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

Eduardo de Rê

GOVERNANÇA GLOBAL DO CIBERESPAÇO COMO MECANISMO NA PROMOÇÃO DA SEGURANÇA INTERNACIONAL: UMA ANÁLISE A PARTIR DAS PERSPECTIVAS DE EUA, CHINA E RÚSSIA

Florianópolis
2024

Eduardo de Rê

GOVERNANÇA GLOBAL DO CIBERESPAÇO COMO MECANISMO NA PROMOÇÃO DA SEGURANÇA INTERNACIONAL: UMA ANÁLISE A PARTIR DAS PERSPECTIVAS DE EUA, CHINA E RÚSSIA

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

Orientador(a): Profa. Dra. Danielle Jacon Ayres Pinto

Florianópolis

2024

de Rê, Eduardo
Governança global do ciberespaço como mecanismo na promoção da segurança internacional: uma análise a partir das perspectivas de EUA, China e Rússia / Eduardo de Rê ; orientadora, Danielle Jacon Ayres Pinto, 2024.
159 p.

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

Inclui referências.

1. Relações Internacionais. 2. Segurança internacional. 4. Governança global. I. Ayres Pinto, Danielle Jacon. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Eduardo de Rê

GOVERNANÇA GLOBAL DO CIBERESPAÇO COMO MECANISMO NA PROMOÇÃO DA SEGURANÇA INTERNACIONAL: UMA ANÁLISE A PARTIR DAS PERSPECTIVAS DE EUA, CHINA E RÚSSIA

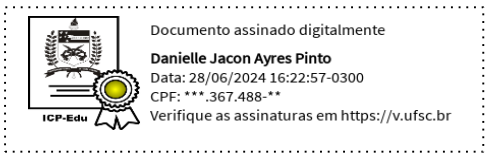
O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 19 de abril de 2024, pela banca examinadora composta pelos seguintes membros:

Profa. Danielle Jacon Ayres Pinto, Dra
Universidade Federal de Santa Catarina

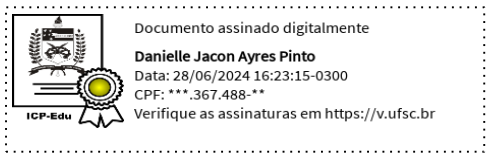
Profa. Graciela de Conti Pagliari, Dra
Universidade Federal de Santa Catarina

Prof. Jacintho Maia Neto, Dr.
Escola Superior de Guerra

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



Coordenação do Programa de Pós-Graduação



Profa. Dra. Danielle Jacon Ayres Pinto
Orientadora

Florianópolis, 2024.

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer à minha família, que me deu todo o suporte e as condições necessárias para que eu pudesse chegar até aqui. Em especial, agradeço aos meus pais, Dirceu e Elisandra, que sempre estiveram ao meu lado me apoiando e amparando emocionalmente, psicologicamente e materialmente. Muito obrigado por tudo.

Aos professores que tive durante a toda a minha vida e trajetória acadêmica, pessoas que dedicam suas vidas ao ensino e à educação, uma profissão nobre e essencial na formação de todo cidadão. Em especial agradeço à minha orientadora, Danielle, que me auxiliou não só na elaboração deste trabalho, mas em grande parte da minha vida acadêmica.

Aos meus amigos de vida e da pós-graduação, suas companhias me auxiliaram e animaram sempre.

À minha namorada e companheira, Ana Paula, que esteve ao meu lado durante a elaboração deste trabalho, me amparando, apoiando e tornando os meus dias mais alegres. É um privilégio poder compartilhar a vida com você.

Por fim, mas não menos importante, agradeço à UFSC e ao sistema público de ensino, que proporciona um caminho de luz e conhecimento para muitos brasileiros, mesmo diante de tantas adversidades.

RESUMO

O ciberespaço se tornou um domínio de poder capaz de afetar tanto as nossas atividades mais básicas, quanto atividades que exigem um grande grau de especialização. Dessa forma, a interconexão entre o mundo digital e o mundo material faz com que esse domínio faça parte da agenda da política internacional e o seu gerenciamento, controle e administração tenha grande relevância para o cenário geopolítico. No entanto, esse domínio carece de um conjunto aceito de regras e regulamentos em nível internacional que orientem o comportamento e as responsabilidades dos Estados. Sendo assim, este trabalho tem como objetivo principal compreender se a construção e implementação de uma governança global para o ciberespaço tem a capacidade de mitigar tensões e desconfianças entre os Estados no que concerce aos seus comportamentos no espaço cibernético. Parte-se de uma abordagem metodológica hipotética-dedutiva com base na análise qualitativa de informações, tendo como hipótese que o estabelecimento da governança global para o ciberespaço promove a segurança internacional. Entende-se que a governança envolve diversas dimensões, incluindo uma estrutura normativa, com regras, normas e princípios, padrões de condutas e coordenação de políticas, sendo assim, o trabalho analisa como esse fenômeno aplicado ao espaço cibernético produz efeitos para as relações entre os Estados, especialmente no que tange à segurança. Para isso, além do entendimento do conceito tradicional de governança, foram observados as perspectivas e os posicionamentos de Estados Unidos, China e Rússia sobre a governanaça global do ciberespaço, por meio da análise dos seus documentos governamentais que abordam sobre o assunto, compreendendo também os modelos *multistakeholder* e multilateral de governança que estão em debate nas discussões internacionais. Com isso, com base na linha da segurança ontológica, foram analisadas as implicações para a segurança internacional que a implementação de uma governanaça global para o ciberespaço pode suscitar, chegando à conclusão de que ao prever um sistema de regras e a conformidade, com o estabelecimento de uma ordem, essa implementação pode fomentar a segurança para as relações entre os Estados.

Palavras-chave: governança global; ciberespaço; segurança internacional.

ABSTRACT

Cyberspace has become a domain of power capable of affecting both our most basic activities and activities that require a high degree of specialization. In this way, the interconnection between the digital world and the material world makes this domain part of the international politics agenda, and its management, control, and administration are of great relevance to the geopolitical scenario. However, this domain lacks an accepted set of rules and regulations at the international level to guide the behavior and responsibilities of States. Therefore, this work aims to understand if the construction and implementation of a global governance for cyberspace have the ability to mitigate tensions and distrust among States regarding their behaviors in cyberspace. It starts from a hypothetical-deductive methodological approach based on qualitative analysis of information, assuming that the establishment of global governance for cyberspace promotes international security. It is understood that governance involves various dimensions, including a normative structure with rules, norms, and principles, standards of conduct, and policy coordination. Thus, the work analyzes how this phenomenon applied to cyberspace produces effects on relations between States, especially regarding security. In addition to understanding the traditional concept of governance, the perspectives and positions of the United States, China, and Russia on global governance of cyberspace were observed through the analysis of their government documents addressing the subject, also encompassing the multistakeholder and multilateral governance models being debated in international discussions. Based on the ontological security line, the implications for international security that the implementation of global governance for cyberspace can raise were analyzed, leading to the conclusion that by foreseeing a system of rules and compliance, with the establishment of an order, this implementation can promote security in relations between States.

Keywords: global governance; cyberspace; international security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA Advanced Research Projects Agency
ASO Adress Supporting Organization
CERN Conselho Europeu para Pesquisa Nuclear
ccNSO Country Code-Names Supporting Organization
DFI Declaração para o Futuro da Internet
DHS Department of Homeland State
DNS Sistema de Nomes e Domínio
DoD Department of Defense
DDoS Ataques de negação de serviço
END Estratégia Nacional de Defesa
EUA Estados Unidos da América
GAC Governmental Advisory Committee
GGE Grupos de Especialistas Governamentais da ONU
GNSO Generic Names-Supporting Organization
ICANN Internet Corporation for Assigned Names and Numbers
IETF Força-Tarefa de Engenharia de Internet
IP Protocolo da Internet
MD Ministério da Defesa
NSA Agência de Segurança Nacional
OCDE Organização para a Cooperação e Desenvolvimento Econômico
OIT Organização Internacional do Trabalho
OMC Organização Mundial do Comércio
ONU Organização das Nações Unidas
OTAN Organização do Tratado do Atlântico Norte
PNUD Programa de Desenvolvimento das Nações Unidas
RIs Relações Internacionais
SCO Shanghai Cooperation Organization
TICs Tecnologias da Informação e Comunicação
UE União Europeia
UIT União Internacional de Telecomunicação
WCIT Conferência Mundial sobre Telecomunicações Internacionais
WGIG Grupo de Trabalho sobre a Governança da Internet

WWW World Wide Web

SUMÁRIO

1 INTRODUÇÃO

De acordo com o *Internet World Stats*[1], em 2022 o mundo atingiu a marca de mais de 5.3 bilhões de pessoas com acesso à Internet, dando uma proporção da relevância do ambiente digital e das tecnologias ligadas a ele para a sociedade global. Dessa forma, chega a ser impensável a maneira de vida levada hoje pela humanidade sem a Internet e os sistemas digitais. A conexão e a interdependência criada entre o setor cibernético e as relações sociais transbordaram os seus efeitos para todas as áreas da vida, fazendo com que hoje o espaço cibernético, ou ciberespaço, esteja presente nas pautas das políticas nacionais tomadas pelos países, bem como na política internacional. Na verdade, o ciberespaço não é exógeno à interação social, mas sim um fator político que já está embutido na condição material do mundo (Blount, 2016).

Isso porque o ciberespaço, além de criar novas oportunidades de inovação a partir da digitalização de sistemas antes analógicos, resultando, por exemplo, no aprimoramento da comunicação por meio de um intenso fluxo de informações, também possibilitou que novas ameaças viessem à tona. Ameaças essas que atualmente poderiam colocar em risco todo o funcionamento e ordenamento de uma nação. À vista desse contexto, somado à uma mudança na natureza dos conflitos ao redor do mundo, sendo que o ciberespaço possui influência, mesmo que de maneira indireta, em todos esses aspectos, a forma como o domínio cibernético e a Internet são governados é uma preocupação de política pública, com efeitos sobre os direitos humanos, economia internacional, segurança nacional e internacional e direitos de propriedade, com capacidade de aumentar as tensões na geopolítica mundial (DeNardis, 2020).

Não sem motivo, o que antes era visto como um assunto estritamente técnico, como controle de dados e programação de sistemas, agora está na agenda política da comunidade internacional. Sendo assim, a atenção dada aos Estados para questões como a segurança cibernética e a defesa cibernética reside no entendimento de que, com o gradual e acelerado processo de digitalização, os métodos e as estratégias convencionais de segurança e defesa não serão eficazes contra as ameaças cibernéticas (Haddad; Binder, 2019). Dessa forma, muitos governos passaram a investir recursos para o desenvolvimento de capacidades defensivas e ofensivas no setor cibernético (Borghard; Lonergan, 2017).

Por ser um novo domínio, o ciberespaço possui variadas interpretações e conceituações, tanto no meio acadêmico quanto pelos países ao definirem e compreenderem esse espaço em

[1] Disponível em: https://www.internetworldstats.com/stats.htm

seus documentos estratégicos. Autores como Singer e Friedman (2013) elucidam que o ciberespaço consiste em um ambiente virtual onde há fluxos de informações e dados que podem ser armazenados e compartilhados. Países como os Estados Unidos (EUA), enxergam o ciberespaço como um domínio de poder, que possibilita vulnerabilidades e a utilização de capacidades defensivas e ofensivas (Estados Unidos, 2018c). Já a China, por exemplo, enxerga o ciberespaço como um ambiente composto por redes de comunicação, Internet, controle de sistemas automatizados, dispositivos digitais, serviços e dados, que está transformando a vida em sociedade, sendo que a soberania nacional deve prevalecer de forma que a segurança cibernética seja garantida (China, 2016a).

Dentre a gama de definições, neste trabalho será levado em consideração a definição de Daniel T. Kuehl (2009), que expressa que o ciberespaço é um domínio global que tem como característica o uso de eletrônicos e de espectros eletromagnéticos para criar, armazenar, modificar, trocar e explorar informações a partir da utilização de Tecnologias da Informação e Comunicação (TICs). Dessa forma, o ciberespaço acaba sendo um espaço capaz de proporcionar preocupações aos Estados, não apenas devido aos fluxos de informações em seu território, mas também por permitir que ações hostis possam ser perpetradas através dele.

Contudo, mesmo muitos países vendo o ciberespaço como uma possível fonte de insegurança e instabilidade, tanto em nível nacional, quanto internacional, a grande parte das políticas, diretrizes e estratégias construídas para a proteção do espaço cibernético se dá apenas na dimensão nacional. Isso significa que atualmente não há uma convenção ou uma regulamentação internacional efetiva para o espaço cibernético. Para Anne Verhelst e Jan Wouters (2020), a inexistência dessa regulamentação se deve às próprias características do ciberespaço, em que o seu escopo, definição e significado ainda são imprecisos e distintos entre os atores do sistema internacional. Sendo assim, pode-se dizer que situação atual é marcada pela falta de um entendimento comum entre os Estados sobre o que o espaço cibernético representa, sobre como deve ser utilizado e sobre as dinâmicas que ele possibilita.

Dessa forma, apesar da relevância do ciberespaço para o cenário global, este trabalho parte da premissa de que atualmente não existe uma governança composta por um sistema de princípios, normas e regras que regulamentem esse domínio em nível global deixando com que os Estados nacionais formulem e promovam os seus próprios entendimentos e políticas para o espaço cibernético. O teórico Joseph Nye (2014) caracteriza esse cenário como um regime complexo, em que há uma governança imperfeita, marcada por um fraco acoplamento entre um conjunto de normas e as instituições que o integram. Assim, como uma resposta a esse contexto

anárquico, muitos Estados vêm adotando ações de projeção de poder que visam proteger o seu espaço cibernético, em uma espécie de territorialização do ambiente virtual.

Nesse sentido, na busca por tentar compreender esse complexo contexto e os seus efeitos para a segurança internacional, visto que o ciberespaço tem potencial de proporcionar grandes instabilidades e gerar conflitos a partir da sua utilização, este trabalho tem a intenção de responder a seguinte pergunta de partida: como a implementação de uma governança global para o ciberespaço impacta o cenário da segurança internacional? Para isso, será levado em consideração a conceituação de governança por James N. Rosenau (1992), que manifesta que a governança é determinada como um arranjo de normas e regras com objetivos estabelecidos e compartilhados entre os atores, para construir uma regulamentação e uma ordem, se caracterizando por ser um fenômeno que engloba instituições governamentais e não governamentais.

Dessa forma, a governança é entendida como um sistema de regras que cumpre seu papel ao ser aceito pela maioria, sendo capaz de produzir um ordenamento que facilita as interações no sistema internacional, visto que os atores tendem a se comportar conforme um conjunto de princípios e diretrizes em comum (Rosenau, 1992). Por essas características, a governança pode ser confundida com os regimes internacionais, visto que estes também tratam sobre princípios, normas, regras e procedimentos de áreas que englobam as relações internacionais. Nesse sentido, como coloca Stephen Krasner (1982), a função dos regimes é arquitetar uma coordenação para o comportamento dos Estados em áreas particulares de interesse. Assim, quando pensamos no ciberespaço, isso parece fazer sentido, já que se trata de uma área particular de interesse dos atores estatais, em que a construção de princípios e normas que guiem o comportamento desses atores configuraria a construção de um regime internacional, mas não é o caso.

Isso porque há uma característica dos regimes internacionais que faz com que a construção de uma regulamentação internacional para o espaço cibernético seja concebida como governança. Essa característica é a de que os regimes, além de tratarem de arranjos especiais, normalmente envolvem somente alguns membros específicos da sociedade internacional (Rosenau, 1992). O ciberespaço, por sua vez, é um domínio que, diferente dos outros, engloba a participação de múltiplos atores no sistema internacional e envolve praticamente todos os membros da sociedade internacional, que ou afetam ou são afetados pelo espaço cibernético, devido ao enorme grau de dependência que a vida humana possui com o setor cibernético.

E não apenas isso, mas também pela peculiaridade do ciberespaço em afetar todos os demais domínios, em vista da sua significativa transversalidade, conforme ressalta Walfredo Bento Ferreira Neto (2013). Isso significa que a amplitude da área cibernética dentro das relações internacionais faz com que a confecção de um sistema de regras, condutas, comportamentos, princípios e procedimentos em âmbito global para o ciberespaço não se configure como um regime internacional, e sim uma governança, formando uma gama de arranjos para se estabelecer uma ordem.

Nesse contexto, de ausência de governança global para o ciberespaço, este domínio cria desafios globais não somente por proporcionar ameaças cibernéticas, mas também por conta das suas particularidades que diferem dos domínios tradicionais, como a falta de fronteiras em vista da sua dimensão não-física. Com isso, questões como a aplicação do princípio da soberania para o espaço cibernético emergem como um dilema a ser resolvido, já que seu aspecto virtual pode questionar a capacidade do Estado em controlar a movimentação de dados e informações em suas fronteiras (Khanna, 2018). Ocorre que essas questões e preocupações parecem não serem respondidas pelo direito internacional contemporâneo, já que seus dispositivos não são voltados a atender as especificidades do domínio cibernético.

De maneira geral, as atribuições de ataques cibernéticos por Estados invocaram o direito internacional apenas nos termos mais gerais possíveis (Efrony; Shany, 2018). Isso porque a forma sobre como aplicar os princípios do direito internacional ainda é uma incógnita não resolvida pela comunidade internacional. E, para além disso, a ausência de regulamentação específica faz com que os Estados se sintam livres para agir da forma como enxergam o ciberespaço, sem constrangimentos em relação às suas atitudes nesse ambiente (Eilstrup-Sangiovanni, 2018). Dessa forma, isso poderia favorecer um cenário de disputas entre os Estados, visto que o ciberespaço é um ambiente de projeção de poder, que resultaria em um maior risco para a segurança internacional.

Assim, este trabalho tem como hipótese que a implementação de uma governança global para o ciberespaço possibilita um cenário de maior segurança para os Estados no âmbito internacional. E, para observar se a ausência dessa governança favorece um cenário de insegurança entre os Estados, será levado em consideração a linha teórica construtivista. Pois, como coloca Alexander Wendt (1992), a busca pela segurança no sistema internacional não é um processo dado pela anarquia, mas um processo construído pelos Estados a partir dos seus comportamentos e ações, que estão ligados com a concepção que possuem de si e dos outros, formando suas identidades e interesses. Nesse sentido, é levado em consideração que os Estados ainda estão em um processo de formação de suas identidades e interesses em relação ao

ciberespaço, visto que esse domínio é novo e as concepções sobre ele ainda não estão totalmente definidas.

