bases e os propósitos de políticas públicas ligadas ao ciberespaço, Maciel e Zaniboni (2023) argumentam que esses instrumentos resultam das percepções de políticos, militares e da sociedade de cada país, os quais estão em constante mutação. Os autores argumentam que, para que tais políticas atendam às prioridades particulares de cada país, é fundamental que estejam inseridas em um debate público e social amplo, capaz de aplicar senso crítico sobre as normas formuladas.

Documentos estratégicos são instrumentos de poder discursivo e normativo, a formulação deles é capaz de determinar aspectos cruciais a respeito do uso do ciberespaço como os seus níveis de justiça, transparência e integridade. Frente a essa conjuntura, os EUA têm papel significativo na formulação de políticas de cibersegurança, considerando que são a nação fundadora da Internet e, assim, são o país com a maior influência no discurso sobre o ciberespaço (Zheng, 2014).

Conforme exposto na seção anterior deste capítulo, no início da história intelectual da cibersegurança, seus aspectos políticos eram discutidos quase exclusivamente em *think tanks* e colégios de guerra estadunidenses, o que marca uma preponderância discursiva dos EUA sobre esse tema. Além disso, a própria disciplina de Relações Internacionais começou como uma disciplina americana "focada na segurança americana e escrita por americanos" (Dunn Cavelty e Wenger, 2019). Isso culmina em uma história de segurança cibernética marcada pelas percepções práticas e domínio epistêmico da potência americana, na qual as ideias fundamentais sobre tecnologias, poder e ameaças no ciberespaço foram construídas a partir dessa perspectiva dominante (Dunn Cavelty, 2024). Para mais, por a própria Internet ser uma invenção essencialmente estadunidense, os valores incorporados nas arquiteturas de *hardware* e *software* da rede "refletem o contexto de sua criação, expressando um viés liberal" (McCarthy, 2015). Consonantemente, os Estados Unidos não apenas desenvolveram políticas de cibersegurança com influência internacional, mas também estabeleceram as normas, discursos e práticas que influenciam todo o SI.

O australiano Daniel McCarthy (2015), ao analisar a política externa dos EUA em relação à tecnologia da informação em seu livro "*Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet"*, observa que a formulação de políticas de cibersegurança pelas autoridades estadunidenses foi um mecanismo crucial para manter e maximizar o poder do país, integrando objetivos econômicos, políticos e de segurança. O autor desenvolve seu trabalho a partir de uma teoria materialista histórica marxista que analisa o relacionamento entre poder, tecnologia e política internacional. Apesar de o arcabouço teórico utilizado pelo referido estudo diferir da perspectiva realista adotada nesta pesquisa, a fonte fornece constatações empíricas ricas para a análise da atuação dos EUA sobre políticas de cibersegurança, as quais podem ser

empregadas a partir do viés do Realismo Ofensivo condizente com a presente análise.

Portanto, emprega-se aqui o trabalho de McCarthy como fonte secundária sobre a política externa dos EUA ligada à segurança cibernética. O argumento do livro se resume na ideia de que o poder estadunidense na política de tecnologia da informação é exercido através da interação de três formas de poder: poder estrutural, poder produtivo e poder institucional. É possível interpretar a aplicação empírica de cada uma dessas modalidades como mecanismos pelos quais a potência mantém e maximiza sua posição no Sistema Internacional, de forma a separar o nível da explicação fundamental (o materialismo histórico) do nível de descrição e identificação de ferramentas de poder (de acordo com a lógica realista ofensiva). Assim, as três formas de poder serão traduzidas em três vetores principais de maximização de poder, sendo eles, respectivamente: vetor econômico, vetor produtivo e vetor material.

O vetor econômico consiste na utilização da dominância econômica e tecnológica dos EUA para forçar a adesão global a regras que garantam a reprodução de seus ativos e recursos, como propriedade intelectual e Direitos de Propriedade Intelectual (DPIs). Esse aspecto pode ser relacionado com as políticas de financiamento dos Estados Unidos na OEA, uma vez que, a partir disso, se cria certa dependência econômica da organização com o país, fenômeno que possui potencial de aumentar o poder de barganha ou mesmo o poder coercitivo dos EUA sobre a instituição (McCarthy, 2015).

Ainda a respeito do emprego da dominância econômica sobre regras de tecnologia, McCarthy dedica o Capítulo 6 de seu livro a detalhar como a política de DPIs serve para reproduzir as relações de poder estrutural do capital estadunidense. Observa-se que a formulação de políticas não é neutra, mas condiz com interesses de maximização de poder da potência regional frente a outros Estados.

O vetor produtivo, por sua vez, é o uso, por parte da potência americana, de retóricas de valores liberais — como direitos humanos e democracia — para legitimação de suas ações, deslegitimação da resistência de adversários e estruturação da agenda internacional, garantindo a aceitação de seu modelo tecnológico. O autor dedica um capítulo inteiro (o Capítulo 5) para descrever como os EUA buscam consolidar sua visão sobre tecnologia usando o poder produtivo

para vincular o viés liberal da Internet a normas internacionais propagadas como legítimas.

Zheng (2014), teórico chinês, também aponta para a competição de valores cibernéticos como uma das principais características da competição estratégica no ciberespaço, a qual é manifestada como um embate entre o ideal de "*cyber freedom*" e o de "*cyber sovereignty*". Esse confronto se relaciona diretamente com a instrumentalização do discurso liberal identificada por McCarthy, pois ambos autores destacam o fato de que a ideia da Internet livre não é uma verdade absoluta, e sim uma ideologia que favorece interesses norte-americanos. Inversamente, países orientais como China e Rússia investem no conceito de soberania cibernética, enfatizando a proteção de direitos individuais, mas simultaneamente protegendo a cibersegurança e soberania nacionais e buscando desenvolvimento cibernético cooperativo com o restante do mundo (Zheng, 2014).

Com relação à atuação da OEA em matéria de segurança cibernética, é possível constatar uma continuidade entre as políticas de dissuasão disseminadas pelos EUA durante a Guerra Fria e as estratégias cibernéticas na época e, posteriormente, uma coincidência entre as políticas de segurança desenvolvidas a partir dos interesses da Guerra ao Terror e as definições e objetivos em cibersegurança propagados a partir do início do século XXI. Esses aspectos corroboram com a perspectiva exposta acima, segundo a qual o vetor produtivo de maximização de poder dos EUA molda o direcionamento das normas de cibersegurança em fóruns internacionais a favor de sua própria estratégia de defesa e de política externa no geral. Ainda com referência à prática de direcionamento arbitrário sobre quais retóricas e ideias sobre o ciberespaço são priorizadas na criação e aplicação de políticas de segurança cibernética, o arcabouço teórico e os valores adotados por cada organização multilateral demonstra alinhamento ou não a cada um desses países ou blocos. A abordagem da OEA se aproxima claramente da visão estadunidense, enquanto se afasta da visão oriental, especialmente do eixo Sino-Russo (Diplo Foundation, 2017).

Aspectos da política externa dos Estados Unidos na Guerra Fria que influenciam as políticas cibernéticas do país são: a doutrina da dissuasão e a defesa de um fluxo livre de informação. A teoria da dissuasão (*deterrence theory*) ganhou destaque em função da ameaça de destruição mútua assegurada (MAD) pelas armas nucleares (Craig e Valeriano, 2018). Atualmente, a lógica da dissuasão

influencia explicitamente a política cibernética estadunidense, a qual enfatiza tanto a defesa quanto a dissuasão (Ayres Pinto et al., 2024). Além disso, a prevenção de ataques cibernéticos destrutivos em larga escala se alinha com o *framework* da dissuasão, que busca inspiração na Guerra Fria. Os EUA definem sua política cibernética nacional com o objetivo de "convencer um potencial adversário de que ele sofrerá custos inaceitáveis se conduzir um ataque contra os Estados Unidos" (Craig e Valeriano, 2018, tradução nossa).

Portanto, a dissuasão é um conceito estratégico de continuidade da Guerra Fria aplicado ao ciberespaço, de maneira que a ênfase no combate ao ciberterrorismo e proteção de infraestruturas críticas dentro da instituição — mesmo que essas não fossem as principais ameaças cibernéticas sobre os países da América Latina (Seoane, 2023) — configura uma clara coincidência e uma resposta direta aos interesses de segurança dos EUA propagados a partir da Guerra ao Terror.

Quanto ao livre fluxo de informação, essa é uma ideia que o governo estadunidense frequentemente alude à Guerra Fria, ligando as tentativas de censura na Internet aos esforços de censura soviéticos, usando analogias como a "cortina de informação" (McCarthy, 2015). Essa visão promove a aceitação de normas e regras do ciberespaço que apoiam os objetivos e política externa da potência americana de liberalizar o Sistema Internacional e expandir o capitalismo globalmente.

Posteriormente, os posicionamentos dos Estados Unidos ligados à Guerra Fria deram lugar às ideias que amparavam a Guerra ao Terror. Nesse contexto, a definição e os objetivos da cibersegurança nos fóruns regionais, como a OEA, demonstram uma clara coincidência com a agenda de segurança global impulsionada por esses novos interesses estadunidenses (Solar, 2020).

No artigo "A Geopolítica do Espaço Cibernético Sul-Americano" de Gonzales e Portela (2018), os autores identificam que a atuação da OEA em matéria cibernética pode ser divida em dois momentos cruciais, ligados a eventos globais: o foco em delitos cibernéticos e a adoção da Estratégia Integral e Inclusão do Terrorismo. Aprofundando essa divisão, o estudo constata que a preocupação inicial da organização, manifestada em 1999, era combater os delitos cibernéticos com ações vinculadas aos Ministérios da Justiça. Já a partir de 2001, após o atentado de 11 de setembro, a OEA ampliou seu foco — focando também em

crimes, ataques e, crucialmente, terrorismo —, mudança que foi consolidada em 2004, pela aprovação da "*Estrategia Interamericana Integral de Seguridad Cibernética*" (Gonzales e Portela, 2018). O desenvolvimento dessa Estratégia Integral de 2004 reflete diretamente a nova agenda global de segurança pós-11 de setembro, frente a elaboração de um projeto que abordasse os aspectos multidimensionais e multidisciplinares da cibersegurança (Ibid., 2018).