Em sintonia com a teoria construtivista, será utilizado a perspectiva da segurança ontológica, trazida por autores como Catarina Kinnvall e Jennifer Mitzen (2016) e Amir Lupovici (2023), que relacionam a segurança com a percepção que um ator possui de si mesmo com o mundo ao seu redor, levando em consideração diferentes aspectos como incertezas, ansiedades, capacidades, sentimentos e sensações que podem conduzir um ator a se comportar de determinada maneira. Nesse sentido, a partir da segurança ontológica, interpreta-se que os atores do espaço cibernético ainda estão em uma fase inicial de compreensão do que efetivamente representa a segurança no ambiente cibernético e como podem lidar com as ameaças possibilitadas por ele.

Por isso, este trabalho se propõe a explorar a relevância da construção de uma governança global para o ciberespaço, na pretensão de preencher a lacuna de verificar se o estabelecimento dessa governança pode ser capaz de promover a segurança internacional. Sendo assim, tem-se como objetivo geral compreender se a possível construção de uma regulamentação internacional oficial para o ciberespaço, representando assim uma governança que engloba mecanismos, diretrizes e normas, é capaz de atenuar as tensões e inseguranças entre os Estados em relação aos seus comportamentos no espaço cibernético.

Em concomitância com o objetivo geral da pesquisa, apresentam-se os seguintes objetivos específicos: (i) analisar o fenômeno do ciberespaço e os seus efeitos para as relações internacionais, especialmente no que tange à segurança internacional; (ii) evidenciar e compreender sobre os dois modelos de governança global do ciberespaço em debate na agenda internacional, o modelo *multistakeholder* e o modelo multilateral, entendendo as suas principais características e possíveis impactos; (iii) compreender e apresentar como Estados Unidos, China e Rússia enxergam o estabelecimento de uma governança global para ciberespaço; (iv) entender se a manutenção da ausência de uma governança global para o espaço cibernético gera um cenário de incertezas e imprevisibilidade entre os Estados, resultando em um contexto de insegurança.

Para isso, parte-se de um método hipotético-dedutivo de abordagem, visto que se tem um problema, já exposto, que instiga a formulação de uma hipótese, podendo ser interpretada como uma espécie de solução provisória para o problema apresentado. A lógica em relação à busca pela comprovação ou rejeição de tal hipótese é a dedutiva, visto ser baseada na análise qualitativa de informações e pesquisas previamente realizadas sobre governança global e o ciberespaço. Nesse sentido, a investigação tem como caminho apresentar o que constitui uma

governança a partir dos seus conceitos tradicionais nas relações internacionais; realizar uma análise sobre como essa governança pode ser implementada ao ciberespaço, levando em consideração as suas características; e evidenciar os impactos, em termos qualitativos, que a implementação dessa governança acarretaria ao sistema internacional, especialmente em relação à segurança internacional.

De forma a compor a parte empírica da investigação e atender aos objetivos específicos, são analisados os documentos governamentais de Estados Unidos, China e Rússia que abordam sobre a governança global do ciberespaço, bem como declarações de autoridades, já que esses países possuem divergência em relação às suas concepções sobre o espaço cibernético e são potências mundiais com grandes capacidades de projeção de poder e de influência no contexto da segurança internacional. A análise documental e de declarações dos três países supracitados será feita de modo a demonstrar como algumas das mais importantes nações do mundo estão pensando sobre o tema, bem como para verificar se as suas posições indicam que a governança global do ciberespaço afeta, mesmo que indiretamente, a segurança internacional.

Além disso, a investigação conta com uma revisão bibliográfica a partir de fontes secundárias que englobam o assunto, como artigos científicos, teses, dissertações e livros, de forma a servir como uma base informativa capaz de fundamentar o trabalho conceitualmente e teoricamente. Isso significa que essas fontes terão os seus conteúdos analisados, visto que isso caracteriza uma técnica de pesquisa geralmente utilizada para uma série de bibliografias e produções acadêmicas (Megale, 1990). Ademais, como forma de facilitar a leitura por parte do(a) leitor(a), seguindo o exemplo de Barros (2004), as citações em língua estrangeira são traduzidas para o português no corpo do texto, com a citação original em língua estrangeira em nota de rodapé, exceto determinadas definições e títulos para não afetar o significado original.

Por fim, os resultados são abordados de forma qualitativa, de modo a atribuir conteúdo valorativo à realidade existente ao analisar o fenômeno da governança global e a sua aplicabilidade ao ciberespaço - regulamentando esse domínio -, compreendendo que dentre os efeitos da sua implementação no mundo está a promoção da segurança internacional. Dessa forma, o trabalho está dividido em quatro capítulos, além desta introdução e as considerações finais. O primeiro capítulo trata sobre o conceito de governança global e de bens públicos globais, visto que o espaço cibernético pode ser entendido como um bem público global a partir da conceituação de Inge Kaul *et al.* (1999), além de abordar sobre a questão da soberania nacional nas relações internacionais. O capítulo apresenta as concepções tradicionais sobre esses elementos para que se possa fazer as suas correlações com o espaço cibernético como um novo domínio que afeta a política internacional.

O segundo capítulo aborda sobre a definição e características do ciberespaço, apresentando as suas especificidades, de forma a compreender os seus efeitos para as relações internacionais. Assim, o capítulo também abrange questões como a segurança cibernética e a defesa cibernética, bem como sobre a ausência de uma regulamentação internacional para o ciberespaço, a partir da análise sobre como o direito internacional rege o espaço cibernético, de modo a evidenciar as lacunas deixadas pelas normas internacionais atuais na aplicabilidade dos seus dispositivos para o domínio cibernético.

O terceiro capítulo trata sobre os modelos *multistakeholder* e multilateral de possível governança global para o ciberespaço, identificando suas características e destacando as suas diferenças, para que se possa evidenciar o que representam. Além disso, o capítulo versa sobre as posições e entendimentos de Estados Unidos, China e Rússia sobre a governança global do ciberespaço e os modelos citados, a partir da análise dos documentos governamentais. Por fim, o quarto e último capítulo consiste na análise e reflexão crítica sobre todo o exposto nos capítulos anteriores, de modo a responder à pergunta de partida, bem como averiguar o falseamento ou não da hipótese proposta. Assim, o capítulo aborda sobre os impactos da implementação de uma governança global, especialmente a partir do molde multilateral, traçando a sua relação com a segurança internacional.

2 A GOVERNANÇA NA POLÍTICA INTERNACIONAL

Neste capítulo serão abordadas questões teóricas e conceituais sobre governança, bens públicos globais e soberania. O entendimento conceitual dessas questões é fundamental para que se possa fazer a correlação desses conceitos com o espaço cibernético como um novo domínio na política internacional. Por isso, este capítulo apresenta as concepções tradicionais sobre o que caracteriza a governança em nível global, o que significa um bem público global, qual a definição de soberania e como esses elementos acabam se inter-relacionando nas relações internacionais. Além disso, será apresentado de maneira introdutória e superficial, que o ciberespaço como um novo domínio de poder se interliga com a governança, os bens públicos globais e o princípio da soberania.

Essa interligação ocorre principalmente pelo ciberespaço produzir efeitos sobre como os atores se relacionam e criar certos desafios e dificuldades de implementação de conceitos tradicionais, como no caso da soberania. Dessa forma, ao final do capítulo é apresentado, de forma sucinta, visto que esse ponto será também adentrado nos próximos capítulos, o debate existente sobre a implementação de uma soberania do espaço cibernético.

2.1 O CONCEITO DE GOVERNANÇA E SUA RELAÇÃO COM BENS PÚBLICOS GLOBAIS

A humanidade possui como habilidade a capacidade da cooperação em grande escala, sendo essa uma das razões pela qual a nossa espécie ainda sobrevive e foi capaz de se tornar soberana no planeta Terra. Olhando para os considerados clássicos, como Thomas Hobbes, John Locke e Jean Jacques-Rousseau, interpreta-se que essa competência foi um dos fatores essenciais para que pudéssemos construir arranjos sociais, políticos e econômicos capazes de proporcionar ordenamento para a vida em sociedade. Assim, os “contratos sociais” foram estabelecidos e estruturas de governabilidade foram formadas de modo a legitimar normas e princípios capazes de conduzir as relações sociais.

Isso significa que o ser humano tem uma tendência a preferir a ordem ao caos, em que o cumprimento de regras é uma das condições para que isso se torne realidade. Assim, da mesma maneira em que podemos enxergar a importância da construção de diretrizes para que a organização social seja alcançada em nível micro - como em vilas, cidades e até países - podemos enxergar para o nível macro, nas relações internacionais entre os Estados. No mundo atual, grupos, instituições, organizações e governos estão cada vez mais integrados e

interconectados, ao mesmo tempo em que estão fragmentados no que tange a resolução de problemas e as políticas e arranjos utilizados para lidar com cada diferente área.

Isso significa que, especialmente após o fim da Guerra Fria e com a intensificação da globalização, tem se acentuado a natureza pluralística da política internacional, em relação aos atores e seus papéis. Contudo, apesar da pluralidade e fragmentação de problemas e áreas, existem desafios globais que envolvem e afetam, diretamente ou indiretamente, todos os atores do sistema internacional contemporâneo. Nesse sentido, esses desafios precisam ser enfrentados de maneira coordenada e com amplitude mundial, sendo que os Estados têm construído e realizado arranjos intergovernamentais para lidar com áreas chaves por meio de políticas coordenadas, como é o caso de grupos como o G-20, G-7 e G-8 (Weiss; Wilkinson, 2018).

Não por acaso, foi com o objetivo de determinar uma série de preceitos e procedimentos entre os Estados para que a paz prevalecesse no mundo que o direito internacional foi idealizado e organizações internacionais como a Organização das Nações Unidas (ONU) foi fundada. Com isso, a previsibilidade de comportamentos e ações entre os atores estatais foi ampliada, bem como mecanismos de constrangimentos em casos de ações que rompem com as convenções estabelecidas. No entanto, o contexto internacional é marcado pela ausência de um robusto regime regulatório ou uma autoridade central no qual os Estados e os demais atores estão submetidos, caracterizando uma anarquia internacional. Esse contexto urge para a existência de mecanismos de governança que sejam adequados para lidar com distintos assuntos globais, em que os atores estatais e não estatais tenham capacidade de se relacionar e implementar medidas conjuntas de resolução para determinados assuntos. Nesse sentido, muitas vezes a governança é confundida com a construção de uma autoridade central ou uma espécie de governo.

No entanto, James N. Rosenau (1992) expressa que esse cenário mundial representa uma governança sem governo, constituída pela necessidade de resolver desafios e prevenir conflitos entre os atores do sistema internacional, de forma a obter os recursos necessários para a preservação e o bem-estar, visto que é preciso lidar com problemas em escala global, como poluição ambiental, tráfico de drogas, terrorismo e outras questões transnacionais que fazem parte da agenda global. Assim, a governança é definida pelo autor como um sistema de regras que só funciona e cumpre seu papel se é aceito pela maioria, sendo composta por atividades com objetivos orientados e compartilhados, bem como comportamentos intencionais pelos atores, se caracterizando como um fenômeno abrangente que engloba ao mesmo tempo instituições governamentais, informais e não governamentais (Rosenau, 1992).

Além disso, Rosenau (2004) aponta que, apesar de governo e governança terem como base de existência e funcionamento um sistema de regras no qual a ordem pode ser exercida, o governo é constituído por estruturas formais, como instituições destinadas a lidar com diversos assuntos e até confrontar a população que está sob sua tutela. Já a governança, o autor elucida que se trata de um sistema de regras que atua ou implementa funções sociais de variadas maneiras, em diferentes momentos e lugares, bem como é constituída por uma ampla gama de organizações.

> Governança, por outro lado, é um conceito mais amplo. Refere-se a qualquer coletividade, privada ou pública, que emprega mecanismos de direção informais e formais para fazer demandas, definir metas, emitir diretivas, seguir políticas e gerar conformidade (Rosenau, 2004, p. 31, tradução nossa)[2].

Dessa forma, Thomas G. Weiss e Rorden Wilkinson (2018), em uma tentativa de compreender como o mundo está organizado atualmente e, consequentemente, entender sobre as relações internacionais, expressam que a governança global, em uma perspectiva limitada e objetiva, tende a ser a combinação de diversos elementos como as atividades de organizações internacionais como a ONU; a preservação de projetos normativos e idealistas interessados num mundo melhor e as burocracias políticas que atuam em assuntos econômicos, ambientais e sociais. Nesse sentido, a governança global pode se referir a totalidade dos caminhos, formais ou informais, em que o mundo é governado, em que há o reconhecimento de problemas transnacionais que restringem a capacidade do Estado em resolvê-los (Weiss; Wilkinson, 2018).

A presença da governança é concebida nas funções que ela exerce em um sistema, em que dentre as diversas funções necessárias está a necessidade em prevenir conflitos entre os seus membros, em obter recursos para a preservação desse sistema, bem como determinar as políticas capazes de alcançar isso (Rosenau, 1992). Mas, para realizar as funções, é preciso que a governança tenha algum grau de autoridade e/ou legitimidade, em que os atores reconheçam mutuamente as políticas e diretrizes estabelecidas pelo sistema de regras construído. Rosenau (2004) define isso como esferas de autoridade que uma governança possui por meio do seu sistema de regras, expondo que essa esfera determina o alcance da capacidade desse sistema em gerar conformidade entre os atores no qual as diretrizes da governança são destinadas.

Assim, por envolver também mecanismos e instituições informais, a governança é um sistema de normas que é dependente de significados subjetivos, bem como de regulamentos

[2] Texto original: Governance, on the other hand, is a broader concept. It refers to any collectivity, private or public, that employs informal as well as formal steering mechanisms to make demands, frame goals, issue directives, pursue policies, and generate compliance.

constituídos formalmente, no qual só irá funcionar se for aceito pela maioria, ou ao menos pelos atores mais poderosos que são afetados pelo sistema (Rosenau, 1992). Por conseguinte, interpreta-se que, para ser efetiva, a governança precisa não apenas ser construída a partir da vontade dos atores envolvidos e afetados por ela, mas também precisa ser constantemente legitimada por esses mesmos atores ao passo que as diretrizes, políticas e normas são respeitadas e implementadas.

Dessa forma, a conformidade necessária para a existência da governança deriva da relação de cumprimento de um amplo pacote de hábitos, princípios, práticas e valores compartilhados pelos membros que a compõe. Com isso, há o aumento de uma complexa interdependência entre os membros e, por esses aspectos, a governança pode ser encontrada em diversos tipos de coletividades que não são consideradas governos (Rosenau, 2004). Nesse caso, a legitimidade de um sistema de regras implícito e explícito, que abrange a governança, ganha um caráter de extrema importância, visto que os processos de tomadas de decisão estão diretamente ligados com as expectativas, interesses e identidades que os atores possuem e, se não há congruência e uma aceitação comum sobre esse sistema, a governança será falha e as instituições e organizações que buscam implementá-las simplesmente serão descreditadas. A legitimidade pode ser entendida como "[...] a percepção ou suposição generalizada em que as ações de uma entidade são desejadas, próprias ou apropriadas dentro de um sistema de normas, valores, crenças e definições socialmente construído" (Suchman, 1995, p. 574, tradução nossa)[3].

"Em termos de governança, três elementos relacionados são centrais: poder, autoridade e legitimidade" (Ku, 2012, p. 159, tradução nossa)[4]. Por isso, Rosenau (1992) aponta para a essencial correlação entre governança e ordem, expondo que ambas não conseguem viver separadas. Isso porque os arranjos construídos pela governança florescem de atividades que são direcionadas propositalmente para manterem uma determinada ordem, mesmo que não haja uma autoridade central. "Não existe governança sem ordem e não existe ordem sem governança" (Rosenau, 1992, p. 8, tradução nossa)[5]. Sendo assim, governança e ordem são fenômenos interativos, já que a governança pode ser vista como atividades intencionais desenvolvidas para regulamentar arranjos de assuntos globais, conseguindo moldar a ordem global predominante (Rosenau, 1992).

---

[3] Texto original: [...] generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions.

[4] Texto original: In matters of governance, three related elements are central: power, authority, and legitimacy.

[5] Texto original: There can be no governance without order and there can be no order without governance.

Essa capacidade da governança em adequar uma ordem prevalecente está diretamente vinculada com a influência que o ambiente externo possui sobre o ambiente interno de um país, instituição ou organização, seja estatal ou não. Isso porque os arranjos criados a partir de um sistema de regras, princípios e condutas pode ter um efeito disseminador de práticas e políticas a serem seguidas em uma lógica semelhante na qual a política externa é capaz de instigar políticas domésticas. Tanto a própria conjuntura externa, quanto a política externa explícita de determinados atores, podem alterar o ambiente interno em que os atores domésticos tomam as suas decisões (Krasner; Weinstein, 2014). Nesse sentido, a governança em nível global sobre certo assunto ou problema, por representar a formação de um conjunto de padrões internacionais a serem cumpridos, pode ter potencial suficiente para adaptar a forma como os atores lidam com tal assunto ou problema, gerando por fim, uma conformidade.

Logicamente, compreende-se que essa influência só terá resultado e será efetiva se os atores internos, especialmente o Estado e as elites, estiverem propícios a aceitar as demandas externas. O próprio estabelecimento da governança só irá ocorrer se houver interesse e incentivo dos atores envolvidos na sua construção e manutenção. Nesse sentido, a demanda ou reivindicação pela governança ocorre quando sistemas de regras que ainda não existem são procurados (Rosenau, 2004), de forma a conduzir e/ou organizar as relações sociais e políticas desejadas. Rosenau (2004) aponta que são diversas as razões para a emergência de demandas pela governança, sendo a principal delas o fato de vivermos em um mundo bagunçado. Ou seja, que consequentemente urge por ordem.

Dessa forma, mesmo os Estados sendo os principais atores do sistema internacional, a governança global não se trata somente da relação entre os Estados, mas também das relações entre os processos de formação de políticas globais e a sua implementação em diferentes localidades, perpassando por todo o relacionamento entre instituições, grupos e mecanismos de diferentes setores e níveis (Weiss; Wilkinson, 2018). Isso ocorre porque já não vivemos em um mundo onde o poder, a autoridade e a legitimidade são provenientes de uma única e exclusiva fonte, o Estado. Principalmente após a segunda metade do século XX, emergiram no sistema internacional novos atores capazes de impactar as tomadas de decisões políticas, sendo responsáveis por uma certa difusão do poder, que entre a era Westfaliana e o século XIX emanava quase que exclusivamente da figura estatal.