A interferência dos interesses de manutenção de poder e hegemonia dos Estados Unidos na OEA se torna ainda mais clara quando se compara a abordagem sobre ameaças no ciberespaço desta com outras instituições regionais americanas. Com efeito, enquanto a primeira concentra seus esforços na segurança cibernética, outras organizações como o Mercado Comum do Sul (Mercosul), a União de Nações Sul-Americanas (UNASUL) e o Fórum Para o Progresso e Desenvolvimento da América do Sul (PROSUL) focam na defesa cibernética.

Em mais detalhes, o Mercosul tem como sua iniciativa principal na área cibernética a repudiação da espionagem estadunidense nos países Sul-Americanos; a UNASUL atua sobre a defesa cibernética (cujas diferenças com relação ao conceito de segurança foram aprofundadas na primeira seção deste capítulo); e o PROSUL tem experiência limitada no setor, mas possui um Grupo de Trabalho de Defesa que visa melhor a cooperação e troca de informações sobre ciberdefesa, através de protocolos de intercâmbio informacional (Maciel e Zaniboni, 2023). O que se conclui a partir dessas indubitáveis diferenças é que organizações onde as lideranças são Estados pertencentes à América Latina refletem interesses mais condizentes com as demandas e particularidades da região, ao passo que a OEA, mesmo que carregue a proposta de beneficiar igualmente todos as nações americanas, pende para concretizar os interesses particulares da potência hegemônica do continente, os Estados Unidos.

Por fim, o vetor material é definido pela exploração do viés institucional da Internet — uma invenção americana — para impor custos de desconexão ou filtragem a Estados rivais, maximizando o poder por meio de recursos tecnológicos materiais (McCarthy, 2015). McCarthy analisa como a própria arquitetura da Internet serve aos objetivos estratégicos dos Estados Unidos ao favorecer inerentemente o livre fluxo de informação, de maneira que Estados que desejam censurar ou filtrar conteúdo devem pagar um custo em tempo, recursos e esforços para contrariar o viés dessa rede. Isso contribui diretamente com o embate supracitado entre valores

cibernéticos, haja vista que países que buscam consolidar sua soberania cibernética enfrentam obstáculos impostos por essa arquitetura inerente da Internet, imposta pelos EUA. Na prática, o efeito geral desse mecanismo beneficia as corporações e o capital da potência, contribuindo para a manutenção da hegemonia regional norte-americana. Os três vetores de maximização de poder extraídos da análise empírica de McCarthy convergem na elucidação de que os Estados Unidos utilizam da cibersegurança para propagar seus intuitos particulares.

Incrementando ainda mais esse argumento, Dunn Cavelty também escreve sobre formas como a política externa e as definições de ameaças dos EUA foram disseminadas pelas nações ocidentais no terceiro capítulo de seu livro "*The Politics of Cyber-Security*" (2025). A teórica expõe que a "filosofia de proteção" (Dunn Cavelty, 2025, p. 43, tradução nossa) propaganda a partir da *President's Commission on Critical Infrastructure Protectio*n (PCCIP) publicada por Washington em 1997 culminou na adoção de conceitos sobre setores de infraestruturas críticas similares aos dos Estados Unidos em outros Estados que seguiam o modelo de democracia neoliberal. Segundo ela, as políticas de cibersegurança implementadas pelos EUA no final dos anos 1990, que foram adotadas por vários outros países, seguiam uma abordagem definida por três eixos principais: parcerias público-privadas para proteção de infraestruturas críticas; esforços legislativos contra o crime cibernético; e uma combinação de iniciativas públicas e privadas para assegurar outras infraestruturas em rede (Ibid., 2025). Esse enfoque reflete claramente uma lógica neoliberal, em que a intervenção estatal é minimizada, a liberalização é reforçada e a individualidade de cada setor é valorizada, enfoque esse que favorece o governo estadunidense e sua forma de funcionamento e propagação de poder.

Sumarizando, ao considerar que o ciberespaço é uma nova arena de poder onde os princípios realistas sobre o Sistema Internacional são reproduzidos e os Estados atuam em constante competição e busca por maximização de poder juntamente com a constatação de que a cibersegurança pode ser aplicada como um meio para essa maximização, cabe investigar de que maneiras a política de cibersegurança na OEA é instrumentalizada a favor da hegemonia regional dos Estados Unidos.

O presente capítulo expôs um panorama geral sobre os conceitos envolvidos nesta investigação, bem como aspectos empíricos de fontes secundárias que

corroboram para a elaboração da descrição sobre a apresentação desse fenômeno, trazendo a perspectiva histórica de comparação entre as medidas de cibersegurança anteriores e posteriores ao ataque às Torres Gêmeas de 11 de setembro de 2001. A partir de todo o enquadramento teórico desenvolvido até aqui, o capítulo seguinte analisa como essas dinâmicas se manifestam na Organização dos Estados Americanos em tempos mais recentes — especificamente, na década de 2015 a 2024 — a partir de uma análise empírica de fontes primárias, compondo um estudo de caso.

4 ESTUDO DE CASO

Conforme exposto nos capítulos anteriores, existe clara relação entre os interesses de manutenção de hegemonia regional dos Estados Unidos e a formulação e implementação de políticas de cibersegurança na OEA, principalmente considerando as abordagens da instituição sobre o tema nas décadas de 1990 e 2000. Neste capítulo, o objetivo é desenvolver um estudo de caso capaz de compreender o efeito das políticas de cibersegurança da Organização dos Estados Americanos (OEA) na manutenção e expansão da hegemonia dos Estados Unidos (EUA) na América Latina e Caribe em uma temporalidade mais recente, ilustrando o fenômeno ampliado sob o qual potências hegemônicas manifestam seus interesses em organizações internacionais.

Os anos escolhidos para o desenvolvimento da análise são 2015 a 2024, um recorte temporal de uma década. Considera-se que esse intervalo de tempo proporciona uma análise que equilibra amplitude com especificidade, de modo que torna possível obter um escopo de amostras vasto ao mesmo tempo que oferece proximidade com a contemporaneidade, o que resulta em coerência com os objetivos do trabalho. Essa coerência se explica pelo fato de que o objetivo deste estudo é verificar se as medidas recentes e atuais da OEA são influenciadas pelos EUA no tempo presente. Ao se verificar o que foi feito nas últimas décadas é possível identificar se existe um padrão que vem sendo seguido e que pode ser esperado hodiernamente e no futuro próximo.

Para investigar uma possível generalização, será examinada a relação causal entre as duas variáveis – políticas de cibersegurança da OEA e interesse hegemônico dos EUA – de acordo com o modelo temporal proposto por Gerring (2004). As amostras serão os Relatórios Anuais da OEA publicados de 2015 a 2023; os Relatórios Anuais do CICTE dos anos 2021 a 2023 e, para a observação das medidas adotadas em 2024, o documento “*2024 Cybersecurity Program*”. A adoção dos Relatórios do CICTE somente a partir de 2021 é justificada pela mudança no modelo do Relatório Anual geral da organização desse ano em diante, de forma que, ao contrário dos anos anteriores, depois dessa alteração as medidas de cibersegurança não são abordadas com detalhes nos documentos. E a utilização de um documento diferenciado para o ano de 2024 se dá por conta da ausência de um

Relatório Anual geral ou do CICTE para esse ano na data de realização deste estudo.

Para identificar os interesses dos EUA em cibersegurança serão utilizados os seguintes documentos: a Estratégia Cibernética do Departamento de Defesa (DoD) de 2015; a Estratégia Cibernética Nacional dos Estados Unidos, publicada em setembro de 2018, a qual foi a primeira estratégia cibernética totalmente articulada em 15 anos; a Visão de Comando para o Comando Cibernético dos EUA (USCYBERCOM) de 2018; a Estratégia Nacional de Cibersegurança de março de 2023; e o Plano de Implementação da Estratégia Nacional de Cibersegurança (NCSIP) de maio de 2024.

Este capítulo será estruturado em três seções. Inicialmente, a primeira seção descreve as principais medidas da Organização dos Estados Americanos sobre o ciberespaço no período de 2015 a 2024, utilizando os documentos citados anteriormente, ainda sem, contudo, apresentar uma análise crítica. A segunda seção apresenta os interesses dos Estados Unidos em relação à cibersegurança, fundamentados nos documentos estratégicos indicados no parágrafo acima. Por fim, a terceira e última seção relaciona os elementos abordados nas duas primeiras, analisando como os interesses norte-americanos se refletem nas diretrizes da OEA e desenvolvendo, finalmente, a crítica sobre os limites da atuação das instituições internacionais frente a interesses hegemônicos.

4.1 POLÍTICAS DE CIBERSEGURANÇA DA OEA DE 2015 A 2024

Inicialmente, é possível listar quais são os principais órgãos da Organização dos Estados Americanos que atuam na área da cibersegurança. O mais proeminente é o Comitê Interamericano Contra o Terrorismo (CICTE) — dependência da a Secretaria de Segurança Multidimensional (SSM) —, que abrange a maior quantidade e variedade de atividades em matéria de segurança cibernética. Além dele, o Departamento de Cooperação Jurídica (DLC), a Comissão Jurídica Interamericana (CIJ), a Secretaria para o Fortalecimento da Democracia (SSD), a Comissão Interamericana de Telecomunicações (CITEL) e o Departamento de Serviços de Informação e Tecnologia (DOITS) são ramos da instituição que colaboram no setor. Em todos os anos aqui analisados, cada um desses órgãos promoveu suas próprias iniciativas.

Ao examinar as iniciativas sobre cibersegurança, ciberdefesa, ciberterrorismo e temas adjacentes de cada um dos órgãos citados em cada ano de 2015 a 2024, é possível observar algumas tendências e características marcantes que se relacionam com os modos de influência sobre políticas de ciberespaço descritas no Capítulo 3. Para mapear a relação causal entre essas diretrizes e os interesses dos EUA, com precisão, primeiramente serão descritas as medidas tomadas em cada ano da década analisada. A partir deste ponto, esta seção estrutura-se cronologicamente: cada parágrafo é dedicado a um único relatório anual, e todas as informações contidas nele são extraídas exclusivamente dessa fonte, que será devidamente referenciada ao final do respectivo parágrafo.

Em 2015, a grande maioria das menções a ciber são relacionadas às atividades do CICTE. Entre as ações tomadas, a secretaria responsável por documentos do comitê imprimiu e distribuiu folhetos de cibersegurança, o livro "*Cybersecurity Trends in Latin America and the Caribbean*" e o livro "*Cybersecurity and Critical Infrastructure in the Americas"*. Além disso, o CICTE continuou seu apoio aos CSIRTs (Equipes de Resposta a Incidentes de Segurança de Computadores) na forma de treinamentos para aproximadamente 2.500 oficiais em mais de 30 eventos tratando da importância dos esforços de cibersegurança e contra o cibercrime. Já o DLC promoveu vários treinamentos e workshops sobre cibercrime para juízes e magistrados. Por fim, o Secretário Geral da OEA participou da Conferência Global sobre Ciberespaço 2015. (OEA, 2015)

Durante o ano de 2016, as atividades em cibersegurança e ciberdefesa foram bastante abrangentes. O Programa de Cibersegurança do CICTE demonstrou papel crucial ao prestar assistência no desenvolvimento de estratégias nacionais de cibersegurança em países como Chile, Costa Rica, República Dominicana, Guatemala e Panamá. O Comitê também contribuiu para a criação dos CSIRTs na República Dominicana e em São Cristóvão e Neves, e publicou um guia de "Melhores Práticas para Estabelecer um CSIRT Nacional". No âmbito da capacitação, o Programa treinou mais de 3.000 pessoas em investigação forense digital, proteção de infraestrutura crítica e gerenciamento de crises, e lançou o Observatório de Cibersegurança na América Latina e no Caribe. Paralelamente, outras instâncias da OEA também se engajaram: a REMJA/DLC (Reunião de Ministros da Justiça e Outros Ministros ou Procuradores-Gerais das Américas) realizou cinco workshops; o Instituto Inter-Americano da Infância (IIN) conduziu

consultas sobre bullying e cyberbullying; e a Junta Interamericana de Defesa (JID), que participou de eventos e emitiu resoluções sobre cibersegurança agrupada com terrorismo e questões militares/de defesa, iniciou esforços exploratórios em cibersegurança, refletindo a crescente preocupação do setor de segurança e defesa com o tema. realizou um seminário sobre a participação das Forças Armadas em tarefas não convencionais incluindo cyber-war na pauta, juntamente com crime organizado e ameaças socioeconômicas, além disso, a cibersegurança foi incluída como disciplina eletiva no programa de mestrado do IADC (Inter-American Defense College). Por fim, o Comitê Jurídico Interamericano (CIJ) também realizou reuniões com conselheiros legais sobre cibersegurança (OEA, 2016).

No ano de 2017, o CICTE manteve-se como ator principal, aprovando estratégias nacionais de cibersegurança no Chile, Costa Rica, México e Paraguai, além de trabalhar no desenvolvimento de planos para a Guatemala e a República Dominicana. No campo da cooperação e do desenvolvimento normativo, o Comitê criou o "Working Group on Cooperation and Confidence-Building Measures in Cyberspace" por meio da Resolução RES.1/17. O CICTE também focou na geração de conhecimento e conscientização, elaborando um relatório sobre o impacto de incidentes de computador na Colômbia e conduzindo pesquisas sobre o impacto desses incidentes no setor bancário na América Latina e no Caribe. A capacitação continuou intensa, com o treinamento de 3.000 oficiais dos setores público e privado. Paralelamente, a SSD ofereceu suporte direto para a criação de um plano de cibersegurança no Haiti. A dimensão de ciberdefesa também ganhou destaque: a JID realizou um seminário crucial sobre a participação das Forças Armadas em tarefas não convencionais, incluindo explicitamente a guerra cibernética em sua pauta, juntamente com crime organizado e ameaças socioeconômicas. Reforçando essa institucionalização, a cibersegurança foi incluída como disciplina eletiva no programa de mestrado do Colégio Interamericano de Defesa (IADC). No setor judicial, a REMJA/DLC deu continuidade aos seus workshops sobre temas cibernéticos para juízes e magistrados. O tema também foi inserido na agenda de cooperação internacional, com o DEIR (Departamento de Relações Internacionais) formalizando um memorando de cooperação entre o Secretariado Geral e o governo de Israel que incluía a cibersegurança entre seus assuntos (OEA, 2017).

O ano de 2018 demonstrou uma consolidação e expansão das iniciativas de cibersegurança e ciberdefesa no âmbito da OEA. A SSD manteve o suporte

fundamental ao Haiti, continuando os esforços para a elaboração de um plano de cibersegurança e e-governo, e ampliou seu alcance através do "Programa Interamericano de Apoio aos Poderes Legislativos" com ações de capacitação, regulação e a criação de um grupo de trabalho focado em "tecnopolítica" e cibersegurança. O CICTE continuou a ser o principal motor, fornecendo apoio crucial para a finalização das estratégias de cibersegurança da Guatemala e da República Dominicana. A capacitação em 2018 foi notavelmente diversificada e inclusiva, com treinamentos para 155 participantes, um *Cybersecurity BootCamp* para 300 pessoas, exercícios específicos para 160 mulheres, e um projeto de carreira para 160 jovens e um curso online que atingiu mais de 5.000 pessoas. No campo da defesa, a JID realizou a conferência "*Cyber defense in the Americas: The importance of Cyberspace as a Battlefield of the 21st Century*", sublinhando a importância estratégica do ciberespaço para as Forças Armadas. Institucionalmente, o CIJ estabeleceu um Relator específico de cibersegurança, sinalizando a importância da dimensão legal e normativa. Além disso, o DLC deu continuidade aos seus workshops, e o Secretário-Geral Adjunto abriu o workshop regional da REMJA, reforçando o compromisso de alto nível da OEA com a segurança cibernética na região (OEA, 2018).

Em 2019 houve um foco particular no desenvolvimento de capacidades cibernéticas regionais e na inclusão. O CICTE intensificou o treinamento especializado, atingindo 3.500 pessoas, e destacou-se pela inclusão de gênero, capacitando 790 mulheres através da iniciativa Cyberwoman Challenge, além de focar em jovens, oficiais e outros setores. Complementando a capacitação, a SSD, em um esforço de colaboração, criou o Laboratório de Cibersegurança para Ramos Legislativos. Em nível estratégico e de alto escalão, o Escritório do Secretário-Geral, as Agências Interamericanas e os Escritórios Nacionais fortaleceram as reuniões sobre cibersegurança, e a REMJA deu continuidade a seus workshops. A JID participou de 36 eventos sobre defesa que abordavam o tema como elemento central da "nova agenda de segurança hemisférica" e, reforçando essa institucionalização, o IADC promoveu a "Primeira Conferência de Ciberdefesa: Hemisfério Ocidental" em Bogotá e um "Seminário de Ciberdefesa e Cibersegurança" em sua sede. Finalmente, no aspecto legal, o CIJ discutiu a cibersegurança, o “*conventionality control”* e a proteção de dados pessoais,

demonstrando a crescente intersecção entre o ciberespaço e o direito interamericano (OEA, 2019).

O ano de 2020 foi marcado por uma adaptação intensificada às plataformas digitais devido à pandemia de Covid-19, refletindo-se em uma expansão significativa das atividades de cibersegurança e ciberdefesa da OEA. A SSM demonstrou um engajamento política e de capacitação inédito: organizou o Primeiro Encontro Digital de Presidentes dos Ramos Legislativos com a participação de 16 países, abordando temas de segurança cibernética e transformação digital, e criou o Laboratório de Cibersegurança e Transformação Digital para Ramos Legislativos das Américas, em colaboração com diversos setores. A SSD também produziu um vasto material de e-learning, realizando 25 encontros online, 30 podcasts e sete webinários sobre os temas. O CICTE continuou sendo o órgão central, e, nesse ano, focou consideravelmente em cibersegurança e biossegurança, em consequência da pandemia. O secretariado apoiou o Equador e a Jamaica na elaboração de suas estratégias nacionais, continuou as operações do CSIRTS Américas, realizou simpósios e *bootcamps,* e publicou cinco relatórios sobre cibersegurança no continente. A JID intensificou o uso de plataformas digitais para organizar e participar de atividades de segurança e cooperação, com um foco particular em ciberdefesa, promoveu a II Conferência de Ciberdefesa do Hemisfério Ocidental e ofereceu treinamento em ciberdefesa para 544 militares dos estados-membros. A dimensão legal e jurídica também progrediu: o CIJ adotou um relatório crucial intitulado *International Law and State Cyber Operations*, que ofereceu parâmetros para a aplicação do direito internacional no ciberespaço e ilustrou as posições dos estados-membros. Adicionalmente, a REMJA/DLC realizou análise legislativa sobre cibercrime e webinars sobre o tema, e o DOITS continuou a fornecer dados anuais sobre prevenção e ataques cibernéticos. Essas ações em 2020 sublinham o esforço coordenado da OEA para abordar a cibersegurança de forma holística, abrangendo os domínios político, técnico, de defesa e legal, em um contexto de aceleração digital forçada (OEA, 2020).