A fundação de organizações internacionais são um exemplo disso. Pode-se considerar a formação do Conselho de Segurança da ONU como uma grande inovação na governança global (Murphy, 2018). Outro exemplo, dentre muitos, é a Organização Internacional do Trabalho (OIT), que estabeleceu padrões de atividades e práticas de proteção ao trabalho de maneira

internacional, apesar de que os maiores avanços na proteção aos trabalhadores ocorreram por meios de acordos entre as classes domésticas e os Estados preocupados no bem-estar social (Murphy, 2018). Nesse sentido, essas organizações foram capazes de construir, através da legitimidade que lhes foi dada pela comunidade internacional, procedimentos, preceitos e regulamentos sobre como o trabalho deveria ser respeitado, no caso da OIT, e como os países deveriam se portar no âmbito da segurança internacional, no caso do Conselho de Segurança.

Outro exemplo que envolve a ONU como uma importante ferramenta de governança é na questão dos direitos humanos universais, em que por meio de diversos tratados e convenções internacionais, os direitos humanos e os seus princípios são amplamente promovidos ao redor do mundo. Nesse sentido, mesmo que determinados atores, estatais e não estatais, desrespeitem ou simplesmente não sigam os preceitos e normas estabelecidas para a proteção dos direitos humanos, há toda uma conjuntura aprovada pela maioria dos países do sistema internacional em defender e valorizar os direitos humanos, criando uma conformidade de valores a partir de um sistema de normas. A construção dessa conformidade se deu com o tempo, os direitos humanos surgem no contexto pós Segunda Guerra Mundial, mas foi somente após a Guerra Fria que a transmissão internacional dos seus padrões passou a ocorrer de forma efetiva, emergindo como uma prioridade global na década de 1990 e se espalhando por diversos atores (Pegram, 2015).

Com isso, certos consensos e diretrizes sobre a promoção e defesa dos direitos humanos foram estabelecidos globalmente e, sob a tutela da ONU, determinadas condições foram propiciadas para que a implementação desses direitos se tornasse uma realidade. Nesse sentido, houve a proliferação de práticas que influenciaram no comportamento de Estados e atores não estatais em relação aos direitos humanos, mesmo que em muitos casos a convergência plena não é alcançada. Como coloca Tom Pegram (2015):

> Raramente exercida, mas mesmo assim abertamente coercitiva, dimensões de aplicação dos direitos humanos foram articuladas na doutrina "Responsabilidade de Proteger", e o Conselho de Segurança da ONU reconheceu as violações de direitos humanos como uma ameaça à segurança internacional. Neste caso, as regras são "duras" (Capítulo VII da Carta das Nações Unidas) e "diretas" (aplicação sobre o alvo pela autoridade executiva). Necessariamente, tal aplicação interestatal requer um alto grau de convergência de objetivo entre os membros do Conselho de Segurança – uma condição raramente encontrada. (Pegram, 2015, p. 6, tradução nossa)[6].

[6] Texto original: Rarely exercised, but nevertheless overtly coercive, dimensions of human rights enforcement have been articulated in the doctrine 'Responsability to Protect', and the UN Security Council has recognised human rights violations as a threat to international security. In this instance, the rules are 'hard' (Chapter VII of the UN Charter) and 'direct' (enforcement upon the target by the executive authority). Necessarily, such interstate enforcement requires a high degree of goal convergence among members of the Security Council – a condition that is rarely met

Dessa forma, é possível traçar um paralelo entre as ações e determinações da ONU, em casos como o de direitos humanos, com o raciocínio exposto por Rosenau (2004) sobre a necessidade de demandas para a construção da governança, em que diretrizes e políticas acabam sendo construídas após os atores relevantes enxergarem a importância de certo assunto ou área. No caso dos direitos humanos, essa necessidade foi vista pelos países vencedores da Segunda Guerra Mundial para que as atrocidades cometidas na guerra não se repetissem. Na verdade, as próprias organizações internacionais não fogem dessa lógica, visto que foram criadas a partir dos interesses das potências em aprimorar as suas capacidades para alcançar seus objetivos (Ku, 2012).

No entanto, a atmosfera política possibilitada por essas organizações fez com que outros atores não-governamentais pudessem ter maior acesso a uma plataforma em que suas agendas podiam ser promovidas em nível global. Consequentemente, a idealização e implementação de leis internacionais passaram a ser mais acessíveis e participativas, sendo que "essa combinação de representação universal e participação geral também forneceu a instituições internacionais como a ONU uma legitimidade e até mesmo autoridade única" (Ku, 2012, p. 167, tradução nossa)[7].

Importante salientar, entretanto, que as organizações internacionais não são sinônimas de governança global. Elas estão correlacionadas e uma é fator fundamental para a outra, mas as organizações internacionais são somente um elemento histórico do contingente que forma a governança global como um todo (Weiss; Wilkinson, 2014). Isso porque, durante um período do século XX, houve o processo de criação e aprimoramento dessas instituições, sendo que, junto com elas, foram também construídas práticas e procedimentos que agora realizam funções legítimas nos assuntos internacionais (Ku, 2012). Como colocado, a relação entre as organizações internacionais e a governança global é fundamental em vista da estrutura e da legitimidade formada dessas organizações, que se tornaram importantes atores no sistema internacional, sendo que atualmente já não é possível desvincular o sistema ONU da política internacional.

Dessa forma, essas organizações também acabam sendo responsáveis por promover a governança dos considerados bens públicos globais. Como aponta Inge Kaul *et al*. (1999), um bem público global é algo que não é excludente e é marcado pela não rivalidade em relação ao seu consumo, além de ser global em termos de acesso, tanto em relação aos países, quanto das

[7] Texto original: This combination of universal representation and general participation also provides international institutions like the UM with a legitimacy and even authority that is unique

populações e gerações futuras. Esse tipo de bem se diferencia dos bens privados já que estes não têm por característica serem universais, sua disponibilidade ser restrita, além do seu consumo gerar competição e exclusão por conta de sua escassez (Kaul *et al*., 1999). Neste trabalho, interpreta-se o ciberespaço como um bem público global, já que esse ambiente é transnacional e global por natureza e o seu acesso, uso e benefícios do seu uso não são exclusivos, isto é, todos ao redor do mundo podem usufruir desse espaço sem gerar privação e exclusividade, sendo que ele não se esgotará para as próximas gerações. Mas essa questão será tratada melhor mais adiante.

Por enquanto, é importante entender que, como esclarecem Inge Kaul e Ronald Mendoza (2003), é preciso de uma boa administração dos bens públicos para que toda uma sociedade ou população tenha uma vida digna e equilibrada, visto que lidar com problemas como a pobreza é uma tarefa mais difícil quando determinados bens não estão sob o domínio público e são de extrema importância, como água, alimentos de qualidade, segurança, saúde. Nesse sentido, os autores ampliam o conceito de bens públicos, expressando que eles também podem ser caracterizados como bens que o mercado falha ou tem grande dificuldade em precificar, em que a intervenção governamental é vista como necessária. Assim, os bens privados seriam de responsabilidade do mercado, já os bens públicos, do Estado, apesar de ambas entidades se confluírem na administração de bens em geral.

> O domínio público aparece como uma categoria residual, com Estados performando tarefas que o mercado não realiza. Mas como notado, "privado" não pode mais ser simplesmente equiparado a mercados, e "público" a Estados. Ambos contribuem, dentre outros, para os domínios público e privado. Ademais, as propriedades dos bens podem mudar de públicas para privadas e de privadas para públicas (Kaul; Mendoza, 2003, p. 80, tradução nossa)[8].

Nesse sentido, os aspectos do consumo e do acesso aos bens são aspectos que precisam ser levados em consideração quando se trata da diferenciação entre bens públicos e privados, sendo que a depender do caso, determinado bem pode ser visto como parcialmente público ou parcialmente privado. Assim, um bem totalmente público é aquele que está no domínio público por ser não exclusivo, por pertencer ao domínio público em vista de decisão política e ter acessibilidade para todos consumirem (Kaul; Mendoza, 2003). Projetando isso para o âmbito global, temos que certos bens são qualificados como públicos e globais quando abrangem as

[8] Texto original: The public domain appears as a residual category, with states performing tasks that markets cannot. But as noted, "private" can no longer simply be equated with markets, and "public" with states. Both contribute, among others, to the public and private domains. Moreover, the properties of goods can change from being public to private and from private to public

características supracitadas e beneficiam mais de um grupo de países, de forma a não discriminar nenhuma população, grupo ou geração (Kaul; Mendoza, 2003).

Alguns exemplos trazidos pelos autores como bens públicos globais são a atmosfera, a órbita geoestacionária, o espectro eletromagnético, os altos mares, etc. Por se tratarem de bens compartilhados no mundo todo, interpreta-se que a cooperação e a governança internacional possuem um papel fundamental no gerenciamento e a na sua administração, visto que por conta da amplitude desses bens, é preciso construir uma concordância entre os atores em relação a manutenção do acesso e do consumo como públicos. E não só isso, mas também em relação a quais políticas, boas práticas e diretrizes que devem ser seguidas pelos atores para que esses bens públicos globais sejam governados de forma a harmonizar os interesses envolvidos no seu acesso e utilização.

Dessa forma, ao levar em consideração a assimetria de poder e de recursos entre os Estados no sistema internacional, a construção de governança e a realização de acordos internacionais podem viabilizar uma melhor gestão e usufruto de bens públicos globais. Isso porque podem ter a capacidade de atuar como ferramentas de constrangimento ou, até certo ponto, limitação das ações ou imposições dos atores, já que estabelecem condições e políticas mútuas a serem seguidas. Nesse sentido, como afirmam Kaul e Mendoza (2003), não é uma surpresa que a sociedade civil e países não desenvolvidos estão cada vez mais ativos e preocupados em ter um espaço nas negociações internacionais em assuntos de relevância global. Assim, conforme os autores, a cooperação internacional acaba sendo vista como necessária para reduzir ineficiências e uma voz efetiva para todos ser uma realidade, como por exemplo, nos casos em que organizações internacionais são designadas para implementar padrões na promoção de certos bens como segurança internacional e estabilidade financeira internacional.

De modo geral, a criação de arranjos para lidar com bens públicos globais envolve o próprio reconhecimento desses bens como relevantes para os atores internacionais, sendo que diretamente ou indiretamente a sua administração incluirá questões como tomada de decisões, distribuição, acesso, boas práticas, entre outros. Pois, como expressam Kaul e Mendoza (2003):

> Esses problemas são ainda mais urgentes no nível internacional, particularmente quando um considera a cooperação internacional no suporte de bens públicos globais. As razões são que no nível internacional não há equivalência real para as instituições do Estado e que o público global tem mais interesses diversos e preferências do que qualquer público nacional. Além do mais, muitas pessoas – de fato países inteiros – frequentemente se encontram em situações "sem saída". Sob estas condições, um processo de tomada de decisão e produção para bens públicos globais que seja mais

> participativo e "de baixo para cima" é talvez o mais ideal (Kaul; Mendoza, 2003, p. 105, tradução nossa)[9].

A governança, portanto, por englobar elementos cooperativos, pode ser um fator pertinente na construção de disposições e ordenamentos para assuntos críticos como pode ser o caso de bens públicos globais. E ao retornarmos ao conceito de Rosenau (1992) sobre governança, tem-se que ela só será efetiva e terá capacidade para criar determinado ordenamento global se possuir e implementar três níveis de atividades: a ideacional, a comportamental e a política. A ideacional tem um caráter mais subjetivo e refere-se ao que as pessoas sentem e entendem, formando um sistema de crenças e valores compartilhados; a comportamental refere-se ao que as pessoas fazem regularmente, muitas vezes sem saber, para manter os arranjos globais predominantes; por fim o nível político é onde a governança ocorre e instituições orientadas por regras implementam as políticas inerentes nos níveis anteriores. Nesse sentido, interpreta-se que as organizações internacionais fazem parte do terceiro nível indicado por Rosenau (1992), em que as suas ações normativas e políticas compõem o que se entende por uma governança apta a gerar uma ordem global.

Isso significa que os três níveis expostos por Rosenau (1992) referem-se às diferentes camadas de ações e práticas que precisam ser implementadas para que a governança ocorra, desde à esfera micro, em relação ao sentimento e as concepções individuais que movem uma pessoa ou um grupo a tomar certa decisão ou ação; até a esfera macro, que diz respeito ao estabelecimento dos dispositivos políticos que carregam determinados valores que, diretamente ou indiretamente, estarão conectados com os sentimentos e concepções das pessoas. Sem essa conexão, não há a o estabelecimento de uma conformidade entre a determinação de políticas e o comportamento dos atores nos quais essas políticas são destinadas. Se voltarmos ao caso dos direitos humanos, podemos observar que o respeito e a proteção plena desses direitos perpassam justamente pela concepção de políticas e normas, pelo alinhamento dessas normas com as visões e princípios das pessoas e grupos e pelo comportamento social que essas pessoas e grupos terão a partir disso. Ou seja, sem uma identificação social que reverbere no comportamento do Estado em relação a certo assunto ou problema, a governança não será efetuada.

---

[9] Texto original: These issues are even more urgent at the international level, particularly when one considers international cooperation in support of global public goods. The reasons are that at the international level there is no real equivalente to the institution of the state and that the global public has far more diverse interests and preferences than any national public. Furthurmore, many people – indeed, entire countries – often find themselves in "no exit" situations. Under these conditions a decisionmaking and production process for global public goods that is more participatory and "bottom up" is perhaps most ideal.

Assim, valores comuns, percepções compartilhadas, padrões de comportamento como expressão de entendimentos ideológicos e o reconhecimento de instituições formais que moldam arranjos na política internacional são alguns dos exemplos de práticas e condutas que devem ser tomadas para que uma ordem seja criada ou mantida por meio da governança. Porém, quando se trata de bens públicos globais, essa conciliação e coordenação de políticas são de extrema importância, já que, como aponta Inge Kaul (2013), para melhor gerenciamento de um bem público global, é preciso que políticas sejam tomadas por muitos países em conjunto, se não todos. Isso se mostra crucial também nos casos dos bens públicos globais não naturais, ou seja, criados pelo ser humano, como é o caso da comunicação internacional, sistemas de transporte, bens de controle de doenças transmissíveis, estabilidade financeira, paz e segurança (Kaul, 2013).

Ocorre que as políticas para os bens públicos globais estão imbuídas de uma interdependência entre os países no que diz respeito a sua elaboração, já que as vontades e as preferências em relação aos bens são variadas (Kaul, 2013). Nesse sentido, um alinhamento por meio da cooperação acaba sendo um atrativo, ou uma proposição aceitável, entre os atores, visto que se há o desejo ou a vontade de se chegar em um ponto em comum, incentivos são necessários e a cooperação pode possibilitar isso ao servir como um caminho político para alcançar os próprios interesses nacionais dos países (Kaul, 2013). Contudo, é justamente a concordância das concepções, visões e interesses dos múltiplos atores envolvidos na governança de determinada área que pode consistir em um obstáculo a ser superado. Isso porque para que a governança seja promovida, é necessário que haja vontade entre esses atores em estruturar essa governança.

Nesse caso, até mesmo um entendimento e uma visão comum sobre a necessidade de existir um arranjo de governança sobre um assunto, problema ou área acaba sendo um fator inicial para que essa governança se torne realidade. Assim, compreender porque certa área necessita de uma governança global é um aspecto essencial. Seguindo o raciocínio de Weiss e Wilkinson (2018), para saber e entender se um determinado problema ou área se encaixa com a concepção de governança global, é preciso levantar algumas questões: essa área necessita de uma governança a nível global? Por acaso é uma área em que os seus problemas são de nível mundial e não podem ser resolvidos localmente?

No caso deste trabalho, acredita-se que o ciberespaço envolve o mundo todo e que somente soluções locais não parecem ser capazes de lidar com algo transnacional e com uma dimensão que não possui fronteiras físicas, como é o espaço cibernético. Na realidade, além dessas perguntas, no caso do espaço cibernético é interessante também perguntar por que ainda

não existe uma governança global para esse ambiente, de forma a regulamentá-lo, e quem se beneficia ou pode se beneficiar com essa ausência. Um grande desafio, que será desenvolvido melhor no capítulo 3, é conciliar aspectos como identidades, interesses, visões e concepções que os atores possuem sobre o espaço cibernético, especialmente os Estados, que muitas vezes divergem em suas posições no que se refere ao uso, proteção, estrutura e gerenciamento do ciberespaço. Um elemento que pode ser questionado e ser motivo de divergência entre os países em relação à governança do ciberespaço é o princípio da soberania, que acaba sendo desafiado pelo domínio cibernético em relação à sua concepção tradicional nas relações internacionais. Dessa forma, é importante compreendermos bem a importância desse princípio para a política internacional e como ele pode ser afetado pelo fenômeno da governança global e do ciberespaço.

2.2 O PRINCÍPIO DA SOBERANIA SOB O PRISMA DA GOVERNANÇA GLOBAL

A formação do sistema internacional como concebemos hoje perpassa pela constituição dos seus atores formadores e as suas relações. Nesse sentido, ao considerarmos o Estado nacional como o principal ator desse sistema, é preciso olhar para os aspectos que o originou, compõem e caracterizam. Isso porque esses aspectos foram e são determinantes para a maneira como os Estados interagem e se comportam no sistema internacional. Um dos mais relevantes aspectos, apesar de não ser absoluto, é a soberania. Na verdade, a literatura tradicional das Relações Internacionais (RIs) abraça o princípio da soberania e a sua efetividade como a primeira regra constitutiva da organização do sistema internacional, em que o elemento definidor desse sistema é a divisão do mundo em Estados soberanos (Barkin; Cronin, 1994).

Essa divisão, pelo menos a partir da visão tradicional das RIs, ocorreu a partir da assinatura e implementação dos tratados de Paz de Westfália (1648), que encerraram a Guerra dos Trinta Anos na Europa e definiram a organização institucional e também territorial dos envolvidos. Nesse sentido, os acordos de Westfália são tidos como um ponto de referência chave na construção do moderno Estado nação e do direito internacional clássico, visto que os acordos fortaleceram e promoveram a autonomia de cada um dos territórios dentro de uma complexa estrutura política (Sánchez, 2015). Isso porque, dentre as determinações, houve o reconhecimento de uma quase-soberania das potências da época, capaz de garantir os instrumentos necessários para que pudessem se consolidar, a partir daquele momento, como Estados (pré-) modernos, tendo o direito de constituírem tropas, firmar alianças com outros Estados e ter autonomia política interna (Mainka, 2021).

Como coloca Stéphane Beaulac (2004), os dispositivos dos tratados possuíam três principais eixos: religião, território e a possibilidade de firmar obrigações internacionais. Sendo assim, os acordos de paz deram origem ao princípio da não-intervenção e, mais do que isso, possibilitaram uma acomodação fronteiriça entre os Estados envolvidos, a partir do conluio de interesses das potências em respeitar os limites territoriais (Junior, 2017). Como consequência, nasce o chamado sistema Westfaliano, formado pelos Estados modernos fundamentados no reconhecimento da soberania territorial, da autonomia nas políticas domésticas e do princípio de igualdade entre os Estados.