Em 2021, as ações da OEA no ciberespaço foram predominantemente virtuais e concentradas em três pilares: desenvolvimento de políticas, capacitação técnica e conscientização. A Secretaria do CICTE liderou os esforços, fornecendo apoio crucial para o desenvolvimento e revisão de políticas e estratégias nacionais de cibersegurança no Equador, Guiana, Jamaica e Costa Rica. O fortalecimento da

capacidade técnica regional foi alcançado pela Rede CSIRTAmericas (26 CSIRTs de 18 países), que realizou workshops focados em habilidades como ferramentas forenses digitais e diplomacia de crise. O CICTE também liderou o grupo de trabalho de cibersegurança da Red GEALC. A capacitação em massa continuou com sucesso em formato virtual, reunindo mais de 2.000 profissionais em eventos de destaque: o Simpósio sobre Cibersegurança 2021 (800 participantes), que abordou políticas para tecnologias emergentes e a cibersegurança para o setor judicial, e o Cybersecurity Summer Bootcamp 2021 (600 profissionais). Houve, ainda, um foco social importante, com o programa "Criando uma trajetória profissional em cibersegurança" capacitando mais de 200 estudantes de comunidades de baixa renda em cinco países. O Comitê também priorizou a diplomacia cibernética com cursos para 70 funcionários públicos e a questão de gênero, realizando diversas edições do Cyber Women Challenge e publicações sobre a violência online e a cibersegurança das mulheres durante a pandemia de COVID-19, confirmando um intenso foco na capacitação e no combate aos delitos e terrorismo cibernéticos (OEA, 2021). O relatório anual deste ano não apresenta informações específicas sobre a atuação de outros órgãos sobre cibersegurança, mas é possível compreender a abordagem geral por meio das iniciativas do CICTE.

Durante 2022, as medidas concentraram-se no desenvolvimento de políticas, fortalecimento de capacidades técnicas e uso de TICs para o desenvolvimento. A Rede CSIRTAmericas manteve sua relevância, operando ativamente para facilitar a cooperação e a coordenação técnica entre os CSIRTs nas Américas. Um marco diplomático importante foi a realização da Quarta Reunião do Grupo de Trabalho do CICTE sobre Medidas de Fomento da Confiança (CBMs) no Ciberespaço, no México, sublinhando o foco na segurança cooperativa. A capacitação e o intercâmbio de conhecimento foram intensos, com a realização de grandes eventos como o Simpósio sobre Cibersegurança 2022 e as Jornadas STIC (ICT Security Days) em Medellín, em colaboração com o Centro Criptológico Nacional da Espanha. O CICTE também lançou relatórios cruciais, como o "Estratégias Nacionais de Cibersegurança: Lições aprendidas e reflexões", e promoveu um diálogo sobre o Direito Internacional aplicável ao ciberespaço com os Estados membros. Paralelamente, a Assembleia Geral considerou um projeto de resolução que enfatizava o "Papel Fundamental da OEA no Avanço das Telecomunicações/Tecnologias da Informação e Comunicação por meio da CITEL".

Por fim, houve um foco contínuo na questão de gênero, com a participação da Secretaria do CICTE no evento do Grupo de Trabalho de Composição Aberta da ONU sobre Mulheres em Cibersegurança, e na gestão de ameaças, impulsionando ferramentas e redes especializadas de intercâmbio de informação (OEA, 2022).

As ações sobre o ciberespaço da OEA de 2023 foram focadas no desenvolvimento de políticas nacionais, fortalecimento de redes de resposta a incidentes e capacitação maciça, com ênfase na inclusão de gênero e no combate a ameaças emergentes. O Programa do CICTE continuou a apoiar o desenvolvimento de estratégias nacionais de cibersegurança, incluindo criação de planos de ação para implementação. No fortalecimento de capacidades técnicas, a Rede CSIRTAmericas expandiu-se para 46 CSIRTs associados de 21 estados-membros e inaugurou a Academia CSIRTAmericas, um espaço de formação virtual que capacitou cerca de 345 técnicos em respostas a incidentes. A capacitação em massa incluiu o IX Simpósio de Cibersegurança da OEA, realizado presencialmente nas Bahamas, que reuniu mais de 200 profissionais para discutir os desafios da Inteligência Artificial no mundo digital, e o *Cybersecurity Bootcamp 2023*, que contou com mais de 300 profissionais. A OEA lançou também a iniciativa *SheSecures* (sucessora do *Cyberwomen Challenge*), que envolveu mais de 1.200 mulheres de nove países. Adicionalmente, o programa "Criando uma trajetória profissional" capacitou mais de 400 estudantes de baixa renda, e a OEA colaborou com a CIM no desenvolvimento de uma lei modelo para erradicar a violência online. Em termos de governança, o ano viu a realização de cursos sobre Direito Internacional Humanitário (DIH) aplicável a operações cibernéticas e a organização de uma reunião interna para fortalecer a coordenação entre os 14 departamentos da Secretaria Geral que trabalham com segurança digital (OEA, 2023).

Por fim, o ano de 2024 demonstrou ênfase na defesa, cooperação técnica e inclusão. A JID intensificou o foco em ciberdefesa, organizando o Primeiro Exercício de Gestão de Crises Cibernéticas na Guatemala e promovendo o Seminário Hemisférico de Defesa Cibernética, tratando o ciberespaço explicitamente como um ambiente de perigo constante. Esse órgão também abriu inscrições para os cursos Hacker Rangers para mulheres, em associação com a iniciativa "Mulheres, Paz e Segurança". No âmbito político e de governança, houve discussões em nível regional, coordenadas pela OEA, sobre boas práticas em governança digital e a proposta de um marco de referência, visando a integração regional e a

padronização na gestão de dados e confiança, como abordado em um encontro em novembro. O CICTE continuou ativo em suas frentes tradicionais: o lançamento do *SheSecures 2024* reforçou o esforço de inclusão de mulheres na cibersegurança, e a organização do X Simpósio de Cibersegurança da OEA + RICET buscou o intercâmbio de informações e a discussão sobre tecnologias disruptivas com especialistas. A OEA/CICTE também lançou o Guia de Conceitos Básicos sobre a Violência de Gênero Online em setembro e esteve ativa no combate a ameaças específicas, como o ransomware no Brasil, por meio da *Brazil Ransomware Task Force* (OEA, 2024).

A coleta cronológica das medidas da OEA em cibersegurança revela que a maioria de suas ações se concentra em capacitação e treinamentos. No entanto, é importante ressaltar o apoio da organização na criação de estratégias e planos de cibersegurança, bem como na publicação de diagnósticos e relatórios sobre cibersegurança e ciberdefesa. Desse modo, o discurso que define a cibernética na Organização adquire relevância proeminente, pois molda não apenas as atividades de capacitação e instrução, mas também as diretrizes e o arcabouço conceitual disseminado aos estados-membros.

Ao considerar a articulação do discurso utilizado perante as políticas de cibersegurança da instituição, é pertinente investigar os atores que coordenaram e coordenam essas atividades, pois suas perspectivas sobre o tema influenciam diretamente as iniciativas que lideram. Com efeito, tanto articulação de termos e ideias sobre o ciberespaço, cibersegurança e ciberdefesa, quanto a consideração sobre os líderes da OEA são vetores de maximização de poder (conforme discutido no Capítulo 3). Esse poder discursivo, que apesar de não gerar poder é reflexo do poder material, perpetua retóricas de valores liberais, promove a aceitação do modelo tecnológico dos EUA, consolida a visão americana sobre tecnologia e confere vantagem na competição por valores cibernéticos (o modelo da Internet livre versus o da soberania digital).

No âmbito da cibersegurança, o discurso molda a agenda de segurança, visto que o Estado preponderante pode definir quais são as ameaças cibernéticas a serem priorizadas (o *threat subject* de Buzan) e assim, direcionar o processo de securitização do ciberespaço a seu favor. Desse modo, a priorização temática e institucional identificada na exploração dos relatórios da OEA é capaz de demonstrar a preponderância dos EUA na instituição. Por isso, a próxima seção é

dedicada a destrinchar esses aspectos, com o fim de associá-los à hipótese central desta pesquisa no final do presente capítulo.

4.2 INTERESSES DOS EUA EM CIBERSEGURANÇA

Conforme a argumentação desenvolvida até este ponto, entende-se que o Sistema Internacional se distingue pela insegurança recíproca entre os Estados, o que os impele a buscar incessantemente a otimização de sua segurança individual por meio da acumulação de poder. Assim, os países do mundo não se contentam com o equilíbrio de poder global, almejando, em última instância, ser a nação mais poderosa. Em outras palavras, o Realismo Ofensivo sustenta que a hegemonia, entendida como a dominação do sistema, é a melhor garantia de segurança (Mearsheimer, 2001). Perante o fato de que os Estados Unidos são o hegemon regional nas Américas, infere-se que seu maior interesse é manter essa supremacia para otimizar seu próprio poder e segurança. No que diz respeito ao contexto da cibersegurança, retoma-se o argumento desenvolvido por McCarthy (2015) segundo o qual a formulação de políticas de cibersegurança pelas autoridades estadunidenses foi fundamental para sustentar e ampliar o poder do país, alinhando metas econômicas, políticas e de segurança.

Segundo os documentos estratégicos dos Estados Unidos consultados, os principais interesses da potência no campo da cibersegurança e ciberdefesa ao longo do decênio 2015-2024 podem ser resumidos em: superioridade no ciberespaço; defesa de infraestruturas críticas; prosperidade econômica e inovação; e influência global por meio da propagação dos princípios da Internet Livre, parcerias internacionais e dissuasão cibernética[7] (EUA 2015, 2018a, 2018b, 2023, 2024).

Especificamente, na Estratégia Cibernética do Departamento de Defesa (DoD) de abril de 2015 o país estabelecia cinco objetivos estratégicos com vigência até 2020. O propósito geral do documento era guiar o desenvolvimento das forças cibernéticas do DoD e fortalecer sua postura de dissuasão cibernética, focando na

[7] A aplicação da teoria da dissuasão no domínio cibernético constitui uma questão complexa que protagoniza um debate contínuo. Nye (2017) ressalta que a eficácia da dissuasão cibernética está condicionada a uma abordagem matizada, a qual deve considerar o sujeito da dissuasão e o objeto em risco, sugerindo, assim, que a dissuasão opera de maneira distinta para cada tipo de ator e nível de ataque. Para uma compreensão mais aprofundada do tema, recomenda-se a leitura do artigo "*Deterrence and Dissuasion in Cyberspace*" de Joseph S. Nye Jr. (2017).

construção de capacidades e organizações para três missões principais: defender redes, sistemas e informações do DoD; defender a pátria e os interesses nacionais contra ciberataques; e apoiar operações e planos contingenciais. Em tempo, os cinco objetivos estratégicos definidos em 2015 foram: (i) construir e manter de prontidão forças e capacidades para condução de operações no ciberespaço; (ii) defender a rede de informações, proteger os dados e mitigar riscos para as missões do DoD; (iii) estar preparado para defender a pátria e os interesses vitais dos EUA de ciberataques destrutivos com consequências significativas; (iv) construir e manter opções cibernéticas e planos de ação para controlar escalação de conflitos e para moldar o ambiente conflituoso em todos os seus estágios; (v) construir e manter alianças e parcerias internacionais robustas para deter ameaças compartilhadas e melhorar a estabilidade e segurança internacionais (EUA, 2015). Essa estratégia serviu de base para o desenvolvimento do Comando Cibernético dos EUA (USCYBERCOM) e sua visão posterior, conforme mencionado no documento Visão de Comando para o Comando Cibernético dos EUA (2018b).

Por sua vez, os documentos de 2018 analisados apontam uma abordagem de “Defesa Avançada” (*Defend Forward*), que representa uma mudança significativa na postura militar dos EUA em 2018. Essa abordagem contou com cinco imperativos estratégicos: (i) alcançar e sustentar a superioridade decisiva sobre as capacidades do adversário; (ii) criar vantagens no ciberespaço para aprimorar operações em todos os domínios; (iii) criar vantagens de informação para apoiar resultados operacionais e alcançar impacto estratégico; (iv) operacionalizar o campo de batalha para manobras ágeis e responsivas; (v) expandir, aprofundar e operacionalizar parcerias. Para sustentar a vantagem estratégica nessa abordagem, o Comando se concentra em aumentar a resiliência, defender avançado (operando o mais próximo possível da origem da atividade adversária) e engajar continuamente os adversários (EUA, 2018b).

A partir desses dados é possível identificar como os interesses de manutenção de hegemonia são refletidos na postura dos EUA em cibersegurança e ciberdefesa. Todos os imperativos estratégicos supracitados colaboram para a construção de capacidades cibernéticas superiores aos adversários e vizinhos, corroborando na formação de um poder material maximizado no âmbito cibernético. O interesse de manutenção de hegemonia é traduzido claramente em pontos que

visam conservar superioridade sobre outros atores e capacidades de condução de operações no ciberespaço.

Em consonância, tanto os objetivos estratégicos definidos no documento de 2023 quanto seu plano de implementação de 2024 seguem uma linha similar. Nas diretrizes publicadas em 2024 são estipuladas 100 iniciativas de alto impacto que o governo federal está buscando para realizar os objetivos da Estratégia Nacional de Cibersegurança de 2023. As principais medidas em andamento incluem: defesa da infraestrutura crítica; desarticulação e desmantelamento de atores ameaçadores; moldagem de forças de mercado; e investimento em resiliência cibernética (EUA, 2024).

Isto posto, a análise das estratégias norte-americanas evidencia a permanência de um eixo de ação coerente com os princípios centrais do Realismo Ofensivo: preservar e ampliar o poder relativo por meio da superioridade tecnológica, militar e informacional. A cibersegurança não é tratada como mera pauta técnica, mas sim como imperativo de segurança nacional e projeção de poder. Isso converge com a ideia de que o ciberespaço consiste em um novo elemento estratégico devido à crescente interação humana e interconectividade global (Medeiros e Goldoni, 2020). No período de 2015 a 2024, observa-se a persistência na priorização da dissuasão, da defesa avançada e da cooperação internacional seletiva, empregadas como ferramentas de contenção e projeção de influência. A política de “defender adiante” e o investimento em alianças multilaterais — em especial com organismos regionais como a OEA — configuram mecanismos de externalização dos interesses nacionais.

Essa agenda de segurança cibernética reflete claramente o discurso de segurança coletiva multidimensional e resiliência hemisférica, o qual postula que os desafios securitários do ocidente são de natureza diversa e, por isso, exigem que o conceito e os enfoques tradicionais sejam expandidos para abranger ameaças novas e não tradicionais (OEA, 2003). A adoção e a priorização da cibersegurança neste escopo demonstram uma compreensão mais ampla e complexa das ameaças contemporâneas. A segurança não é mais vista apenas sob a ótica da defesa militar tradicional contra Estados-nação, mas incorpora dimensões não-militares, transnacionais e até mesmo não-estatais.

Ademais, ao difundir normas, padrões técnicos e narrativas de "livre e seguro uso da Internet", Washington impõe seu posicionamento frente ao embate de

valores digitais que vigora no cenário internacional contemporâneo. A concepção de Internet livre é relacionada à ideologia neoliberal propagada pelos EUA e confronta a noção de soberania digital, característica do eixo Sino-Russo. A perspectiva oriental sobre governança digital preconiza que um ambiente digital pacífico, seguro e cooperativo deve ser estabelecido por meio da regulação estatal e da cooperação internacional para o desenvolvimento tecnológico, partindo do pressuposto de que a soberania digital constitui uma extensão da soberania nacional para o ciberespaço. Em contrapartida, o conceito estadunidense de liberdade digital (*cyber freedom*) busca enfatizar que a liberdade de expressão e os direitos humanos transcendem a governança estatal e a soberania (Zheng, 2014). Contudo, o teórico chinês Ye Zheng (2014) tece críticas a esse conceito, classificando-o como hipócrita, ao argumentar que ele é mantido somente enquanto não ameaça a segurança dos próprios Estados Unidos e serve a suas práticas de intervenção sobre outros atores; caso contrário, é observada a prática de punição estatal contra atores que atuam no ciberespaço.

Assim, a agenda cibernética dos EUA reflete uma estratégia de manutenção de hegemonia que combina dominação tecnológica e diplomacia institucional. Em última instância, a cibersegurança é convertida em instrumento de poder, garantindo à potência a capacidade de moldar a governança digital internacional e de preservar sua primazia sistêmica.

A seção seguinte abordará esses aspectos em detalhe, estabelecendo a conexão entre eles e a estrutura institucional da OEA, bem como as medidas de cibersegurança identificadas nos documentos analisados. Essa análise será complementada por uma investigação específica sobre os líderes e chefes dos órgãos da instituição e uma discussão crítica sobre a influência hegemônica dos EUA na organização.

4.3 MATERIALIZAÇÃO DOS INTERESSES DOS EUA NA OEA

Para o Realismo Ofensivo, o papel das instituições internacionais é servir primariamente como um reflexo da distribuição de poder no mundo (Mearsheimer, 1994). Nesta perspectiva, a OEA serve como mecanismo de manutenção e expansão da hegemonia estadunidense, inclusive na área da cibersegurança. Os interesses dos EUA se manifestam principalmente através da instrumentalização da instituição para refletir e reforçar seu poder regional, isso ocorre por meio da

definição da agenda de segurança; modelagem das políticas de cibersegurança; projeção de poder e discurso; e predominância de atores estadunidenses em cargos de poder.

O estudo de caso revela claramente a aplicação dos vetores de poder adaptados da teoria de McCarthy (2015), desenvolvidos no capítulo anterior deste trabalho. Notavelmente, o vetor econômico (ou poder estrutural) é evidenciado pela proeminência econômica e tecnológica dos EUA na instituição regional. Além disso, o vetor produtivo (ou poder produtivo) manifesta-se através do uso do poder discursivo para moldar a agenda, as normas e os treinamentos da OEA.

A significativa presença de atores estadunidenses ou alinhados aos EUA em posições de liderança na organização contribui diretamente para a propagação de influência pelo vetor produtivo. Luis Almagro, Secretário-Geral da OEA de 2015 a 2025, iniciou sua carreira política no Uruguai, seu país natal, em uma coalizão de esquerda. Contudo, sua atuação internacional o posicionou em uma vertente cada vez menos alinhada aos ideais dessa coalizão em diversas questões regionais, sobretudo se afastando da defesa das instituições democráticas e do combate a regimes autoritários. Essa mudança de orientação gerou críticas à OEA: em 2021, o então Ministro das Relações Exteriores da Argentina, Felipe Solá, chegou a descrever Almagro como "imoral absoluto", acusando-o de colaborar com os Estados Unidos e de ter contribuído para o afastamento de Evo Morales do governo boliviano (Diplomatic Times, 2021); há críticos que argumentam que a eleição de Almagro em 2015 sinalizou um retorno da OEA a uma agenda que prioriza os interesses norte-americanos, o que foi evidenciado pela postura da organização em relação à Venezuela e pela deslegitimação das eleições bolivianas de 2019 (Seoane, 2023).

Com relação ao CICTE, os quatro Secretários Executivos do Comitê que ocuparam o cargo entre 2015 e 2025 são estadunidenses e ligados a serviços governamentais dos EUA: Neil Klopfenstein; Alfred Schandlbauer; Alison August Treppel e Violanda Botet (OEA, 2015b). Atualmente, a chefe da seção de cibersegurança do CICTE é Kerry-Ann Barrett, também natural dos EUA e alinhada com os interesses do país (Barrett, 2025). Ou seja, observa-se que cargos importantes de lideranças são ocupados por agentes ligados aos interesses do hegemon regional, o que facilita a legitimação das ideias para o ciberespaço das forças sociais estadunidenses e de seus Estados aliados. Além disso, o CICTE

estabeleceu convênios e publicou relatórios com empresas de cibersegurança estadunidenses, como Microsoft, Symantec e Trend Micro (Seoane, 2023).