Essa ordem Westfaliana foi comprometida e corrompida ao longo da história, com o desrespeito aos seus princípios por parte dos entes estatais, muito em vista da busca dos Estados em alcançar e satisfazer seus interesses e objetivos, consolidando uma assimetria de poder no sistema internacional (Jesus, 2010). Mas isso não significa que o reconhecimento da soberania nacional não promoveu certa segurança e estabilidade para os Estados modernos, ou ao menos um arcabouço institucional e jurídico no qual esses atores pudessem tratar sobre regras no âmbito internacional e suas condutas no jogo de poder interestatal.

> A Paz de Westfália, que acabou com a Guerra dos Trinta Anos em 1648 é geralmente entendida como um momento crítico no desenvolvimento do moderno sistema internacional composto por Estados soberanos cada um com autoridade exclusiva dentro dos seus próprios limites geográficos. A soberania Westfaliana, baseada no princípio da autonomia territorial, reconhecimento mútuo e controle, oferece uma simples, atraente e elegante imagem. Ela ordena as mentes dos formuladores de políticas (Krasner, 2001, p. 17, tradução nossa)[10].

Nesse sentido, ao construir no imaginário dos governantes uma diretriz ou um comando a ser seguido e respeitado, o princípio da soberania acaba por conduzir, mesmo que indiretamente, as ações e reações dos Estados dentro do sistema internacional. Assim, é possível considerar que o chamado sistema Westfaliano se configurou num conjunto de postulados envolvendo normas no ambiente internacional, que garantiam ao Estado uma posição de ator singular (Bragança, 2019). Isso porque a própria formação do sistema dos Estados nacionais repousa no mútuo reconhecimento de que cada um representa uma sociedade específica e um domínio jurídico, englobando todos os elementos diplomáticos, normativos e outras instituições

[10] [Texto original]: The Peace of Westphalia, which ended the Thirty Years' War in 1648, is generally understood as a critical moment in the development of the modern international system composed of sovereign states each with exclusive authority within its own geographic boundaries. The Westphalian sovereign state model, based on the principles of autonomy, territory, mutual recognition and control, offers a simple, arresting, and elegant image. It orders the minds of policymakers.

que fornecem a possibilidade de comunicação e interação entre os Estados e funcionam como requisitos para a sua participação como membro do sistema (Barkin, 1994).

E não apenas isso, mas do ponto de vista da estabilidade internacional, as normas e a diplomacia podem favorecer para uma estabilidade entre os Estados contra uma imprevisibilidade em caso da ausência desses fatores (Barkin, 1994). Pode-se entender, portanto, que a própria compreensão dos Estados em relação a sua soberania, isto é, como reconhecem e interpretam os aspectos constitutivos desse princípio tanto para si como para o outro, pode afetar, mesmo que indiretamente, na maneira como irão atuar e se serão constrangidos ou habilitados a tomar determinadas atitudes nas relações internacionais. Pois, essa compreensão, caso seja congruente entre os atores estatais, leva à legitimidade de como se portar internacionalmente e interagir entre si. Essa visão assumida aqui, que vai ao encontro de um pensamento construtivista das relações internacionais, enxerga que a soberania só consegue existir porque é acreditada e fundamentada por todos os Estados.

Como coloca Thomas J. Biersteker e Cynthia Weber (1996), a soberania é um conceito inerentemente social, em que a sua reivindicação pelos Estados constrói um ambiente social no qual eles podem interagir como uma sociedade internacional de Estados, ao mesmo tempo em que o reconhecimento mútuo dessa reivindicação é um fator crucial para própria construção do Estado em si. Isso significa que os limites territoriais só existem porque lhes foram dados significados políticos. Para isso, uma entidade política com autoridade suficiente para exercer domínio e controle sobre o território dentro desses limites é um elemento constitutivo para legitimar a existência desses limites. Assim, a soberania pode ser interpretada como um poder político reconhecido externamente que tem como direito o exercício da autoridade sobre os seus assuntos (Biersteker; Weber, 1996).

Além disso, essa perspectiva permite interpretar que a realidade física não é o elemento primordial e fundador da soberania, e sim o âmbito normativo e legal que dimensiona a soberania a partir do reconhecimento dos atores do sistema internacional, que apenas se utilizam do território geográfico para construir os seus limites e concepção de autoridade. Nesse sentido, para que um Estado tenha a sua soberania reconhecida, é necessária uma base territorial, em que seus limites são socialmente construídos em determinado momento histórico (Biersteker; Weber, 1996). Olhando somente para o âmbito interno, a construção da identidade do Estado também é um importante fator na constituição da soberania, visto que a maneira como o Estado constrói e estabelece os seus valores normativos e reivindica a sua legitimidade política resulta em como esse Estado se enxerga, como é visto pelos outros e como a sua população e instituições atestam a sua autoridade.

Sendo assim, como coloca Winston P. Nagan e Craig Hammer (2004), no contexto social, político e dos processos constitutivos, a soberania é o reflexo da atribuição de competências no processo de tomada de decisão em relação às instituições de governo, em que essas instituições precisam da autorização e do reconhecimento social e político para tomarem suas decisões. Ou seja, a soberania reflete a legitimidade e a autoridade do governo nacional em ter as suas instituições consideradas competentes para tratar dos assuntos internos e fazer valer a ordem legal e normativa estabelecida, sem interferência externa.

Nesse sentido, a relação entre o ambiente externo e interno no que tange à construção e validação da soberania também é um fator constitutivo desse princípio, em que a concepção das identidades internas e externas de um Estado são interdependentes para o reconhecimento soberano.

> As definições de Estado e soberania são assim mutuamente dependentes. Um Estado é o ente político que reivindica a autoridade no seu território. Isso, no entanto, não basta. É preciso ainda que os demais atores o reconheçam enquanto ator no sistema internacional. O mútuo reconhecimento auxilia na definição de Estado soberano e também na definição do sistema internacional (Scherma, 2012, p. 123).

Importante ressaltar, entretanto, que esse princípio de igualdade entre os Estados, surgida na era pós-Westfália, não foi respeitado na prática por muito tempo e carregava em si um caráter eurocentrista e ocidental em relação à própria concepção de Estado moderno. Como consequência, por séculos as grandes potências do sistema internacional agiram ativamente para intervir em nações periféricas para atingirem seus interesses econômicos e políticos, estabelecendo, muitas vezes por meio da violência, ações de ingerência interna nessas nações. O colonialismo talvez seja o maior exemplo de intervencionismo realizado na era pós-Westfália no que tange ao desrespeito à soberania nacional e à autodeterminação dos povos. Nesse processo, os Estados europeus integraram, por meio da conquista coercitiva, diversos territórios africanos, asiáticos e latino-americanos e impuseram as suas regras coloniais (Rubin, 2005). A disputa colonial entre as potências gerou até mesmo a necessidade de regular a competição, sendo a Conferência de Berlim (1884), responsável por estabelecer uma divisão estável das colônias na África aos países europeus, um exemplo disso (Rubin, 2005).

A consequência tanto do período colonial quanto do imperialismo, perpetrados especialmente entre os séculos XVII e XX, foi um sistema mundial de desigualdade entre os Estados, caracterizado por um processo histórico de exploração social e econômica de subjugação de nações e raças, sendo que essa subjugação foi fator determinante para a construção e estruturação das relações políticas, econômicas, sociais e securitárias entre os

Estados nos dias de hoje. Pois, como coloca Walter Mignolo (2012), o surgimento do Estado moderno ocorre no âmbito do "sistema-mundo moderno/colonial", em que ele não deve ser visto como uma entidade separada do sistema de relações mundiais, mas sim como um mecanismo ativo no próprio interior desse sistema. Isso significa que a fundação do Estado moderno, sob a égide da soberania, teve por característica a promoção da assimetria de poder no sistema internacional.

Assim, o período pós-colonial das relações internacionais, iniciado no século XX até os dias de hoje, carrega esses elementos de desigualdade entre os países devido ao processo histórico ocorrido no mundo. O direito internacional contemporâneo, portanto, constituído especialmente após a Segunda Guerra Mundial, busca trazer em seus dispositivos a valorização da igualdade entre as nações e povos, em que as relações interestatais se fundamentam a partir do pleno respeito ao princípio da soberania. Como expressa a Carta das Nações Unidas, em seu artigo 2º, os Estados membros da ONU devem se basear na igualdade soberana e respeitar a integridade territorial de todo Estado (Organização das Nações Unidas, 1945). Isso significa que o direito internacional prevê o princípio da igualdade de direitos entre as nações e da autodeterminação dos povos como mecanismos de promoção da paz e da segurança internacional, reconhecendo, portanto, a soberania como um preceito para a harmonia do sistema internacional.

Por conseguinte, aspectos que podem desafiar a soberania poderiam desafiar a própria ordem desse sistema. Contudo, quando pensamos em arranjos transnacionais e também em um mecanismo de governança global, pensamos em situações que ultrapassam os limites territoriais que compõe os países, pois seria algo seguido em conformidade por todos, ou quase todos, que estivessem inseridos nesse contexto. Nesse caso, é preciso compreender como o princípio da soberania se relaciona com a constituição de uma governança global. Isso porque é possível interpretar as soberanias dos Estados como uma possibilidade de liberdade de ação e comportamento dentro do seu território nacional. Assim, o constrangimento de um ente externo por meio de ferramentas de governança global poderia ser interpretado como um desrespeito a essa liberdade soberana.

Mas o contexto do mundo atual, com a interação dos diversos atores que hoje também compõem o sistema internacional para além dos atores estatais, faz com que a concepção tradicional de liberdade total de um Estado em relação aos seus assuntos internos não seja condizente com a realidade. Os diversos corpos públicos, privados e público-privados de governança global e as realidades econômicas e sociais de hoje reduzem o espaço de controle regulatório dos governos nacionais, limitando, em certa medida, os seus poderes (Benvenisti,

2016). Consequentemente, há um cenário de uma complexa rede de órgãos e atores que precisam dialogar e negociar para acomodar os seus interesses, de modo que esses interesses permaneçam eficazes (Benvenisti, 2016). Nesse sentido, interpreta-se que a interdependência construída evita certo isolacionismo e exige que relações ativas sejam feitas e mantidas para que objetivos particulares ou compartilhados sejam atingidos.

A necessidade que hoje existe para se resolver problemas regionais e globais fez com que as regulamentações internacionais se intensificassem. Ou seja, a emergência de problemas comuns em nível internacional, como terrorismo, tráfico humano, mudança climática, entre outros, fez com que respostas coletivas fossem exigidas, em que a governança global passou a ser cada vez mais demandada (Benvenisti, 2016). No entanto, isso não significa que a soberania tenha sido diluída, ou que os Estados nacionais perderam sua capacidade de controle e perderam sua importância como principal ator no sistema internacional. Na verdade, as instituições supranacionais são um elemento que possibilitam os Estados a exercerem a sua soberania e a autodeterminação dos povos (Ronzoni 2012).

Como expõe Miriam Ronzoni (2012), com base no conceito de soberania negativa e soberania positiva de Robert Jackson (1990), os Estados precisam de instituições globais para manter as suas soberanias positivas. A soberania positiva diz respeito à capacidade do Estado em determinar as suas condições internas, tendo recursos suficientes para decidir as políticas que deseja implementar com sucesso na dimensão doméstica (Ronzoni, 2012). Já a soberania negativa refere-se à imunidade que um Estado possui em não sofrer interferências ou intervenções externas, ou seja, ser livre de ingerências de outros atores, constituindo o conceito jurídico central do direito internacional contemporâneo (Ronzoni, 2012). Nesse sentido, a soberania positiva indica a faculdade estatal em providenciar as políticas fundamentais para a sua população viver dignamente no seu território.

Isso significa que um Estado que não é capaz de fornecer condições essenciais como segurança e bem-estar à sua população não é soberano positivamente, apesar de ter a sua soberania negativa reconhecida. Com isso, interpreta-se que a soberania positiva é o alicerce para que o Estado tenha controle efetivo sobre o seu território, visto que esse aspecto está diretamente ligado aos recursos e habilidades disponíveis pelo ente estatal. Além disso, a soberania positiva possibilita até mesmo que a soberania negativa seja garantida, já que é a partir desses recursos disponíveis que o Estado pode ou não ser capaz de se defender e se impor contra intervenções, sendo por fim tratado como igual perante seus semelhantes (Ronzoni, 2012).

Consequentemente, aos olharmos hoje para os considerados Estados fracos, podemos dizer que lhes falta, em alguma medida, a soberania positiva, mesmo que o direito internacional reconheça a sua soberania negativa como um Estado nação no sistema internacional, que deve ter o seu limite territorial e a autodeterminação dos povos respeitados pelos demais atores. Nesse caso, a própria liberdade dos Estados não soberanos positivamente é colocada em xeque, pois os seus governos e instituições podem não ter meios e instrumentos suficientes para agir como deseja e implementar as políticas de interesse. Ademais, pode se considerar que a vulnerabilidade desses atores é alta, e, por conseguinte, a existência de uma dependência externa em termos econômicos e políticos pode fazer com que sejam constrangidos a implementar ações de interesse de terceiros que não vão diretamente ao encontro dos interesses nacionais.

Dessa forma, Ronzoni (2012) aponta que instituições de governança global podem atuar tanto para prejudicar quanto beneficiar a soberania positiva dos países, sendo fundamentais na existência dessa soberania em vista da interconexão que o mundo globalizado se encontra atualmente. Segundo a autora, essa influência sobre a soberania positiva pode ocorrer tanto por meio da imposição de regras e normas internacionais, quanto pela ausência delas. Isso porque a existência de instituições globais pode limitar a capacidade dos Estados, como por exemplo, ao estabelecer requisitos e condições para oferecer ajuda externa, como a condição de abertura de mercados para empréstimos financeiros e a imposição de uma agenda neoliberal que não necessariamente irá beneficiar o Estado que está tomando o empréstimo.

Por outro lado, os mecanismos de governança global podem auxiliar os Estados ao criarem regras e diretrizes que atenuem as desigualdades interestatais, de forma a criar condições justas para que esses atores exerçam suas políticas de maneira autônoma (Ronzoni, 2012). Isso porque a ausência dessas regras pode criar um cenário onde os mais fracos acabam sendo subjugados pelos mais fortes.

> Em outras palavras: as formas problemáticas de poder estão sendo exercidas para além das fronteiras, na ausência de qualquer caminho institucional apropriado para vincular e controlar elas. Isso acontece tanto de maneira internacional quanto transnacional. Internacionalmente, Estados poderosos são frequentemente capazes de influenciar políticas domésticas dos mais fracos em prol dos seus próprios interesses, limitando severamente, portanto, as suas soberanias positivas. Transnacionalmente, diversos atores não-estatais poderosos são capazes de atuar na arena global de forma que favorece seus próprios interesses e enfraquece severamente a capacidade dos Estados de resistir a eles. (Ronzoni, 2012, p. 584, tradução nossa)[11].

[11] Texto original: In other words: problematic forms of power are being exercised across borders, in the absence of any appropriate institutional way to bind and control them. This happens both in an international and in a transnational manner. Internationally, powerful states are often capable of influencing the domestic policies of

Sendo assim, a regulamentação internacional, por meio da construção de uma governança, pode atuar como um instrumento moderador ou regulador das relações entre Estados. Desse modo, um ator estatal de maior proeminência, ao seguir as regras determinadas internacionalmente, pode ter menos capacidade de coagir atores menos expressivos em prol dos seus interesses. Com isso, as assimetrias de poder no sistema internacional podem ser confrontadas ou até mesmo mitigadas, sendo que uma maior pluralidade de Estados teria a oportunidade de elaborar e implementar as suas políticas sem sofrer as influências externas de atores mais relevantes no cenário global. Consequentemente, a soberania positiva de uma maior parcela dos Estados poderia ser promovida e/ou garantida, aumentando a autonomia dos governos nacionais no estabelecimento e execução das suas agendas domésticas.

Essas visões e meios de relacionar a soberania com a governança apenas demonstra como a humanidade foi se organizando ao passar do tempo no que tange à política internacional e a própria estrutura social em termos mundiais. Como comentado anteriormente, o mundo não é o mesmo do período medieval em que o absolutismo era o regime dominante, nem mesmo do período de formação dos Estados nacionais modernos. A globalização e o multilateralismo, bem como o avanço tecnológico e a intensificação da comunicação e informações, desempenharam um papel catalisador na organização política da humanidade. Nessas transformações, inclui-se a mudança na forma de acumulação de capital, na forma de se fazer guerras, no estabelecimento das políticas estratégicas de segurança, na organização cultural da sociedade global, entre outros fatores políticos e socioeconômicos que foram moldando a construção de sistemas de governança no mundo.

Mas o avanço das instituições internacionais reafirma o direito internacional e o multilateralismo de modo que o sistema estado-cêntrico continua a ser reproduzido em um sistema de governança global (Reus-Smit, 1998). Isso significa que um sistema de governança global pode ter a capacidade de construir constrangimentos no comportamento dos Estados, mas não é capaz de extinguir a sua autoridade soberana, podendo até mesmo assegurá-la ao possibilitar cenários que coíbam abusos nas relações interestatais. Ao fim e ao cabo, o modo organizacional que a humanidade estrutura as suas relações sociais dependem dos fatores de reconhecimento, identidade e interesse que possui em manter o modo de vida que deseja. As transições ocorridas durante a história estão ligadas com a demandas econômicas, políticas e

---

weaker ones to their own interests, thus severely limiting their positive sovereignty. Transnationally, several kinds of powerful non-state actors are capable of acting in the global área in ways that favour their own interest and severely undermine the capacity of states to resist them.

culturais nas quais os seres humanos foram enfrentando para garantir a sua sobrevivência e melhores condições de vida.

Interpreta-se que a governança funciona como uma ferramenta que pode propiciar uma melhor organização dessas relações e melhores condições. Pois, como coloca a Comissão de Governança Global das Nações Unidas, fundada em 1994, os problemas e processos estão demandando melhores gestões de sobrevivência, melhores formas de compartilhamento e de viver em comunidade com a vizinhança global (Organização das Nações Unidas, 1995). Consequentemente, a construção dessas melhores condições precisa ser conjunta, sendo aceita pela maioria dos Estados na condução das suas práticas e, de certa forma, cedendo e/ou reconhecendo a autoridade das instâncias de governança em determinar diretrizes e políticas para todos. Nesse sentido, os Estados, apesar de serem soberanos, não são livres para unilateralmente fazerem o que quiserem (Organização das Nações Unidas, 1995).