Outro ponto ligado à propagação de ideias dos Estados Unidos na OEA, é o fato de que os treinamentos e reuniões do REMJA/DLC são coordenados pelo Departamento de Justiça dos EUA (OEA, 2016a). Essa coordenação estratégica não se limita à mera organização logística, ela abrange a definição de agendas, a seleção de tópicos prioritários e a escolha de especialistas e facilitadores. Ao assumir essa posição central, os Estados Unidos moldam o discurso e as abordagens em temas de segurança e justiça, garantindo que as perspectivas e os interesses norte-americanos sejam amplamente representados e, muitas vezes, internalizados pelos demais Estados-membros. Isso pode resultar na padronização de práticas e legislações regionais de acordo com modelos estadunidenses, impactando diretamente as políticas públicas e as estruturas jurídicas dos países latino-americanos no combate às ameaças cibernéticas.

Quanto ao vetor econômico de manifestação de poder, as fontes apontam que o financiamento da OEA depende dos EUA, que contribuiu com 59,4% do fundo regular em 2021 (Id., 2023). Essa proporção elevada ressalta a influência econômica que Washington exerce sobre a OEA, impactando diretamente sua capacidade de atuação e a priorização de suas agendas. Tal dependência levanta questões sobre a autonomia da organização e sua capacidade de agir independentemente dos interesses de seu principal financiador, especialmente em contextos de divergência política ou estratégica entre os membros. A principal consequência recai sobre o vetor produtivo de poder, pois a preponderância técnica e econômica acaba servindo como instrumento de coerção e convencimento, culminando na predominância da propagação do discurso favorável à dominação dos EUA dentro da organização.

Essa prática se evidencia na abordagem da segurança enquanto um aspecto multidimensional, formulada no âmbito da OEA e fortemente impulsionada nas estratégias dos EUA. O próprio alojamento do programa de cibersegurança da instituição na Secretaria do CICTE exemplifica claramente esse enquadramento institucional, visto que a finalidade do Comitê consiste em prevenir, combater e eliminar o terrorismo. A inclusão da cibersegurança na "nova agenda de segurança hemisférica" (OEA, 2019) também ilustra essa questão. Ademais, a abordagem da ciberdefesa como parte da pauta de “tarefas não convencionais” (OEA, 2017) das

Forças Armadas, ao lado do crime organizado e ameaças socioeconômicas, em seminários e treinamentos promovidos pela JID e pelo DLC, demonstra essa perspectiva.

A definição da segurança hemisférica enquanto uma problemática multissetorial tem sido, desde sua implementação, criticada pelos atores latino-americanos por ser um instrumento de manipulação hegemônica dos EUA e da legitimação de intervenções externas em nome da paz e segurança (Ziccardi, 2013). Após o fim da Guerra Fria, a justificativa para intervenção dos EUA a partir da luta contra o comunismo se esvaiu. Nesse cenário, a ampliação aparentemente progressista do escopo da segurança hemisférica criou um campo discursivo no qual qualquer fenômeno interno de um país da América Latina pode ser reinterpretado como risco hemisférico. Transferir o foco da segurança do Estado para o indivíduo (segurança humana) desqualifica o conceito de soberania e legitima intervenções diretas ou indiretas dos EUA (Silva Filho e Moraes, 2012). Com efeito, a construção dessa narrativa é também uma manifestação do vetor produtivo de maximização do poder estadunidense dentro da OEA.

As situações atuais da Colômbia e da Venezuela demonstram o uso do conceito de segurança multidimensional para legitimação da intervenção do hegemon regional norte-americano. Como aliada preferencial dos EUA, a Colômbia é usada como vitrine de adesão à agenda de segurança hemisférica. Isso é resultado do enquadramento do combate às drogas como uma ameaça hemisférica desde o Plano Colômbia (2000), que resultou na permissão da presença militar, financiamento, monitoramento e influência sobre a sua política interna por parte dos EUA. Inversamente, o caso da Venezuela se configura como um exemplo de como um Estado pode ser transformado discursivamente em uma ameaça regional, um movimento que pavimentou o caminho para a expansão da influência estadunidense na região. Essa transformação é frequentemente articulada por meio da retórica da segurança multidimensional, que inclui dimensões como o narcotráfico, o terrorismo, as crises humanitárias e a instabilidade democrática como ameaças dignas de intervenção externa. Essa narrativa se constrói explorando as vulnerabilidades internas do país (crise econômica, êxodo migratório e polarização política) e projetando-as como fontes de instabilidade que transcendem suas fronteiras, ameaçando a segurança e a estabilidade de seus vizinhos e, em última análise, os interesses dos Estados Unidos no hemisfério (Marshall, 2021). Dessa forma, a

inclusão da cibersegurança na perspectiva da segurança hemisférica, vinculada ao enfrentamento do terrorismo, representa uma nítida importação das preferências normativas dos Estados Unidos, em consonância com a agenda estabelecida no pós-Guerra Fria e alinhada à lógica da Guerra ao Terror.

No que diz respeito à cibersegurança, a menção à "segurança coletiva multidimensional" sugere que o enfrentamento de desafios cibernéticos não pode ser feito por um único país isoladamente. Pelo contrário, exige cooperação regional e hemisférica, compartilhamento de informações e coordenação de esforços para construir uma defesa cibernética robusta e interligada. Essa visão é um elemento central para justificar a execução de intervenções financeiras, de monitoramento e de capacitação dos EUA sobre os outros estados-membros da OEA, conforme descrito nos documentos analisados na primeira seção deste capítulo. A agenda de cibersegurança, portanto, é um pilar fundamental na implementação prática da visão de segurança que fundamenta a intervenção dos EUA nos assuntos securitários da América Latina e Caribe.

Outra consequência relevante da definição de ameaças ser guiada pelas prioridades dos EUA é que, ao focar em terrorismo e cibercrime, a OEA ignora problemas estruturais mais relevantes para a América Latina, como a espionagem (prioridade do MERCOSUL) ou a defesa cibernética em um sentido que contempla a soberania digital nacional. O caso do escândalo de espionagem do governo brasileiro pelos EUA, divulgado por Edward Snowden em 2013, exemplifica essa problemática, pois o caso gerou um fortalecimento do movimento regional Sul-Americano na UNASUL focado em defesa cibernética, ao passo que a OEA não demonstrou o mesmo apoio (Gonzales e Portela, 2018). Enquanto isso, a abordagem adotada se alinha com os objetivos estratégicos colocados nos documentos dos EUA, principalmente os que são focados na proteção da pátria, na combate a ameaças não-estatais/transnacionais e na projeção de influência global.

É evidente que a maioria dos países latino-americanos enxerga a reprodução da balança de poder regional na OEA, especialmente no que diz respeito à preponderância dos EUA[8]. Particularmente após a revelação de

[8] Desde a criação da OEA, os países da América Latina e Caribe demonstram insatisfação com a dominância dos Estados Unidos. É relevante assinalar que não se observa uma postura passiva por parte desses atores. Contudo, o foco deste trabalho reside em relacionar os interesses dos Estados Unidos com as diretrizes de cibersegurança da OEA. Sendo assim, o tópico relacionado às posturas dos outros estados-membros não será aprofundado.

ciberespionagem dos EUA em 2013, a busca por uma abordagem sul-americana afastada da ingerência de potências externas cresceu. A reação de países como Brasil, Argentina e Equador ao ocorrido enfatizou que as intromissões se deram em tempos de paz, o que prejudicou qualquer reconhecimento da intervenção como benéfica (Bustamante et al., 2015). Apesar disso, a preponderância dos Estados Unidos enquanto hegemon regional nunca deixou de se manifestar dentro da instituição, pois resulta da distribuição de poder do Sistema Internacional como um todo, conforme teorizado pelo Realismo Ofensivo.

Em última análise, o enquadramento na OEA espelha a distribuição de poder no continente americano, o que corrobora a teoria do Realismo Ofensivo de que as instituições multilaterais são um reflexo da balança de poder do Sistema Internacional. Apesar de, para a teoria realista, o discurso não gerar poder, ele o disfarça e normaliza, transformando relações assimétricas em narrativas de cooperação e resiliência regional. Nota-se que a OEA não é alicerçada na dimensão material, e sim em parâmetros de convencimento e ideologia. Embora o Realismo Ofensivo priorize o poder material como principal guia de análise, o elemento discursivo também se mostra relevante e não deve ser negligenciado. É crucial reconhecer que a problemática em estudo possui múltiplas causas, o que exige a abordagem de fatores que transcendem aqueles identificados e descritos por Mearsheimer.

5 CONSIDERAÇÕES FINAIS

Este trabalho foi desenvolvido com o objetivo central de investigar o efeito da hegemonia estadunidense nas instituições multilaterais, especialmente por meio da cibersegurança, utilizando as políticas de cibersegurança da Organização dos Estados Americanos como estudo de caso. A análise buscou avaliar em que medida os princípios da OEA, descritos pelos documentos da própria organização como alinhados à tradição diplomática latino-americana de solução pacífica de conflitos, são deturpados pela balança de poder e pelos interesses hegemônicos de maximização de poder dos Estados Unidos.

A investigação adotou a modalidade de estudo de caso qualitativo, findando realizar um estudo aprofundado de uma unidade para elucidar características de um fenômeno mais amplo. O estudo foi realizado de forma exploratória, com a finalidade de esclarecer como o fenômeno geral da influência hegemônica se manifesta a partir da política de cibersegurança da OEA de 2015 a 2024. Para guiar a pesquisa, foi adotada a hipótese de que as políticas de cibersegurança da OEA são influenciadas pela hegemonia dos EUA, na medida em que instituições internacionais servem como cenários de reprodução das estruturas de poder vigentes no Sistema Internacional.