O compartilhamento de valores e práticas, portanto, é um dos fatores responsáveis pela viabilidade da governança, promovendo um ordenamento, como visto anteriormente a partir da perspectiva teórica de Rosenau (1992). Pois, como aponta Christian Reus-Smit (1998):

> As instituições básicas de governança e as principais organizações da governança ficam em uma relação constitutiva mútua, com instituições primárias definindo as identidades e o âmbito da ação legítima das organizações e as organizações reproduzindo e transformando instituições através das suas práticas (Reus-Smit, 1998, p. 6, tradução nossa)[12].

Dessa forma, sendo o reconhecimento e a definição de identidades aspectos cruciais na construção tanto de um modelo organizacional para reger as relações entre os Estados, quanto para a própria valorização da soberania, temos que as concepções que esses atores possuem sobre si e sobre o mundo são relevantes para designar a forma em que a organização das suas relações irá se dar. De modo geral, a lógica aqui exposta segue um viés construtivista das relações internacionais. Conforme Alexander Wendt (1992), os Estados têm os seus cálculos impactados pela distribuição de poder no sistema internacional, sendo que a forma como esses cálculos ocorrem dependem das expectativas que possuem, assim como das concepções que constituem acerca dos outros e de si. Ao elucidar que a "anarquia é o que os Estados fazem dela" (Wendt, 1992, p. 395), o autor, juntamente com o movimento

[12] Texto original: The basic institutions of governance and the principal organizations of governance stand in a mutually constitutive relationship, with primary institutions defining the identities and realm of legitimate action of organizations and organizations reproducing and transforming institutions through their practices

construtivista, enxerga que o processo de formação de identidades e de interesses são endógenas às interações entre os atores, não sendo dado pela estrutura em que esses atores estão inseridos.

"Os atores não têm um "portfólio" de interesses que carregam independentemente do contexto social; contrariamente, eles definem seus interesses no processo de definição das situações" (Wendt, 1992, p. 398). A análise construtivista leva em consideração que o Estado é o produto de uma sociedade doméstica, que projeta a sua interação no processo constitutivo da sociedade internacional. Assim, a ação na política internacional depende da atribuição que os Estados dão para determinada situação, sendo essa atribuição determinante para o conflito ou à cooperação; ou seja, para o consenso ou para a divergência. Nesse caso, o reconhecimento por parte de todos sobre o direito ao controle territorial e a legitimidade do monopólio do uso da força é o que faz com que a soberania exista. Sem tal reconhecimento mútuo, não seria possível existir Estados soberanos. Assim, a soberania pode ser definida como "[...] não apenas a liberdade de ação relativa à sociedade, ou a autonomia do Estado, mas sendo reconhecida pela sociedade como possuidora de certos poderes, tendo autoridade" (Wendt, 1999, p. 206-207, tradução nossa)[13].

Nesse sentido, a autoridade da soberania é conferida por todos os atores do sistema internacional e, sendo assim, a autoridade da governança segue a mesma lógica. Assim, conforme o contexto exposto, não necessariamente a atribuição de autoridade para órgãos e instituições de governança faz com que se esteja retirando a autoridade da soberania dos Estados. O reconhecimento de um não anula o de outro. Ao contrário disso, os instrumentos de governança, por meio de regulamentações, podem favorecer para a proteção da soberania estatal, especialmente dos Estados com maiores debilidades em relação ao seu ordenamento interno e maiores vulnerabilidades externas.

A globalização e a interdependência entre os atores fazem com que algumas salvaguardas econômicas, políticas e sociais exijam instituições que atuem para além do Estado nacional. Assim, uma governança legítima, por meio de instituições internacionais, possibilita atuações políticas frente a processos que ultrapassam os limites nacionais, podendo, portanto, fazer parte da solução de problemas considerados globais (Innerarity, 2012). Como consequência, a soberania acaba sendo questionada por não demonstrar ser capaz de lidar com os novos problemas que emergiram nos últimos anos de modo unilateral. Em verdade, para lidar de maneira responsável com os bens comuns, os Estados se veem compelidos, ou por necessidade, ou por pressão, a jogar o jogo da interdependência (Innerarity, 2012).

[13] Texto original: [...] is not about *de facto* freedom of action relative to Society, or "state autonomy", but about being recognized by Society as having certain powers, as having authority.

Sendo assim, se a abolição da soberania se mostra irreal, a sua defesa absoluta e irrestrita também se mostra ser. As relações internacionais não se baseiam somente nas confrontações de entidade soberanas na busca pela proteção dos interesses próprios, mas também em arranjos de princípios e jurisdições que reforçam a integração internacional e constroem alicerces para a disseminação de padrões comuns que podem ter a capacidade de aprimorar as relações sociais em nível global.

A governança, ao pressupor a pluralidade de atores e instituições para a sua legitimidade e funcionamento, acaba representando uma perspectiva de descentralização de poder na qual a soberania está baseada. Nesse sentido, os arranjos construídos pela governança podem influenciar na forma como os Estados interagem. Isso porque a governança envolve variadas dimensões, como a capacidade de produzir resultados frente problemas comuns; envolver participação ampliadas nos processos decisórios; necessitar de consenso para o estabelecimento de ações e requerer a existência de um conjunto de normas e regras (Gonçalves, 2014).

As mudanças nas formas de organização social e política em nível internacional possuem ligação com a própria mudança e reestruturação do capitalismo nas últimas décadas, em que a descentralização, desregulamentação, maior flexibilidade, aumento da concorrência econômica global e diferentes modos de intervenção estatal ganharam proeminência (Teixeira; Sabo, 2016). Um dos fenômenos que permitiu e/ou fomentou essas mudanças organizacionais nas estruturas socioeconômicas e políticas da sociedade e da economia global foi o avanço tecnológico dos sistemas de comunicação. As inovações tecnológicas possuem a capacidade de transformar os modos de produção e os modos de vida de uma sociedade. E, sendo assim, a aceleração de técnicas de comunicação e informação afetam diretamente as interações sociais, de forma a propiciar diferentes dimensões para as atividades humanas e como os processos e procedimentos dessas atividades são realizados.

Uma das inovações que provocou uma transformação nas redes de comunicação e na transmissão de informações foi o desenvolvimento do espaço cibernético, especialmente em vista da sua principal ferramenta: a Internet. Mas, ao mesmo tempo, o ciberespaço criou certos desafios para os Estados nacionais e para as relações internacionais, sendo um desses desafios o questionamento da soberania nacional. “O ciberespaço tem a capacidade de desafiar a soberania nacional, visto que pode questionar a habilidade do Estado em regular os movimentos e os fluxos de informações dentro de suas fronteiras nacionais” (Khanna, 2018, p. 140, tradução

nossa)[14]. Isso ocorre em vista do espaço cibernético englobar atividades, atores e ambientes transnacionais, que ultrapassam a lógica original do território Westfaliano e acaba por produzir relações integradas (Israel, 2020).

Dessa forma, o ciberespaço além de questionar a visão tradicional de soberania, também contesta a capacidade do Estado em implementar e possuir uma soberania no ciberespaço, em termos de controle e autoridade sobre os processos e fluxos que ocorrem nesse ambiente. Uma hipotética implementação de soberania no ciberespaço faria com que os Estados tivessem que mostrar respeito mútuo pelo ciberespaço de cada um, em que a invasão ou a interferência em assuntos e atividades de gerenciamento nesse domínio corresponderia a uma violação dessa soberania (Fang, 2018). Muitos países, especialmente países autocráticos, têm estabelecidos capacidades para um sofisticado controle de informações, em estratégias que tem como propósito implementar uma certa "territorialização" do ciberespaço (Masoumifar, 2022).

No entanto, a soberania estatal sobre o espaço cibernético da mesma forma em que é estabelecida para os domínios tradicionais pode ser irreal, sendo que o paradoxo de territorializar o ciberespaço evidencia uma certa tensão entre o sistema político internacional que se baseou e se baseia nos territórios nacionais e um sistema social e econômico cada vez mais global (Masoumifar, 2022). Como consequência, de certa forma o ciberespaço está contribuindo para influenciar uma mudança na visão das autoridades políticas sobre o mundo e as relações existentes entre os atores no sistema internacional. Isso porque os Estados vão ter a tendência de proteger o seu ciberespaço e suas infraestruturas de perigos externos, mas ainda há um controverso debate em relação a estender a soberania tradicional para o espaço cibernético (Yeli, 2017).

O debate não diz respeito apenas ao que pode ou não ser controlado na prática em uma eventual soberania no ciberespaço, mas principalmente em relação às áreas desse domínio que a soberania pode cobrir, visto que o ciberespaço envolve diferentes dimensões e as visões dos Estados podem diferir sobre quais áreas podem ou devem ser soberanas ou não (Yeli, 2017). Isso tem ligação com uma concepção excepcionalista do ciberespaço, que sugere que o reino digital é qualitativamente distinto do reino analógico, ou territorial, no qual o espaço virtual precisa ter um tratamento diferenciado em vista das inovações que ele proporciona (Pohle, 2020). Esse olhar sobre o domínio cibernético envolve aspectos como a questão da soberania e as formas de implementá-la ao ciberespaço.

[14] Texto original: Cyberspace is also capable of challenging state sovereignty, since it can question the state's ability to regulate movement across borders.

Nesse sentido, entender o ciberespaço a partir do entendimento do mundo físico e aplicar as mesmas lógicas pode não ser o raciocínio ideal. Ao mesmo tempo, o espaço cibernético está cada vez mais interligado e limitado pela complexidade da política territorial, sendo visto como um ambiente de disputa e de poder pelos Estados (Mainwaring, 2020). Assim, interpreta-se que o princípio da soberania pode ser tido como universal em relação aos domínios de poder, mas a sua aplicação ao domínio cibernético tem que estar ligada às particularidades únicas do ciberespaço, sendo que os Estados devem determinar essa aplicação a partir da construção de regras e de comportamentos práticos (Schmitt; Vihul, 2017). Ocorre que o contexto internacional é de ausência de diretrizes comuns reconhecidas pelos atores internacionais quanto a isso.

Entende-se que a existência de dispositivos e normas específicos para tratar sobre a soberania no âmbito do ciberespaço poderia facilitar a identificação e interpretação dos atores sobre questões que envolvem operações cibernéticas, abrangendo ou não o uso da força ou manifestações coercivas, de modo a discernir sobre a possibilidade de violação do espaço cibernético. Não sem fundamento que no ano de 2017, no lançamento do Manual de Tallinn 2.0 na Europa, o Ministro das Relações Exteriores dos Países Baixos, Bert Koenders, expressou que a ocorrência de operações cibernéticas contra instituições, entidades políticas e indivíduos evidencia a necessidade e importância de princípios internacionais legais sobre soberania e não intervenção em relação ao ciberespaço (Schmitt, Vihul, 2017). As controvérsias e a falta de definição no que tange ao reconhecimento de um ciberespaço soberano diz muito sobre a incapacidade ou falta de vontade da comunidade internacional em construir um arcabouço conceitual e jurídico sobre esse espaço e os efeitos que ele produz nas diversas áreas políticas, sociais, econômicas e securitárias.

É claro que o dilema discutido aqui refere-se à dimensão não física desse espaço, ou seja, ao ambiente virtual e informacional no qual ele proporciona, e não à dimensão física dos sistemas e infraestruturas necessárias para que esse espaço exista. Dessa forma, é preciso compreender as características do ciberespaço, bem como as interpretações e concepções existentes sobre ele, abrangendo as suas peculiaridades, definições, indefinições e os impactos da sua utilização para as relações internacionais. Assim, no próximo capítulo, o ciberespaço será tratado de forma mais aprofundada, com a análise das suas complexidades a partir de um viés construtivista das relações internacionais e da perspectiva da segurança ontológica para a segurança internacional.

2.3 CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo, foi abordado uma revisão teórica sobre os aspectos da governança e da soberania nas relações internacionais, trazendo elementos de correlação desses aspectos com o espaço cibernético. Dessa forma, o capítulo serviu não apenas para introduzir e contextualizar o assunto, mas também para definir o entendimento de que a governança no sistema internacional atua de modo a construir princípios e normas que podem ter a capacidade de condicionar condutas e comportamentos dos atores, caso os atores reconheçam e concordem que seguir essas condutas é uma opção melhor do que não as seguir. Nesse sentido, sob um olhar construtivista, a governança é capaz de gerar ordem se construída e adotada por todos ou pela maioria, em que os atores estejam propensos a respeitar aquilo que foi acordado. A partir desse respeito mútuo, a governança consegue promover uma melhor organização e previsibilidade, bem como menores incertezas.

Mas ao passar certa autoridade para os dispositivos criados pela governança, existe a visão de que isso confronta a soberania dos Estados na definição de como podem e/ou devem agir diante de determinada circunstância. Ou até mesmo a visão de que os princípios compostos em nível internacional pela governança correspondem a uma interferência externa. No entanto, nesse capítulo foi possível perceber que muitos dos recursos trazidos pela governança em âmbito global permitem que a soberania seja até mesmo fortalecida, já que podem ter a capacidade de arrefecer as assimetrias de poder existentes em vista das desigualdades vigente no sistema internacional.

Assim, a formação de certa singularidade sobre como reger um bem público global tende a proteger o princípio da soberania ao fazer com que todos os atores sigam um mesmo modelo, no qual os atores não estarão totalmente sujeitos apenas aos seus próprios recursos de poder. O ciberespaço, por sua vez, entra como um novo elemento na dinâmica da soberania por conta da natureza das suas particularidades. E é por isso que no próximo capítulo será explicado com maior profundidade o que caracteriza o ciberespaço e quais as suas reverberações para as relações internacionais.

3 CIBERESPAÇO E AS RELAÇÕES INTERNACIONAIS: AMEAÇAS, DESAFIOS E OPORTUNIDADES

Neste capítulo será apresentado as características do ciberespaço como um domínio nas relações internacionais, de forma a compreendê-lo como um novo ambiente para a projeção de poder. Sendo assim, as particularidades e as dimensões do espaço cibernético serão realçadas de modo que seja possível observar e assimilar os impactos desses aspectos no âmbito das relações internacionais. Dentre eles, a questão da segurança e da defesa cibernética, hoje reconhecidas como vitais para a estabilidade e a funcionalidade regular de toda uma nação. Isso porque as ameaças cibernéticas representam um grande perigo para as infraestruturas críticas e os sistemas essenciais utilizados para a realização de atividades fundamentais em uma sociedade.

Além disso, o capítulo irá abordar sobre a não existência de uma regulamentação internacional para o ciberespaço mesmo com toda a relevância e preocupação que os atores, tanto estatais quanto não estatais, dão para esse novo domínio. Sendo assim, será discutido e evidenciado o porquê dessa ausência e, de forma superficial, sobre como o direito internacional é hoje reconhecido como aplicável ao ciberespaço, mas gera dúvidas e não consegue responder com plenitude as particularidades produzidas pelas ações cibernéticas, especialmente as que envolvem a dimensão não-física do ciberespaço.

3.1 CIBERESPAÇO, UM DOMÍNIO NAS RELAÇÕES INTERNACIONAIS

A interdependência entre o mundo material e o mundo virtual foi sendo construída ao longo das últimas décadas, sendo que é possível considerar que o ambiente digital se tornou indispensável para as relações socioeconômicas e políticas como a concebemos hoje. Essa indispensabilidade fez com que o espaço cibernético, ou ciberespaço, passasse a estar presente na pauta contemporânea das políticas nacionais e internacionais dos Estados, especialmente no que tange à securitização desse espaço visto que, por envolver múltiplos atores e afetar a vida humana e as suas relações, o ciberespaço reverbera os seus efeitos para as relações internacionais (Martins, 2012).

A principal ferramenta tecnológica que proporcionou que isso se tornasse realidade foi a Internet e a sua rápida disseminação no mundo. Importante ressaltar que a Internet não é o ciberespaço, mas sim o seu maior mecanismo, por onde a maior parte das informações fluem no ambiente virtual. A Internet nasceu como um projeto dos Estados Unidos na década de 1950,

denominado de *Advanced Research Projects Agency* (ARPA), que consistia no estabelecimento de uma rede para unir computadores para que pesquisadores pudessem usar essa rede de forma cooperativa, facilitando a comunicação e o uso remoto de programas (Ryan, 2010). Com o resultado positivo do projeto, nas décadas seguintes houve a sua expansão para outros setores, sendo que outras redes foram criadas com o objetivo de promover uma maior transmissão de informações (Leiner *et al.*, 2009).

Mas foi somente nas décadas de 1980 e 1990 que a Internet deixou de ser uma exclusividade dos EUA e começou a ser disseminada para outras partes do mundo, especialmente para a Europa por meio do Conselho Europeu para Pesquisa Nuclear (CERN), que adotou a sua primeira rede interna para computadores em 1985 (Curran, 2012). Foi na década de 90, na CERN, que Tim Bernes-Lee desenvolveu o *World Wide Web* (WWW), transformando a interação e a comunicação nas redes, e, em 1998 a Internet já tinha chegado em todos os países mais populosos do mundo (Curran, 2012). A partir disso, a Internet se difundiu pelo mundo não somente como uma ferramenta acadêmica e militar, mas também servindo para as relações sociais, políticas e econômicas.

No mundo contemporâneo, o número de usuário conectados à Internet atingiu patamares sem precedentes, mostrando a força dessa ferramenta para a realização tanto de atividades básicas, quanto especializadas no nosso cotidiano. Em 2010, havia cerca de dois bilhões de usuários ao redor do mundo (UIT, 2010), sendo que atualmente, como visto, esse número ultrapassa o número de cinco bilhões de usuários, representando um crescimento exponencial na última década. "A Internet agora se tornou quase que um serviço "comódite", e muito da atenção dada recentemente tem sido sobre o uso dessa infraestrutura da informação global para o suporte de outros serviços comerciais" (Leiner *et al*. 2009, p. 30, tradução nossa)[15].

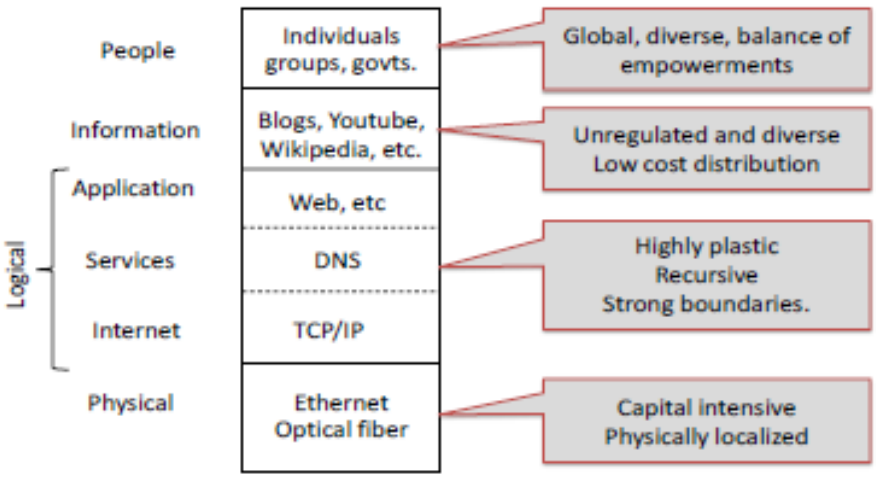
Dessa forma, a Internet propiciou que novas dinâmicas nas relações humanas se tornassem realidade, afetando diretamente nas relações econômicas e comerciais, na redução de custos, na otimização e agilidade de processos, na facilidade de acesso a produtos e serviços e uma maior integração global por meio da intensa troca de informações e dados. As mudanças e transformações geradas pela Internet fizeram com que o espaço cibernético tivesse cada vez mais relevância nas dinâmicas políticas, sociais e econômicas do mundo, passando a ser inserido nas agendas políticas dos países como um setor fundamental para o desenvolvimento e a manutenção da estabilidade e da ordem.

[15] Texto original: The Internet has now become almost a "commodity" service, and much of the latest attention has been on the use of this global information infrastructure for support of other comercial services.

Conforme expressa Daniel T. Kuehl (2009), o ciberespaço pode ser entendido como um domínio global que tem como característica o uso de eletrônicos e de espectros eletromagnéticos para criar, armazenar, modificar, trocar e explorar informações por meio de redes interconectadas, se utilizando de TICs. Isso significa que o ciberespaço possui como base para a sua existência uma dimensão física, composta de equipamentos, aparatos e materiais eletrônicos, que pode ser identificada como o *hardware*, e uma dimensão não-física, ou virtual, em que os dados e as informações são programados e podem fluir, também conhecida como *software*.

Na realidade, Nazli Choucri e David D. Clark (2012) apontam que a Internet, e o ciberespaço como um todo, é arquitetado em quatro camadas, que correspondem a camada física, a camada lógica, a camada informacional e a dos usuários. A camada física refere-se às infraestruturas e equipamentos, como os cabos de fibra óptica, torres de sinais, servidores e computadores. A camada lógica diz respeito ao software e os protocolos que são criados a partir das fundações físicas, como o WWW, os browsers, o sistema de nome e domínios, websites, entre outros. A camada informacional consiste nos textos codificados, fotos, vídeos e outros materiais que são armazenados, transmitidos e transformados no ciberespaço. A camada dos usuários refere-se aos humanos que usufruem do ciberespaço e ajudam a moldar a experiência cibernética ao realizar atividades de comunicação, trabalhos com informação, entre outros.

Figura 1 - Modelo de camadas do ciberespaço



Fonte: Choucri; Clark (2012)

Sendo assim, a dimensão virtual e invisível do ciberespaço se caracteriza por não possuir delimitações como os domínios tradicionais - terra, ar, água e espaço - possuem, sendo a sua demarcação materialmente intangível. Sendo assim, além de levantar questionamentos sobre como os Estados podem e devem reivindicar suas soberanias nesse domínio, o ciberespaço também proporciona que indagações e ambiguidades sejam levantadas sobre o controle efetivo sobre quem transmite informações, o que é transmitido, quando, como e com qual propósito (Choucri, 2012). Essas questões se tornam cada vez mais relevantes no mundo atual devido a dependência social e econômica existente entre o intenso fluxo de informações e o desenvolvimento de novas tecnologias, já que essas tecnologias podem ser capazes de promover o desenvolvimento econômico e transformar as relações sociais. Como expressa Choucri (2012, p. 36, tradução nossa)[16]:

> Ciberespaço abriu um novo contexto de interação, que permite ação e reação dentro e entre níveis de análises e possibilita a transmissão de conteúdo através de mecanismos que não eram disponíveis antes. As pressões constitutivas do acesso cibernético são potencialmente poderosas o suficiente para alterar a natureza das interações, se não os próprios riscos.

Nesse contexto, o rápido avanço tecnológico tem sido reconhecido por propiciar mudanças nas estruturas socioeconômicas, mesmo que essas mudanças sejam distintas e desiguais em diferentes sociedades e regiões, tendo impactos positivos e negativos, visto que os efeitos das TICs podem diferir de acordo com o contexto econômico, social e político de determinado local (Lee; Shao; Vinze, 2018). Isso porque a depender do contexto, a disseminação de TICs pode ser absorvida por uma sociedade de modo a gerar desemprego, desestabilidade social e política e alterar as estruturas socioeconômicas de um país, assim como pode estimular e potencializar o desenvolvimento industrial, os recursos humanos e até mitigar problemas sociais (Lee; Shao; Vinze, 2018).

Sendo assim, a disseminação de informações e a forma como essas informações são transmitidas possuem ligação direta com os benefícios ou malefícios que isso pode trazer para determinada sociedade. Consequentemente, o controle de informações e dados, e até mesmo a sua regulamentação, tem capacidade para influenciar as dinâmicas sociais e podem ir ao encontro dos interesses de quem possui o controle sobre como, quando e por quais motivos determinadas informações são transmitidas ou não. Ao fim e ao cabo, o controle de capacidades

[16] Texto original: Cyberspace has opened up a new context of interaction, one that allows action and reaction within and across levels of analysis and enables the transmission of content through mechanisms that were not available earlier. The constitutive pressures of cyber access are potentially powerful enough to alter the nature of interactions, if not the stakes themselves.

cibernéticas e TICs, que permitem como o fluxo informacional pode ocorrer, representa um exercício de poder com reverberações políticas.

Isso porque é possível interpretar que quem controla propriedades do fluxo de informações, como o conteúdo, a velocidade e quem pode ter acesso, consegue empregar poder sobre quem não tem controle sobre essas propriedades (Marlin-Bennet; Jackson, 2022), sendo condicionados a aceitar, diretamente ou indiretamente, os desígnios estabelecidos pelos detentores. Essa interpretação parte do entendimento que, atualmente, dados e informações influem sobre o comportamento social, mesmo que de maneira sutil ou superficial. A maneira como uma informação é comunicada tem a capacidade de impactar as emoções de quem recebe a informação, podendo transformar questões como crenças, desejos, identidades, em que um ator pode alterar a forma como outro se sente e age ao comunicar determinadas informações (Marlin-Bennet, 2022). "Humanos estão constantemente se comunicando de formas que fazem cada um se sentir diferente, pensar diferente e se tornar diferente" (Marlin-Bennet, 2022, p. 441, tradução nossa)[17].

Em larga escala, a disseminação de informações pode ser vista como um mecanismo capaz de afetar as relações sociais a ponto de criar efeitos sobre as estruturas sociais, políticas e culturais de uma sociedade. Consequentemente, as transformações podem repercutir no próprio Estado. Nesse sentido, o ciberespaço acaba sendo um espaço capaz de proporcionar preocupações aos Estados, não apenas devido aos fluxos de informações em seu território, mas também por permitir que ações hostis possam ser perpetradas através dele. Como expressa Nazli Choucri e David Clark (2012), essa preocupação fez com que os Estados passassem a tratar as questões do domínio cibernético não mais como um assunto da "baixa política", e sim como um assunto da "alta política".

É possível considerar que uma das características do espaço cibernético, que dificulta o estabelecimento de diretrizes estratégicas para a sua proteção, seja a sua fluidez e transnacionalidade. Isso porque as formas de utilização do ciberespaço se modificam ao passo que inovações tecnológicas permitem diferentes interações e ações por meio do domínio cibernético que antes não eram possibilitadas. Assim, o setor cibernético acaba sendo associado com a possibilidade de imersão em diferentes ambientes, experiências e modos de expansão de fronteiras (Choucri, 2012). E, ao enquadrar o espaço cibernético como um meio em que as relações sociais são promovidas, a maneira na qual o ciberespaço é arquitetado e operacionalizado acaba impactando na forma em como essas relações sociais são concretizadas.

[17] Texto original: Humans are constantly communicating in ways that make each other feel differently, think differently and become different

Como já comentado no capítulo anterior, as características das dimensões não-físicas do ciberespaço, marcadas pela não delimitação material, faz com que esse domínio desafie a reivindicação da soberania nacional, visto que apesar dos equipamentos físicos, como os servidores e os cabos de fibras ópticas, estarem localizados no território de determinado país, a dimensão virtual e invisível do espaço cibernético pode questionar a habilidade do Estado em controlar o fluxo de informações nas suas fronteiras nacionais (Khanna, 2018). Nesse caso, olhar para a soberania em uma perspectiva inflexível a partir da sua conceituação tradicional, torna difícil a sua aplicabilidade ao espaço cibernético. Na verdade, essa inflexibilidade pode ser vista até mesmo como fora de contexto ou desatualizada para o ciberespaço, visto que o próprio Estado se tornou um agente multifacetado e, por conseguinte, uma visão limitada e dura da soberania tende a ignorar a influência de outros atores que hoje exercem influência no jogo da política nacional e internacional (Lambach, 2019).

Dessa forma, como coloca Julie Cohen (2007), a importante indagação que deve ser feita não é que tipo de espaço o ciberespaço é ou pode ser definido, mas sim no que o mundo irá se tornar enquanto espaço ao incluir integralmente o ciberespaço. Isso significa que não se pode mais pensar no espaço cibernético como algo separado ou distante do mundo material e "*off-line*", mas como um espaço que permeia o mundo material e virtual, assim como permeia os demais domínios tradicionais. Daniel Ventre (2012) expõe que essa é a característica da transversalidade do ciberespaço, que possibilita que esse domínio possa projetar poder e seus reflexos nos demais domínios materiais, já que os sistemas de comunicação e informação estão presentes em tecnologias utilizadas em todos os domínios e o ambiente virtual por onde as informações e dados trafegam não possui limitação física.

Além disso, diferentemente dos domínios tradicionais, que tiveram a sua origem na natureza, o ciberespaço é o primeiro e único domínio, até então, construído por seres humanos, que não só o criaram como foram responsáveis por dar significado e função aos atos executados nele. Isso significa que tanto as relações sociais, quanto as regras e princípios para reger o ambiente cibernético não possuem registro histórico e precisam ser construídas e até reinventadas (Chenou, 2014). Inevitavelmente, essas construções perpassam pelo elemento político, que acaba por designar os caminhos tomados na formação das interações e das normas voltadas ao ciberespaço.

Como consequência, a delineação de políticas destinadas ao domínio cibernético pelos Estados carrega em si o reconhecimento de que esse domínio possui a capacidade de influenciar a própria ordem social, econômica e política, tanto nacional quanto internacional. Isso ocorre já que os Estados não operam no vácuo, sendo parte de um sistema internacional que impacta

e é impactado pela forma em que eles são constituídos, como se comportam e como interagem (Deibert; Crete-Nishihata, 2012). Com isso, interpreta-se que o ciberespaço hoje faz parte da agenda geopolítica global, com capacidade de produzir implicações sobre as relações interestatais. Assim, o domínio cibernético no contexto geopolítico refere-se ao uso dos sistemas digitais, como a Internet, para se atingir os objetivos políticos de determinado ator (Wood, 2020).

Nessa perspectiva, os principais elementos geopolíticos no qual o ciberespaço afeta diretamente são os aspectos da soberania e dos conflitos, ambos voltados para a apreensão dos Estados em relação à defesa e segurança. Sendo assim, questões como o direito à autodeterminação no ciberespaço e até mesmo o que configura uma violação de soberania nesse espaço acabam se tornando um problema sem definição clara (Hollis; Ohlin, 2018). O reconhecimento da soberania no ciberespaço implicaria num processo de territorialização desse ambiente virtual, no qual os Estados tenderiam a estabelecer controle sobre os processos e fluxos. Esse controle pode ser entendido como uma maior capacidade de vigilância e de impor a sua vontade em relação à terceiros, sendo exercido de maneira hierárquica, em que a projeção de força, imposição de regras e determinação de punições para transgressores pode ser executada (Lambach, 2019). Assim, territorializar o espaço cibernético refere-se à uma:

> [...] analogia ciber para o território estatal físico que solidifica o alcance regulatório do Estado e fundamentam as reivindicações jurisdicionais. Essa estratégia de reterritorialização procede da questão normativa que toda atividade online que ocorre "dentro" de um país (por conta dos usuários, servidores ou dados estarem localizados lá) deve ser tratada como parte correspondente do território do ciberespaço (Lambach, 2019, p. 13, tradução nossa)[18].

Dessa forma, a territorialização está diretamente ligada ao exercício de poder no espaço cibernético, em que o Estado passa a ter maior capacidade de regulamentação desse domínio como um recurso de poder. Se considerarmos que o ciberespaço é constituído pelas camadas indicadas anteriormente, então pode-se assumir que estabelecer o controle do ciberespaço perpassa pela manipulação de todas essas camadas, sendo que especialmente as camadas materiais tem potencial para propiciar disputas entre os atores no sistema internacional, pois são mais fáceis de exercer dominação em contraponto à dimensão não física do ciberespaço.

[18] Texto original: [...] cyber-analogies to physical state territory that solidify states' regulatory reach and undergird jurisdictional claims. This reterritorialization strategy proceeds from the normative assumption that all online activity that occurs "in" a country (because users, servers, or data are "located" there) should be treated as a part of a corresponding cyberspace territory.

As disputas podem ocorrer em decorrência da desigualdade existente em relação a como o controle da camada lógica e física está distribuída no cenário global. Um exemplo concreto é disposição dos servidores-raiz da internet, em que dos 13 existentes no mundo, 10 estão localizados nos Estados Unidos (Canabarro; Gonzales, 2018). Isso significa que caso a territorialização do ciberespaço ocorra no contexto atual, com a implementação do princípio da soberania nacional, questionamentos e objeções sobre a distribuição dos recursos essenciais para o gerenciamento e operacionalização do ciberespaço emergiriam. Pois, os EUA teriam a prerrogativa de coordenar o funcionamento desses servidores-raiz sem prestar contas à comunidade internacional, sendo protegido pela determinação de sua soberania. Sendo assim, a questão da soberania do ciberespaço está diretamente ligada a uma circunstância geopolítica e, com isso, ao próprio exercício de poder dos Estados (Lambach, 2019).

Em relação à dimensão dos conflitos, que também implica em questões geopolíticas, o elemento cibernético tem alterado a sua forma de ocorrência. Isso se deve ao uso e adaptação das novas tecnologias por Forças Armadas, que levanta questionamentos sobre a militarização do domínio cibernético e a utilização do ciberespaço para gerar efeitos em combates (Inkster, 2017). A utilização de capacidades cibernéticas de maneira ofensiva tem aumentado no mundo, com uma crescente execução de ataques cibernéticos. Podem ser consideradas armas cibernéticas qualquer ferramenta, utilizada através do ciberespaço, que foi desenvolvida para causar danos e rupturas em um determinado ator (Wood, 2020). Assim, o uso cada vez mais frequente de tais ferramentas tem sido considerado um fator relevante para o cenário da segurança internacional (Wood, 2020).

Nesse sentido, um debate sobre a possibilidade de ocorrência de uma guerra cibernética tem sido levantado nos últimos anos. Como expressa John Stone (2013), a realização de uma guerra cibernética poderia acontecer visto que ataques cibernéticos poderiam ser considerados atos de violência com capacidade de produzir letalidade se fosse levado em conta a consequência dos ataques, e não somente o seu alvo. No entanto, independentemente de haver ou não uma guerra cibernética nos dias atuais ou futuros, a utilização do ciberespaço em conflitos já é uma realidade, fazendo com que possuir recursos cibernéticos ofensivos e/ou defensivos possa ser visto como um elemento de poder pelos atores, tanto estatais quanto não estatais. Como consequência, emerge a necessidade de analisar o ciberespaço como um domínio capaz de possibilitar a projeção de poder, de forma a observar se o poder cibernético é um elemento relevante na política internacional.

3.2 PODER CIBERNÉTICO COMO UM INSTRUMENTO DE PODER NA POLÍTICA INTERNACIONAL

Para tratar sobre poder cibernético, é preciso antes conceituar e delimitar o que se entende por poder nas relações internacionais. De modo geral, como indica David Baldwin (2016), o poder prevê uma ideia relacional e possui múltiplas dimensões. Isso porque não se pode medir o poder de determinado ator sem levar em consideração as capacidades e dimensões de um outro ator. Dessa forma, as relações de poder e os recursos nos quais essas relações são baseadas são vitais para o pensamento sobre o poder (Baldwin, 2016). Assim, Baldwin (2016) se apoia no conceito de Robert Dahl (1957), apresentando que poder representa a capacidade de um ator "A" fazer com que um ator "B" faça algo que não faria sem a influência de "A", indo ao encontro dos interesses de "A".

Ao analisarmos o setor cibernético e sua influência para as relações internacionais, observa-se uma necessidade de compreender - e até mesmo desenvolver - uma visão sobre a capacidade desse setor em projetar poder entre os atores do sistema internacional, de modo a elucidar como esses atores podem se utilizar de um poder cibernético para alcançar os seus objetivos. Assim, levando em consideração o conceito tradicional de poder apresentado anteriormente, é possível expressar que o ciberespaço é um espaço de poder caso ele tenha o potencial de afetar as relações entre atores de modo que a intenção e o interesse de um ator seja prevalecido em detrimento de outro.

Dessa forma, o ciberpoder, ou poder cibernético, pode ser entendido como a habilidade de utilizar o ciberespaço de forma a criar vantagens e influenciar eventos em diferentes ambientes operacionais e sobre instrumentos de poder (Starr, 2009). Por ser um ambiente de disseminação de informações, o poder cibernético é capaz de operar em diferentes esferas, não apenas no âmbito militar e da guerra, tendo também implicações nas esferas sociais, políticas, econômicas e psicológicas (Starr, 2009). Com isso, em razão dessa e outras características do setor cibernético, para Joseph Nye (2010) o ciberespaço pode ser entendido como um domínio de difusão de poder.

Isso porque, segundo o autor, múltiplos atores podem ter acesso, participação ativa e influência no mundo virtual, já que as barreiras para a entrada no espaço cibernético são baixas e, consequentemente, até mesmo um indivíduo com um computador e acesso à Internet pode ter capacidade de realizar ações com grandes efeitos para a sociedade (Nye, 2010). Nesse sentido, a difusão pode beneficiar atores com menos recursos e capacidades, como os Estados considerados mais fracos ou atores não estatais, em que ações de baixo custo e até mesmo o

anonimato pode permitir que sejam realizadas ações cibernéticas mesmo que exista uma assimetria de poder entre os atores envolvidos (Nye, 2010).