No capítulo inicial foi desenvolvido o referencial teórico, por meio de revisão bibliográfica, ancorado no Realismo Ofensivo de John Mearsheimer. Essa teoria postula que o Sistema Internacional é anárquico, os Estados são seus atores principais e seu objetivo central é maximizar seu poder relativo para garantir a sobrevivência. Para o autor, a hegemonia regional é o maior status alcançável por uma grande potência. Crucialmente, a teoria realista define as instituições multilaterais, como a OEA, não como agentes autônomos de cooperação, mas sim como um reflexo direto da distribuição de poder. Assim, as grandes potências criam e moldam essas instituições para manter ou aumentar sua própria participação no poder mundial. A OEA, nesse sentido, é vista como um palco onde se desenrolam as dinâmicas de poder e é refletida a primazia dos EUA como hegemon regional.

O estudo foi complementado pela perspectiva de Joseph S. Nye sobre poder cibernético, que reconhece o ciberespaço como um novo e relevante contexto na política mundial. A partir disso defende-se que esse ambiente digital, por suas características de anarquia e competição, é condizente com o marco teórico realista

e que a cibersegurança, definida como as ações políticas para salvaguardar o ciberespaço e suas infraestruturas críticas, torna-se um componente estratégico fundamental para projeção e manutenção da hegemonia.

Por sua vez, o contexto da OEA foi traçado historicamente no Capítulo 3, demonstrando sua fundação no contexto da Guerra Fria e seu alinhamento com a agenda anticomunista dos EUA. No início do século XXI, a organização adotou o conceito de segurança multidimensional, ampliando seu escopo para incluir ameaças transnacionais como terrorismo, crime organizado e, notavelmente, ameaças cibernéticas. Essa transição reflete uma adaptação da política estadunidense do anticomunismo para o antiterrorismo, da Guerra Fria para a Guerra ao Terror, garantindo a continuidade de sua influência no continente frente às mudanças da geopolítica internacional.

No capítulo final desta pesquisa, a análise detalhada das políticas de cibersegurança da OEA entre 2015 e 2024, juntamente com a investigação sobre as estratégias de segurança cibernética dos EUA no mesmo período, confirmou a hipótese central do trabalho e forneceu resultados que transcendem a dimensão do poder material. De fato, as políticas de cibersegurança da OEA refletem a hegemonia dos Estados Unidos e servem como instrumentos para a manutenção e expansão de sua influência regional. Mas, além disso, foi possível observar de que formas essa dinâmica se manifesta e quais suas consequências para a política do continente.

A materialização da influência hegemônica dos EUA no campo cibernético foi analisada sob a lente dos vetores de maximização de poder: o vetor econômico (dependência financeira); o vetor produtivo (discurso); e o vetor material (infraestrutura tecnológica). O domínio discursivo da potência americana se mostrou um fator de extrema relevância na potencialização da preponderância do país sobre os outros autores. O fato de ser o país fundador da Internet permitiu aos EUA moldar os conceitos, doutrinas e a própria filosofia de proteção do ciberespaço adotada por organismos regionais como a OEA.

Nesse sentido, os relatórios estudados demonstram que a priorização temática da cibersegurança ao lado de questões como terrorismo, crime organizado e ameaças socioeconômicas alinha-se diretamente aos interesses estratégicos dos Estados Unidos definidos em seus documentos oficiais, que enfatizam a defesa de infraestruturas críticas, a desarticulação de atores ameaçadores não estatais (como

terroristas e criminosos) e a projeção de influência global. Essa abordagem reflete o enquadramento da segurança cibernética como uma problemática de segurança multidimensional, o que valida a intervenção e influência estadunidense sobre os assuntos do ciberespaço em outros países do continente americano, mesmo quando condizentes ao âmbito doméstico de cada Estado.

O alojamento institucional do programa de cibersegurança no Comitê Interamericano Contra o Terrorismo (CICTE), dependente da Secretaria de Segurança Multidimensional (SSM), é a principal evidência dessa influência. Ao vincular a cibersegurança ao antiterrorismo, a OEA importou as preferências normativas dos EUA, alinhando-se à lógica da Guerra ao Terror estabelecida no pós-11 de setembro. Essa dinâmica é reforçada pela proeminência de atores alinhados ou diretamente ligados ao governo estadunidense em posições chave na Organização. Além de os quatro Secretários Executivos do CICTE que ocuparam o cargo entre 2015 e 2025 serem norte-americanos ou ligados a serviços governamentais dos EUA, os treinamentos e reuniões promovidos pelo REMJA/DLC são coordenados pelo Departamento de Justiça dos Estados Unidos, permitindo que a potência molde o discurso e as abordagens jurídicas na região. O vetor produtivo de maximização de poder por meio do discurso é o que domina essa conjuntura.

Em suma, a OEA, ao priorizar uma agenda cibernética alinhada às estratégias de defesa dos EUA, opera como um mecanismo que reforça a ordem regional desejada pela potência hegemônica. Apesar de o discurso da cooperação ser um fator proeminente, o Realismo Ofensivo nos permite concluir que as relações de poder, e não a cooperação autônoma, são a força motriz subjacente às políticas de cibersegurança da Organização.

REFERÊNCIAS

ARRIGHI, Giovanni. Globalização e desenvolvimento desigual. Revista de Estudos e Pesquisas sobre as Américas, Brasília, v. 1, n. 1, p. [s.p.], 2007. Disponível em: https://periodicos.unb.br/index.php/repam/article/view/15910. Acesso em: jun. 2025.

AYRES PINTO, Danielle Jacon; OLIVEIRA, Marcos Aurélio Guedes de; SCHWETHER, Natália Diniz. Nota introdutória: geopolítica contemporânea e os desafios para a segurança e a defesa cibernéticas. Relações Internacionais, n. 82, p. 5-9, jun. 2024. DOI: 10.23906/ri2024.82a01. Acesso em: jun. 2025.

BUSTAMANTE, Gilberto Aranda; RIVERA, Jorge Riquelme; CAÑAS, Sergio Salinas. La ciberdefensa como parte de la agenda de integración sudamericana. Línea Sur, [S. l.], n. 9, p. 100-116, 2015.

CARR, Edward Hallett. Vinte anos de crise: 1919-1939. Brasília: Editora Universidade de Brasília, 2001. 312 p.

CLAUDE, Inis L. Jr. Power and International Relations. 5. ed. New York: Random House, 1962.

CLAUDE, Inis L. Jr. Swords into plowshares: the problems and progress of international organization. New York: Random House, 1971.

COELHO, Anelise Suzane Fernandes. Política Externa dos Estados Unidos em Relação à América Latina na Administração de Harry S. Truman. Revista Relações Internacionais do Mundo Atual, v. 2, n. 14, p. 159-185, 2010. DOI: http://dx.doi.org/10.21902/Revrima.v1i11.261. Acesso em: maio 2025.

COX, Robert W. Social forces, states and world orders: beyond International Relations theory. Millennium: Journal of International Studies, v. 10, n. 2, 1981.

COX, Robert W. Gramsci, hegemony and international relations: an essay in method. In: SINCLAIR, Timothy J. (ed.). Approaches to world order. Cambridge: Cambridge University Press, 1996. p. 124-143.

CRAIG, Anthony; VALERIANO, Brandon. Realism and cyber conflict: security in the digital age. E-International Relations, 3 fev. 2018.

DABLER, Benjamin; HEINKELMANN-WILD, Tim; HUYSMANS, Martijn. Insuring the weak: the institutional power equilibrium in international organizations. International Studies Quarterly, v. 69, 2024. Disponível em: https://academic.oup.com/isq/article/69/1/sqae146/7921925. Acesso em: maio 2025.

DINIZ, Eugenio. Política internacional: guia de estudo das abordagens realistas e da balança de poder. Belo Horizonte: Ed. PUC Minas, 2005. 146 p.

DIPLO FOUNDATION. Towards a secure cyberspace via regional co-operation. 2017. 20 p. Disponível em: https://diplo-media.s3.eu-central-1.amazonaws.com/2017/03/Diplo-Towards_a_secure_cyberspace-GGE.pdf. Acesso em: jun. 2025.

DIPLOMATIC TIMES. Argentina foreign minister describes OAS head Luis Almagro as “Absolute Immoral”. 17 mar. 2021. Disponível em: https://diplomatictimes.net/2021/03/17/argentina-foreign-minister-describes-oas-head-luis-almagro-as-absolute-immoral/. Acesso em: out. 2025.

DUNN CAVELTY, Myriam. The Politics of Cyber-Security. [S. l.]: Routledge, 2024. DOI: 10.4324/9781003497080.

DUNN CAVELTY, Myriam; WENGER, Andreas. Cyber security meets security politics: complex technology, fragmented politics, and networked science. [S. l.: s. n.], 2019.

ESTADOS UNIDOS DA AMÉRICA. President's Commission on Critical Infrastructure Protection (PCCIP). 1997.

ESTADOS UNIDOS DA AMÉRICA. Departamento de Defesa. Estratégia Cibernética do Departamento de Defesa. abr. 2015.

ESTADOS UNIDOS DA AMÉRICA. Comando Cibernético dos EUA. Visão de comando para o Comando Cibernético dos EUA. 2018.

ESTADOS UNIDOS DA AMÉRICA. Estratégia Cibernética Nacional dos Estados Unidos. set. 2018.

ESTADOS UNIDOS DA AMÉRICA. Estratégia Nacional de Cibersegurança. mar. 2023.

ESTADOS UNIDOS DA AMÉRICA. Plano de Implementação da Estratégia Nacional de Cibersegurança (NCSIP). maio 2024.

GALERANI, Kleber Antonio. Conselho Sul-Americano de Defesa: gênese, desenvolvimento inicial e desafios (2008-2010). Associação Brasileira de Relações Internacionais, 2011.

GAVIÃO, Leandro. Do Pan-Americanismo ao Sul-Americanismo: as identidades supranacionais no continente americano em três tempos (1826, 1960 e 2008). 2018. Tese (Doutorado em História) – Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

GERRING, John. What is a case study and what is it good for? American Political Science Review, v. 98, n. 2, 2004.

GILES, Keir; HAGESTAD, W. Divided by a common language: cyber definitions in Chinese, Russian and English. In: International Conference on Cyber Conflict, 5., 2013.

GONÇALVES, Williams da Silva. Segurança internacional na década de 1990. In: SILVA FILHO, Edison Benedito da; MORAES, Rodrigo Fracalossi de (org.). Defesa nacional para o século XXI: política internacional, estratégia e tecnologia militar. Rio de Janeiro: Ipea, 2012. p. 21-48.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. A geopolítica do espaço cibernético sul-americano: (in)conformação de políticas de segurança e defesa cibernética? Austral: Revista Brasileira de Estratégia e Relações Internacionais, Porto Alegre, v. 7, n. 14, p. 217-241, jul./dez. 2018.

GRASSI, Jéssica Maria; AYRES PINTO, Danielle Jacon. A construção de capacidade cibernética na América do Sul. [S. l.: s. n.], 2022.

GRASSI, Jéssica Maria; AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti. Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas. Relações Internacionais, n. 82, p. 11-27, jun. 2024. DOI: 10.23906/ri2024.82a02.

GUIMARÃES, Cesar. A política externa dos Estados Unidos: da primazia ao extremismo. Estudos Avançados, São Paulo, v. 16, n. 46, p. 54-63, 2002.

HERZ, John H. Idealist internationalism and the security dilemma. World Politics, v. 2, n. 2, p. 157-180, 1950.

HERZ, Monica. The Organization of American States (OAS). Abingdon: Routledge, 2011.

JACKSON, Robert H.; SORENSEN, Georg. Introduction to International Relations: theories and approaches. Oxford: Oxford University Press, 2007.

KEOHANE, Robert O. After hegemony: cooperation and discord in the world political economy. Princeton: Princeton University Press, 1984.

KEOHANE, Robert O.; MARTIN, Lisa L. The promise of institutional theory. International Security, v. 20, n. 1, p. 39-51, 1995.

KEOHANE, Robert O.; NYE JR., Joseph S. Power and interdependence in the information age. Foreign Affairs, v. 77, n. 5, p. 81-94, 1998.

LIBICKI, Martin C. Cyberdeterrence and cyberwar. Washington: RAND Corporation, 2009. ISBN 978-0-8330-4734-2.

LinkedIn. Kerry-Ann Barrett – cybersecurity professional. 2025. Disponível em: https://www.linkedin.com/in/kerry-ann-barrett-662b8210. Acesso em: out. 2025.

MACIEL, Tadeu; ZANIBONI, Juliana. Examining the perspective of public policies in cyber defense area: the Brazilian case. Revista da Escola de Guerra Naval, v. 29, n. 2, p. 267-290, 2023. DOI: 10.21544/2359-3075.29210.

MARSHALL, Will. The United States hegemonic challenge in Latin America. 2021. Dissertação (Mestrado) – Universiteit Leiden, Leiden, 2021. Disponível em: https://studenttheses.universiteitleiden.nl/access/item%3A3205095/view. Acesso em: 2025.

MCCARTHY, Daniel. Power, information technology, and international relations theory. London: Routledge, 2015.

MEARSHEIMER, John J. The tragedy of great power politics. New York: W. W. Norton & Company, 2001.

MEARSHEIMER, John J. The false promise of international institutions. International Security, v. 19, n. 3, p. 5-49, 1995. Disponível em: http://www.jstor.com/stable/2539078. Acesso em: maio 2025.

MEARSHEIMER, John J. War and international politics. International Security, v. 49, n. 4, p. 7-36, 2025. DOI: 10.1162/isec_a_00507.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The fundamental conceptual trinity of cyberspace. Contexto Internacional, v. 42, n. 1, p. 31-54, 2020. DOI: 10.1590/S0102-8529.2019420100002.

NETO, Hélio Franchini. A Conferência do Rio de Janeiro e o Tratado Interamericano de Assistência Recíproca. Revista Internacional de História Política e Cultura Jurídica, v. 7, n. 3, p. 473-489, 2015.

NYE JR., Joseph S. Cyber power. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2011.

NYE JR., Joseph S. Deterrence and dissuasion in cyberspace. International Security, v. 41, n. 3, p. 44-71, 2016. DOI: 10.1162/ISEC_a_00266.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Carta da Organização dos Estados Americanos. Bogotá, 30 abr. 1948.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Carta da Organização dos Estados Americanos: Protocolo de reformas, Manágua, 10 jun. 1993. Promulgado pelo Decreto nº 1.111/1994. Diário Oficial da União, Brasília, DF, 14 abr. 1994.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Página institucional. Washington, D.C.: OEA, [s.d.]. Disponível em: https://www.oas.org/en/. Acesso em: 2025.

OEA. Declaração sobre Segurança nas Américas. 2003.

OEA. Estrategia Interamericana Integral de Seguridad Cibernética. 2004.

OEA. Relatório Anual do Secretário-Geral: 2015. Washington, D.C.: OEA, 2015.

OEA. Relatório Anual do Secretário-Geral: 2016. Washington, D.C.: OEA, 2016.

OEA. Relatório Anual do Secretário-Geral: 2017. Washington, D.C.: OEA, 2017.

OEA. Relatório Anual do Secretário-Geral: 2018. Washington, D.C.: OEA, 2018.

OEA. Relatório Anual do Secretário-Geral: 2019. Washington, D.C.: OEA, 2019.

OEA. Relatório Anual do Secretário-Geral: 2020. Washington, D.C.: OEA, 2020.

OEA. Relatório Anual do CICTE: 2021. Washington, D.C.: OEA, 2021.

OEA. Relatório Anual do CICTE: 2022. Washington, D.C.: OEA, 2022.

OEA. Relatório Anual do CICTE: 2023. Washington, D.C.: OEA, 2023.

OEA. 2024 Cybersecurity Program. Washington, D.C.: OEA, 2024.

OEA. Comissão de Segurança Hemisférica. Relatório da Sessão: Reunião para considerar os novos conceitos de segurança hemisférica. 1999.

OEA. Comitê Interamericano contra o Terrorismo. Estatutos e documentos. Washington, D.C.: OEA, 2015.

OEA. Informe Anual 2021 del CICTE. Washington, D.C.: OEA, 2022.

OEA. 2022 Annual Report of the CICTE. Washington, D.C.: OEA, 2023.

OEA. Informe Anual 2023 del CICTE. Washington, D.C.: OEA, 2024.

ORAKHELASHVILI, Alexander. Collective security. Oxford: Oxford University Press, 2011. DOI: 10.1093/acprof:oso/9780199579846.001.0001.

OZEREN, Suleyman. Global response to cyberterrorism and cybercrime. 2005. Tese (Doutorado) – University of North Texas, Denton, 2005.

PRADO, Maria Ligia; PELLEGRINO, Gabriela. História da América Latina. 1. ed. São Paulo: Editora Contexto, 2014.

RID, Thomas. Cyber war will not take place. Journal of Strategic Studies, v. 35, n. 1, p. 5-32, 2012. DOI: 10.1080/01402390.2011.608939.

RID, Thomas; BUCHANAN, Ben. Attributing cyber attacks. Journal of Strategic Studies, v. 37, n. 4, p. 4-36, 2014. DOI: 10.1080/01402390.2014.977382.

ROCHA, Marcio; FONSECA, Daniel Farias da. A questão cibernética e o pensamento realista. Revista da EGN, v. 25, n. 2, p. 517-543, 2019.

SCHWARTAU, Winn. Information warfare: chaos on the electronic superhighway. New York: Thunder's Mouth, 1994.

SEOANE, Maximiliano Vila. La ciberhegemonía de EEUU en la OEA. Estudos Internacionais, Belo Horizonte, v. 10, n. 4, p. 91-112, 2023.

SHELDON, John B. Deciphering cyberpower: strategic purpose in peace and war. Strategic Studies Quarterly, v. 5, n. 2, p. 95-112, 2011.

SILVA FILHO, Edison Benedito da; MORAES, Rodrigo Fracalossi de (org.). Defesa nacional para o século XXI: política internacional, estratégia e tecnologia militar. Rio de Janeiro: Ipea, 2012. 346 p.

SOLAR, Carlos. Cybersecurity and cyber defence in the emerging democracies. Journal of Cyber Policy, v. 5, n. 3, p. 392-412, 2020. DOI: 10.1080/23738871.2020.1820546.

TABANSKY, Lior. Basic concepts in cyber warfare. Military and Strategic Affairs, v. 3, n. 1, p. 75-92, 2011.

THÉRIEN, Jean-Philippe; MACE, Gordon; GAGNÉ, Stefan. The changing dynamics of Inter-American security. Wiley, 2012.

VILLA, Rafael Duarte. A questão democrática na agenda da OEA no pós-Guerra Fria. Revista de Sociologia e Política, Curitiba, n. 20, p. 55-68, jun. 2003.

VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. Computers & Security, v. 38, p. 97-102, 2013. DOI: 10.1016/j.cose.2013.04.004. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404813000801. Acesso em: 2025.

WALTZ, Kenneth. Theory of international politics. Long Grove: Waveland Press, 1979. 251 p.

WALTZ, Kenneth. Structural realism after the Cold War. International Security, v. 25, n. 1, p. 5-41, 2000.

WALTZ, Kenneth. Man, the state, and war: a theoretical analysis. 2. ed. rev. New York: Columbia University Press, 2001. 263 p.