Além disso, o teórico aponta que alterações na maneira em como as informações são distribuídas tiveram, historicamente, um importante impacto nas relações de poder e, com isso, o ciberespaço faz com que a figura do Estado, mesmo as maiores potências mundiais, não possuam o mesmo controle que possuem sobre os outros domínios tradicionais. Desse modo, Nye (2010) busca definir o poder cibernético de duas maneiras, uma tem vinculação com a questão comportamental, referindo-se à habilidade de obter resultados por meio de recursos de informações eletronicamente interconectados do domínio cibernético; a outra consiste na ideia de Starr (2009) já comentada, sobre a influência em outros ambientes e instrumentos de poder.

Contudo, apesar de todos esses aspectos do poder cibernético, o autor argumenta que o Estado ainda prevalece como o principal ator das relações internacionais, sendo detentor das maiores capacidades de controle. Consequentemente, apesar de difundir o poder, o ciberespaço não o torna igualitário entre os atores, sendo que o *status quo* da assimetria de poder acaba por ser mantido (Nye, 2010).

> Enquanto o ciberespaço pode criar certa mudança de poder entre os Estados ao abrir oportunidades limitadas para saltos por Estados pequenos ao usar a guerra assimétrica, é pouco provável que seja um fator de mudança nas transições de poder. Por outro lado, enquanto deixa os governos como os atores mais fortes, é provável que o domínio cibernético aumente a difusão do poder para atores não-estatais, e ilustra a importância das redes como uma dimensão de poder chave no século XXI. (Nye, 2010, p. 19, tradução nossa)[19].

Ao olharmos para maneiras práticas de exercer poder, um dos meios é o uso da força, em que condutas ofensivas tendem a moldar o comportamento daqueles nos quais tais condutas são direcionadas. Sendo assim, a realização de ataques cibernéticos a partir das consideradas armas cibernéticas poderia servir como um instrumento que caracteriza o uso da força através do ciberespaço. As armas cibernéticas podem ser usadas para causar a ruptura de sistemas e redes de adversários, inabilitando o seu uso, ou causar a destruição de dados e sistemas que podem produzir até mesmo efeitos físicos (Lonergan, 2017). Isso significa que o uso tático, estratégico e operacional de capacidades cibernéticas ofensivas poderia constituir um ato de

[19] Texto original: While cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by small states using asymmetrical warfare, it is unlikely to be a game changer in power transitions. On the other hand, while leaving governments the strongest actors, the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century.

poder, caso essa ação configure uma relação em que o agressor consegue alterar, influenciar ou subjugar o comportamento do outro.

Nesse sentido, seria preciso averiguar a efetividade de determinada ação cibernética para caracterizá-la como uma dimensão do poder cibernético. Segundo Robert Bebber (2017), a efetividade cibernética é a habilidade de um ator em traduzir, ou manifestar, o poder cibernético em consonância com a finalidade da política nacional através do ciberespaço e dentro dele. Nesse sentido, o ator que quiser ter algum grau de efetividade, como o Estado, terá que possuir os recursos necessários para formar uma força cibernética, como por exemplo ferramentas cibernéticas militares, leis aplicáveis e inteligência (Bebber, 2017).

Contudo, é possível problematizar a questão da efetividade cibernética como uma ação de poder, visto que dificilmente ela conseguirá ser mensurada em termos quantitativos. E, além disso, por conta da facilidade do anonimato no mundo virtual e da dificuldade de atribuição no ciberespaço, saber a real intenção de determinado agressor em relação à ação executada acaba se tornando um empecilho. Como consequência, ao não saber a motivação – política ou não – do ator que comete o ato, torna-se difícil aferir sobre a efetividade do ato, visto que não se saberá se os efeitos produzidos vão ao encontro dos objetivos e da pretensão inicialmente estabelecida.

Outro meio de implementação de poder que não se vincula ao uso da força bruta, e às vezes está ligada à dissuasão, é a coerção, que consiste em afetar o comportamento de um adversário por meio da ameaça ou força limitada.

> Coerção envolve produzir um comportamento ou um efeito desejado por parte do adversário ao forçá-lo se confrontar com o cálculo do custo-benefício, de forma que o adversário acredita que é menos custoso conceder à preferência de (in)ação de quem faz a ameaça do que desafiar as exigências dele. (Borghard; Lonergan, 2017, p. 453, tradução nossa)[20].

Dessa forma, para a coerção ser assertiva, é preciso que alguns aspectos sejam empreendidos. O primeiro deles é a comunicação, que precisa ser clara e entendível para aquele que está sofrendo a coerção. Para Erica Borghard e Shawn Lonergan (2017), o alvo tem que entender o que está em jogo e quais as consequências de aceitar ou não as condições impostas, sendo que no ciberespaço isso pode se tornar um problema, já que não há nesse ambiente uma linguagem aceita e pré-estabelecida entre os tomadores de decisão, dificultando o entendimento comum entre quem está enviando o sinal cibernético, indicando a coerção, e quem está

[20] Texto original: Coercion involves producing a desired behavior or outcome on the part of an adversary by forcing her to confront a cost-benefit calculus, such that the adversary believes it is less costly to concede to the threatener's preferred course of (in)action than to defy the latter's demands.

recebendo o sinal. A questão da atribuição também cria impedimentos para uma comunicação coerciva efetiva no espaço cibernético. Pois, como mencionado, a facilidade do anonimato no mundo virtual faz com que se torne difícil saber a autoria de uma ação cibernética caso o ator não se manifeste. Nesse sentido, um Estado que queira implementar a coerção através do ciberespaço deve empregar métodos que assegure a atribuição (Borghard; Lonergan, 2017).

Outro aspecto para a coerção ser assertiva é o cálculo de custo-benefício. Isso porque assume-se que os atores são racionais no sistema internacional e, então, irão ponderar sobre como responder às ameaças e provocações de outros atores. A coerção força o alvo a escolher entre fazer concessões ou sofrer as consequências e, assim, o ator que realiza a coerção precisa fazer uma ameaça na qual o alvo perceba que é melhor ceder do que sofrer as consequências (Borghard; Lonergan, 2017). No âmbito do ciberespaço, o agressor pode provocar a coerção por ameaça de ataque de perturbação de sistemas ou de efeitos destrutivos, mas o cálculo das consequências é debilitado pela própria dificuldade de comunicar os sinais cibernéticos, impedindo a plena interpretação do alvo, que não terá as ferramentas suficientes para calcular os custos-benefícios (Borghard; Lonergan, 2017).

Por fim, o terceiro aspecto da coerção é a credibilidade, no qual o ator que pratica a coerção deve ter as capacidades necessárias para concretizar a sua ameaça, sendo que deve também ser capaz de mostrá-las ao alvo. No ciberespaço, ter noção da credibilidade de um ator que pratica a coerção é algo complexo, em vista da dificuldade em mensurar as suas capacidades cibernéticas (Borghard; Lonergan, 2017). O estabelecimento de índices confiáveis poderia ser um caminho para essa mensuração, porém, ter a informação plena sobre os atributos e recursos cibernéticos de determinado ator é uma tarefa extremamente complicada, já que os próprios atores não têm interesse em expor essas informações (Borghard; Lonergan, 2017).

Considerando todos esses aspectos, interpreta-se que o ciberespaço pode não ser um domínio que propicia a dissuasão. O poder cibernético, portanto, tende a consistir em um conjunto de capacidades que não conseguem ser mensurados adequadamente, em que os atores manifestam discretamente os seus propósitos (Willet, 2019). Sendo assim, os atores, especialmente os Estados, buscam contar com as redes de informação para projetar poder no espaço cibernético, de forma a estabelecer os objetivos estratégicos com base na resiliência e em como essas redes de informações podem ser utilizadas, tanto internamente quanto externamente (Bebber, 2017).

Dessa forma, a projeção de poder no ciberespaço por meio da coerção e/ou da força bruta parece não ser o caminho mais propenso a ser utilizado pelos Estados, apesar de ações ofensivas no setor cibernético serem capazes de desestabilizar sistemas essenciais e até mesmo

produzir efeitos físicos. Como aponta Thomas Rid (2012), pelas características do ciberespaço as ações ofensivas tendem a ser realizadas em conjunto com ações cinéticas, sendo auxiliares, como foi no caso da Operação Pomar[21] feita por Israel contra reatores nucleares da Síria. Como consequência, interpreta-se que projetar poder exclusivamente através do espaço cibernético pode ser mais um mecanismo de *soft power* do que de *hard power*.

Como coloca Nye (1990), *soft power* refere-se a outros aspectos, que não a força e recursos militares, que também exercem poder na relação entre atores estatais e tem a capacidade de influenciar os seus comportamentos, como aspectos culturais, ideológicos e as instituições internacionais. Nesse sentido, a forma como as informações e dados fluem no ciberespaço e como o ambiente virtual é estruturado e gerenciado acabam se tornando ferramentas ou instrumentos de poder. Pois, são capazes de influenciar não apenas o modo de funcionamento de importantes mecanismos cibernéticos, como a Internet, mas também a forma como os usuários se comportam no ambiente virtual, podendo ter impacto na conduta cultural e política de uma sociedade.

No entanto, é inegável a utilização de capacidades cibernéticas em ações maliciosas de ataques e uso da força que podem colocar em risco sistemas e infraestruturas que podem levar a desestabilização e o funcionamento ordinário de uma nação. Se hoje os assuntos cibernéticos são considerados da alta política, muito se deve por conta das ameaças e vulnerabilidades que surgiram com o ciberespaço. Por conseguinte, o crime cibernético, o roubo de dados, as sabotagens, dentre outros, geram uma preocupação cada vez maior para os Estados devido à interdependência construída nos últimos anos com a digitalização de processos, atividades, funções e sistemas. Dessa forma, a segurança e a defesa cibernética passaram a ser cada vez mais relevantes no âmbito da segurança e da defesa nacional e internacional.

3.3 A SEGURANÇA CIBERNÉTICA E A DEFESA CIBERNÉTICA NO ÂMBITO DA SEGURANÇA INTERNACIONAL

Os conceitos da cibersegurança e da ciberdefesa provém das perspectivas da segurança e da defesa nacional para a proteção e manutenção da estabilidade do ciberespaço, sendo que a evidência e a necessidade da segurança cibernética e da defesa cibernética ocorrem devido à existência dos riscos e perigos provenientes do setor cibernético. A natureza e o escopo das

[21] A Operação Pomar consistiu em um ataque aéreo israelense contra uma usina nuclear da Síria, no ano de 2007, sendo que antes da realização do ataque cinético, ataques cibernéticos foram feitos para derrubar os sistemas sírios de detecção de ameaças no espaço aéreo.

ameaças cibernéticas mudaram e mudam sucessivamente em vista das mudanças tecnológicas e o uso e aplicabilidade dessas tecnologias pela sociedade civil, pelos governos e pelo setor militar. Dessa forma, para se ter uma completude em relação à compreensão da defesa e da segurança cibernética, é preciso ter primeiro um entendimento geral sobre a defesa e a segurança nacional.

As definições e concepções sobre esses termos são variadas, especialmente em relação à distinção entre segurança e defesa, apesar de ambas possuírem a proteção e a preservação de uma estabilidade pacífica como objetivo final. Na verdade, é importante ter noção de que esses conceitos passaram por processos de transformações ao longo dos anos em vista do contexto histórico da política internacional de cada período. Durante a Guerra Fria, a segurança era vista como um assunto estritamente militar e relacionada majoritariamente às questões de soberania e proteção territorial. Com as mudanças políticas e econômicas ocorridas principalmente a partir da década de 1990, outros temas e assuntos começaram a ser inseridos na agenda da segurança. Em grande parte, isso ocorreu devido à globalização e a emergência de assuntos globais que passaram a ser cada vez mais relevantes para a estabilidade e a ordem dos Estados.

Para Barry Buzan (1997), essa visão tradicional que correlacionava segurança apenas com os assuntos militares começou a se desgastar com a atenuação de guerras interestatais, permitindo que questões de outras naturezas pudessem ser evidenciadas. Por consequência, Buzan (1997) expõe que securitizar determinado assunto é um processo intersubjetivo. Com isso, a segurança sofreu um processo de ampliação, incorporando áreas econômicas, sociais, ambientais e políticas sem se restringir à figura do Estado unicamente, mas também a pessoas, atores não governamentais e a comunidade internacional como um todo (Saleh, 2010).

Não à toa, na década de 90 a ONU trouxe a concepção de segurança humana ao mundo, a partir do Relatório de Desenvolvimento Humano, do Programa das Nações Unidas para o Desenvolvimento (PNUD), em 1994. O documento expressava que:

> O conceito de segurança por muito tempo foi interpretado de maneira estreita: como segurança do território de uma agressão externa, ou como a proteção dos interesses nacionais na política externa ou como segurança global contra a ameaça de um holocausto nuclear. Tem sido mais relacionada com os Estados nações do que com as pessoas. As superpotências estavam presas em uma luta ideológica – travando uma guerra fria em todo o mundo. (PNUD, 1994, p. 22, tradução nossa)[22].

[22] Texto original: The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of a nuclear holocaust. It has been related more to nation-states than to people. The superpowers were locked in an ideological struggle-fighting a cold war all over the world.

Sendo assim, o conceito de segurança passou a focar no ser humano, em relação às condições nas quais as pessoas vivem e nos eventos, acontecimentos e fenômenos que podem afetar as suas vidas, impossibilitando a paz. Isso significa que a segurança, centrada no humano, passou a se referir também sobre questões como fome, repressão, doenças, crises econômicas, entre outras ameaças que perturbam a vida cotidiana (PNUD, 1994). Dessa forma, em um sentido amplo, é possível interpretar a segurança como "um estado de equilíbrio, onde os indivíduos possuem a percepção de liberdade para o acesso a informações, produtos e processos que consideram apropriados para fomentar o seu desenvolvimento [...]" (Raza, 2005, p. 69, tradução nossa)[23].

Tem-se a percepção que a segurança está vinculada às políticas, ações, mecanismos e instrumentos que preservam e tendem a preservar a estabilidade de uma nação de forma a garantir o bem-estar da população e o funcionamento regular dos setores e instituições considerados fundamentais para a ordem social. No Brasil, a definição de segurança nacional encontrada na Política Nacional de Defesa (2016)[24] expressa que a segurança nacional é: "[...] entendida como a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e dos deveres constitucionais" (Brasil, 2016, p. 11).

A definição dada pelo governo brasileiro enfatiza a segurança como uma sensação, ou condição, sendo relacionada a um estado sem perturbações em que a manutenção da organização regular do cenário nacional é assegurada a despeito da existência de ameaças. Já a defesa nacional está vinculada com as pressões e os riscos externos que o país pode sofrer, sendo diretamente ligada às funções das Forças Armadas em garantir a proteção e a integridade do território nacional. Dessa forma, o governo brasileiro define a defesa nacional como "[...] conjunto de atitudes, medidas e ações do Estado para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas" (Brasil, 2016, p. 11).

A visão de separação entre segurança e defesa adotada pelo Brasil, e também neste trabalho, evidencia que esses fenômenos são tratados por atores e instituições diferentes dentro da realidade nacional. Os desafios, ameaças e preocupações para a preservação da segurança

[23] Texto original: state of equilibrium where individuals perceive themselves as having the freedom to access information, products and processes they consider proper for fostering their development.

[24] Ressalta-se que a utilização da Política Nacional de Defesa, do ano de 2016, em contrapartida a documentos mais recentes se deu em vista da não aprovação, em todas as instâncias, de documentos como o Livro Branco de 2020, no momento da elaboração deste trabalho.

podem (mas não necessariamente) ser distintos dos aspectos para a preservação da defesa, envolvendo diferentes aparatos estatais. Nesse sentido, até mesmo a elaboração e implementação de políticas a serem aplicadas para a segurança e a defesa nacional podem ser divergentes.

Entendido a concepção de segurança e defesa, pode-se partir para a compreensão da segurança cibernética e da defesa cibernética. Para isso, foi separado definições desses termos, tanto de fontes primárias com base em documentos governamentais, como fontes secundárias de teóricos e pesquisadores do assunto, de forma que um entendimento geral possa ser proposto neste trabalho. Na tabela a seguir foi esquematizado algumas definições para melhor compreensão e visualização.

Tabela 1 – Definições de segurança cibernética e defesa cibernética no âmbito governamental

Documento	Autor	Definição de segurança cibernética	Definição de defesa cibernética
DOD Dictionary of Military and Associated Terms (2021)	Estados Unidos	Ações tomdas de proteção no ciberespaço para prevenir acessos não autorizados, a exploração ou o dano a computadores, sistemas de comunicação eletrônicos, e outras tecnologias da informação, incluindo tecnologia da informação de plataforma, bem como a informação neles contidas, para garantir a sua disponibilidade, integridade, autenticação, confidencialidade e nã repúdio (EUA, 2021, p. 55, tradução nossa)[25].	Ações tomadas de proteção no ciberespaço para derrotar ameaças específicas que tenham violado ou estejam ameaçando violar medidas de segurança cibernética e incluem ações para detectar, caracterizar, contra-atacar e mitigar ameaças, incluindo *malware* ou atividades não autorizadas de usuários, e para restaurar o sistema para uma configuração segura (EUA, 2021, p. 55, tradução nossa)[26].
Doctrine of Information Security of the Russian Federation (2016)	Rússia	[...] é o estado de proteção do indivíduo, sociedade e do Estado contra ameaças de informação internas e externas, permitindo a garantia dos direitos e liberdades constitucionais dos humanos e do cidadão, a qualidade e o padrão de vida dignos dos cidadãos, a	

[25] Texto original: Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

[26] Texto original: Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration.

		soberania, a integridade territorial e o sustentável desenvolvimento socioeconômico da Federação Russa, bem como a defesa e a segurança do Estado (Federação Russa, 2016, p. 2, tradução nossa)[27].	
Glosario de Términos de Ciberseguridad (2019)	Argentina	É a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço (Argentina, 2019, p. 4, tradução nossa)[28].	
Glossário das Forças Armadas (2015)	Brasil	Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Brasil, 2015, p. 249).	Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (Brasil, 2015, p. 85).

Fonte: Elaborado pelo autor

Tabela 2 – Definições de segurança cibernética e defesa cibernética por organizações internacionais

Documento	Autor	Definição de segurança cibernética	Definição de defesa cibernética
ENISA overview of cybersecurity and related terminology (2017)	Agência Europeia para a Segurança das Redes e da Informação (ENISA)	[...] abrange todos os aspectos de prevenção, previsão; tolerância; detecção; mitigação; remoção; análise e investigação de incidentes cibernéticos. Considerando os diferentes tipos de componentes do espaço cibernético, a segurança cibernética deve abranger os seguintes atributos: Disponibilidade, Confiabilidade,	[...] refere-se a variedade de mecanismos defensivos que podem ser usados para mitigar ou responder a ataques cibernéticos (ENISA, 2017, p. 7, tradução nossa)[30].

[27] Texto original: [...] is the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decente quality and standard of living for citizens the sovereignty the territorial integrity and sustainable sócio-economic development of the Russian Federation, as well as defence and security of the State.

[28] Texto original: Es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

[30] Texto original: [...] refers to a variety of defensive mechanisms that could be used to mitigate or respond to cyber attacks

		Segurança, Confidencialidade, Integridade, Capacidade de manutenção (para sistemas, informações e redes), Robustez, Capacidade de sobrevivência, Resiliência (para suportar a dinamicidade do ciberespaço), Prestação de contas, Autenticidade, e Não repúdio (para suportar a segurança da informação) (ENISA, 2017, p. 6, tradução nossa)[29].	
Overview of cybersecurity (2008)	União Internacional de Telecomunicações (UIT)	[...] a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas securitárias, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente e a organização cibernéticos e os ativos dos usuários. Os ativos da organização e dos usuários incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibenético. Segurança cibernética se esforça para assegurar o atendimento e a manutenção de propriedades de segurança dos ativos da organização e dos usuários contra relevantes riscos para a segurança no ambiente cibernético (UIT, 2008, p. 2, tradução nossa)[31].	

Fonte: Elaborado pelo autor

[29] Texto original: [...] covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security).

[31] Texto original: [...] the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Tabela 3 - Definições de segurança cibernética e defesa cibernética no âmbito acadêmico

Documento	Autor	Definição de segurança cibernética	Definição de defesa cibernética
Implementing Effective Cyber Security Training for End Users of Computer Networks (2015)	Richard E. Beyer; Bradley J. Brummel	[...] envolvem tecnologias, práticas e processos essenciais projetadas para proteger redes, programas de computador, pessoas e dados contra ataques, danos, lesões ou acesso não autorizado (Beyer; Brummel, 2015, p. 3, tradução nossa)[32].	
Guia de Defesa Cibernética na América do Sul (2017)	Marcos Aurélio Guedes de Oliveira *et al.*	Aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para proteger o ambiente cibernético de um país e suas organizações. De forma mais direta, a segurança cibernética trata de temas relacionados à segurança pública (Guedes *et al*., 2017, p. 14).	ato de defender o sistema crítico das TICs de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país (Guedes *et al.*, 2017, p. 13).
Defining Cybersecurity (2014)	Dan Craigen *et al.*	Organização e coleção de recursos, processos, e estruturas usadas para proteger o ciberespaço e sistemas habilitados pelo ciberespaço contra ocorrências que desalinham *de jure* os direitos de propriedade de fato. (Craigen *et al*., 2014, p. 17, tradução nossa)[33].	

Fonte: Elaborado pelo autor

A multiplicidade e divergências entre as definições evidencia a complexidade do assunto e como a própria compreensão dos termos ainda está em uma fase de construção, em que os diferentes atores e autores buscam contemplar uma conceituação a partir das suas visões e entendimento sobre o assunto. A partir da tabela, percebe-se que não são todos que diferem a segurança cibernética da defesa cibernética, utilizando o primeiro termo para englobar ambas. Dessa forma a cibersegurança acaba tendo um sentido ampliado, correspondendo a todos os mecanismos de processos de proteção no que tange ao setor cibernético. No entanto, aqui nesse trabalho vamos seguir a ideia já comentada de separação entre os termos, em que cada um

[32] Texto original: [...] involve core technologies, processes and practices designed to protect networks, computers programs people and data from attack, damage, injury, or unauthorized access.

[33] Texto original: Organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

possui a sua definição e envolve suas próprias particularidades em relação ao domínio cibernético.

Sendo assim, com base nas definições trazidas, de forma a condensá-las e sintetizá-las, entende-se que segurança cibernética abrange as ações, processos, práticas, recursos e mecanismos que visam a proteção e a manutenção da funcionalidade regular de sistemas digitais e do ambiente cibernético, com a finalidade de garantir uma sensação e uma situação de preservação da estabilidade do ciberespaço para a sociedade, de modo que esta possa agir e utilizar TICs de forma resguardada. Já a defesa cibernética consiste em ações e mecanismos de proteção e defesa das infraestruturas e sistemas vinculadas às TICs essenciais para o ordenamento nacional, de forma a deter ameaças e ataques cibernéticos, garantindo a integridade do ciberespaço e a estabilidade do país.

Esse processo de securitização do espaço cibernético, ou seja, incorporá-lo na agenda securitária ocorreu muito em vista da interdependência entre o setor cibernético e o mundo material, já comentada anteriormente, especialmente com as chamadas infraestruturas críticas, fazendo com que o ciberespaço fosse visto como um desafio aos governos em termos de segurança (Haddad; Binder, 2019). A atenção dada aos Estados para a segurança e a defesa cibernética reside no entendimento de que, com o gradual e acelerado processo de digitalização, os métodos e as estratégias convencionais de segurança e defesa não serão eficazes contra as ameaças cibernéticas (Haddad; Binder, 2019). Dessa forma, muitos governos passaram a investir recursos para o desenvolvimento de capacidades defensivas e ofensivas no setor cibernético (Borghard; Lonergan, 2017).

As infraestruturas críticas podem ser consideradas como as infraestruturas em que seu funcionamento são vitais para a ordem e a estabilidade em uma nação, sendo que a sua destruição ou não funcionamento podem acarretar em um grande efeito sobre a segurança nacional e na capacidade do Estado em operar com normalidade (Saltzman, 2013). Dessa forma, a segurança e a defesa cibernética emergem como questões de especial importância para a manutenção da segurança nacional e internacional, visto que essas ameaças podem colocar em risco não apenas os sistemas informacionais, mas estruturas que impactam a vida de milhões de pessoas. Como consequência, essas ameaças podem colocar em risco dados estratégicos e vitais tanto ao Estado quanto à sociedade (Martins, 2012).

Com isso, a segurança cibernética ganha cada vez mais notoriedade, já que as suas aplicabilidades são cada vez mais importantes para a preservação da harmonia na sociedade. Esse contexto atual em relação ao ciberespaço não é sem fundamento, visto que no próprio relatório *Global Risks Report* (2019), do Fórum Econômico Mundial, os ataques cibernéticos

foram destacados entre os dez maiores riscos globais para a humanidade em termos de impacto para a sociedade global. Alguns casos práticos podem dimensionar melhor os impactos que ataques e incidentes cibernéticos podem ter atualmente. Por isso, será tratado os casos da Estonia, em 2007, o caso *Stuxnet*, em 2010, o caso *BlackEnergy*, em 2015 e o caso *NotPetya*, em 2017.

No ano de 2007, o governo da Estonia mudou a estátua que representava a libertação soviética do país contra os nazistas, retirando o objeto de uma praça central para uma região mais afastada e menos expressiva da cidade, próximo ao cemitério militar de Tallinn (Herzog, 2011). Com a mudança de lugar, houve uma retaliação, e durante seguidos dias ataques de negação de serviço (DDoS) foram perpetrados contra as infraestruturas críticas estonianas, levando à derrubada de importantes sistemas do país, como websites do governo, bancos e websites de partidos políticos (Herzog, 2011). Na época, o governo estoniano responsabilizou a Rússia pelos ataques, mas a atribuição pelas ações não foi oficialmente confirmada, sendo que o governo russo negou qualquer envolvimento. Como coloca Herzog (2011), mesmo que especialistas da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN) não conseguiram encontrar evidencia da participação russa nos ataques, parecia ser de interesse de Moscou que os sistemas estonianos fossem derrubados.

O caso *Stuxnet*, ocorrido em 2010, é tido como um dos mais famosos ataques cibernéticos do século XXI. Ele consistiu na implementação de um *malware* nas facilidades nucleares do Irã de modo a prejudicar o enriquecimento de urânio do país. O ataque obteve sucesso ao fazer com que os rotores de centrifugação funcionassem de maneira anormal, acelerando e reduzindo drasticamente as suas velocidades, causando danos às centrífugas (Valo, 2014). O malicioso programa utilizado no caso *Stuxnet* é considerado de alta sofisticação e foi o primeiro caso em que um ataque cibernético afetou de maneira direta o funcionamento de estruturas físicas, prejudicando o enriquecimento de urânio por parte do Irã. Na verdade, o vírus infectou mais de 60 mil computadores em diversos países, como India, China, Azerbaijão, Coreia do Sul, Malásia, Estados Unidos, Reino Unido, Austrália, Finlândia e Alemanha (Farwell; Rohozinski, 2011).

A sofisticação do programa consistia na sua capacidade de atuar de forma autônoma após a infecção e controlar a frequência e velocidade dos motores das centrífugas. “Então o *Stuxnet* alterou a frequência da corrente elétrica que alimenta as centrífugas, causando a alternação das velocidades entre altas e baixas em intervalos nos quais as máquinas não foram

projetadas" (Farwell; Rohozinski, 2011, p. 24, tradução nossa)[34]. A atuação do *Stuxnet* durou meses, afetando principalmente o programa nuclear iraniano, visto que cerca de 60% das infecções ocorreram no país (Farwell; Rohozinski, 2011).

O caso *BlackEnergy* consistiu nas práticas de um grupo, que realizou operações maliciosas e ficou mundialmente conhecido por suas ações na Ucrânia em 2015. Os procedimentos iniciaram ainda em 2014, quando diversos e-mails foram enviados para companhias de energia e membros do governo ucraniano na tentativa de realizar o chamado *phishing* (Cherepanov; Lipovsky, 2016), em que um *malware* é implantado em um arquivo e ativado quando a vítima clica e/ou executa esse arquivo. Mas foi no ano de 2015 que os ataques cibernéticos obtiveram sucesso, em que os sistemas de três companhias energéticas ucranianas foram penetrados, causando a queda de energia em diversas regiões do país por múltiplas horas (Cherepanov; Lipovsky, 2016).

Os ataques impactaram aproximadamente 225 mil clientes e obrigaram as companhias a operarem as suas facilidades energéticas manualmente, já que seus sistemas digitais estavam derrubados (Lee; Assante; Conway, 2016). O *BlackEnergy* também contou com diversos tipos de ataques cibernéticos, com o objetivo de aumentar as chances de sucesso em atingir o maior número de dispositivos, mesmo que não se saiba exatamente quão diversificado foram as ações (Lee; Assante; Conway, 2016). Sendo assim, interpreta-se que a agressão cometida teve forte impacto no ordenamento regular da Ucrânia, em que centenas de milhares de pessoas tiveram o seu acesso à energia bloqueado, acarretando em prejuízos financeiros e sociais. "Os perpetradores por trás do BlackEnergy causaram o primeiro ato documentado de sabotagem cibernética contra uma grande população civil" (Cherepanov; Lipovsky, 2016, tradução nossa)[35].

Por fim, outro relevante caso cibernético no mundo foi o episódio do *malware NotPetya*, iniciado no ano de 2017, também na Ucrânia, mas que teve efeitos colaterais em outros países como Alemanha, França, Itália, Polônia e Estados Unidos (Krasznay, 2020). O ataque consistiu na inserção de um código maligno, caracterizado como *ransomware*, nos sistemas centrais dos computadores de diversas companhias que impedia a sua inicialização ao criptografar os arquivos do sistema, solicitando um resgate em dinheiro para a liberação (Krasznay, 2020).

---

[34] Texto original: Then Stuxnet alternated the frequency of the electrical current that powers the centrífuges, causing them to switch back and forth between high and low speeds at intervals for which the machines were not designed.

[35] Texto original: The perpetrators behind BlackEnergy have caused the first documented act of cyber sabotage against a mass civilian population.

> Eventualmente, milhares de companhias ucranianas foram atingidas pelo incidente. As vítimas incluem certas infraestruturas críticas ucranianas, incluindo bancos ucranianos, Aeroporto Kiev Borispol, e empresas de energia como a Kvivernergo e Ukrenergo. Mas diversas companhias estrangeiras também reportaram infecções, como a empresa americana de medicamentos Merck, a russa Rosnveft e a húngara OTP Bank na Ucrânia, cujos caixas eletrônicos exibiram imagens da infecção NotPetya por dias. Maior publicidade foi dada para a devastação da A.P. Moller-Maersk. Essa empresa é o 558º maior conglomerado do mundo de acordo com a lista de companhias Forbes Global 2000, sendo uma das maiores empresas de logística do mundo (Krasznay, 2020, p. 486, tradução nossa)[36].

Além disso, outras empresas estrangeiras foram impactadas pelo ataque *NotPetya*, tendo os seus sistemas derrubados por diversos dias e impossibilitando suas operações de maneira regular. Um exemplo foi Mondelez International, multinacional de alimentos que teve as suas operações perturbadas por semanas, resultando em um prejuízo estimado de US$ 100 milhões devido aos ataques (Wan, 2020). De maneira geral, as estimativas globais são de que esse caso gerou um dano total de aproximadamente US$ 10 bilhões em empresas ao redor do mundo (Wan, 2020). Dessa forma, esse ataque cibernético pode ser visto como um dos mais custosos já ocorridos financeiramente, sendo de grande magnitude ao envolver grandes empresas de diversos países.

Os exemplos reais trazidos acima são apenas para ilustrar o potencial destrutivo que crimes e ataques cibernéticos possuem na contemporaneidade, em que a digitalização dos sistemas e processos acabaram aumentando a vulnerabilidade das estruturas de instituições, órgãos governamentais, empresas públicas e privadas, entidades da sociedade civil, etc. Consequentemente, a segurança cibernética e a defesa cibernética tiveram seus patamares elevados em termos da necessidade de promover e direcionar recursos e mecanismos basilares para a sua salvaguarda.

Como coloca o relatório *Global Cybersecurity Outlook 2023*, do Fórum Econômico Mundial, as tecnologias são agora compartilhadas por uma gama de organizações, conectando-as, mas também criando uma dependência e até mesmo uma fragilidade. E isso vai para além das organizações, atingindo também o âmbito das relações entre as nações. Como consequência, o relatório aponta que para a grande maioria dos líderes de organizações e em questões cibernéticas, a instabilidade geopolítica afeta diretamente as estratégias cibernéticas

[36] Texto original: Eventually, thousands of Ukrainian companies were hit by the incident. The victims include certain critical Ukrainian infrastructures, including Ukrainian banks, Kiev Borispol Airport, and energy companies such as Kyivenergo and Ukrenergo. But several foreign companies have also reported infections, such as the American medical company Merck, the Russian Rosnyeft and the Hungarian OTP Bank in Ukraine, whose ATMs displayed the images of the NotPetya infection for days. Most publicity was given to the devastation at A.P. Moller–Maersk. This company is the 558th largest conglomerate in the world according to the Forbes Global 2000 list of companies, one of the largest logistics companies in the world

das organizações e os riscos cibernéticos de diferentes naturezas (Fórum Econômico Mundial, 2023). Por essa perspectiva, é possível ir além e manifestar que o inverso também pode ser verdadeiro, em que os riscos e ameaças cibernéticas, bem como o estabelecimento de determinadas estratégias cibernéticas por organizações e/ou países tem capacidade de produzir efeitos geopolíticos.

Contudo, mesmo com a ênfase e importância dada por organizações internacionais e também por governos nacionais, que assumem o ciberespaço como um domínio capaz de ocasionar insegurança e instabilidade, a grande parte das políticas, diretrizes e estratégias construídas para a proteção do espaço cibernético se dá apenas na dimensão nacional. Se olharmos para esse cenário a partir de uma perspectiva construtivista, temos que os Estados adotam essas posturas com base nas identidades e interesses que possuem em relação ao setor cibernético. Isso porque, como expressa Alexander Wendt (1992), a anarquia atua como condicionante que permite os Estados a tomarem as suas ações, fazendo com que a busca pela segurança e a sua preservação no sistema internacional não seja um processo dado pela estrutura anárquica na qual se encontram, mas sim um processo construído pelos Estados a partir dos seus comportamentos e ações. Nesse sentido, esses comportamentos dependem diretamente da concepção que os Estados possuem tanto de si próprios quanto dos outros, que resultam no processo de formação das suas identidades e dos seus interesses.

Isso significa que o sistema de autoajuda, no qual a obtenção da segurança é o objetivo maior para garantir a sobrevivência do Estado, é construído a partir dos processos e ações conjuntos desses atores, em que a estrutura anárquica além de ser um produto disso, atua de forma a permitir que o sistema de autoajuda prevaleça na política internacional. Na realidade, a anarquia permite também a construção social dos interesses e identidades dos Estados, que as adquire com base na interação coletiva com os demais atores do sistema e as define a partir das situações (Wendt, 1992). Com isso, a autoajuda é vista como uma instituição dentre as várias estruturas de identidades e interesses possíveis na anarquia. Consequentemente, sob o olhar construtivista, os Estados agem e tomam posições diferentes em determinadas situações, a depender do entendimento, identidade e interesse que possuem em relação a isso. Nesse sentido, o próprio poder militar de um país, por exemplo, pode representar diferentes significados para diferentes países, podendo ser considerado uma ameaça para um e não para outro.

Portanto, pode-se interpretar que o sentimento de insegurança surge da percepção e da compreensão que um ator possui e/ou atribui em relação a outro e, dentro da construção dessa percepção, diversos são os fatores que impactam diretamente para a sua formação, como o contexto ideológico, social, econômico e político desses atores, bem como a forma com que

interagem entre si. Para Wendt (1992), são as identidades competitivas ou egoístas que geram a insegurança, sendo que a identificação positiva entre os atores é uma condição necessária para a segurança coletiva. Nesse sentido, a formação de identidades competitivas leva ao dilema da segurança, em que há a predominação da desconfiança entre os atores do sistema internacional, sendo que "as formas de identidades e interesses que constituem tais dilemas, no entanto, são elas mesmas efeitos contínuos da interação, e não exógenas a esta; as identidades são produzidas dentro e por meio da 'atividade situada' (Wendt, 1992, p. 407, tradução nossa)[37].

Essa atividade, ou interação, entre os atores faz com que haja a existência de efeitos constitutivos e uma relação causal. Isso ocorre quando elementos como propriedade, distribuição de poder e disposições são dependentes e existem em virtude das ideias e das interações. Wendt (1999) aponta que isso gera uma relação causal de poder, traçando a analogia que o poder de uma pessoa sobre pessoas escravizadas não existe separadamente da sua relação com pessoas escravizadas. Ou seja, a construção da identidade desse indivíduo é diretamente ligada com a sua interação com pessoas escravizadas, caso contrário, essa identidade não existiria, ou outra identidade seria construída.

Dessa forma, o interesse próprio de um ator é caracterizado pela atitude instrumental em direção ao outro, sendo que esse interesse não é algo intrínseco, mas sim algo formado com base em um conjunto de crenças para satisfazer necessidades que é ativada em relações específicas com o outro, sendo constituída culturalmente (Wendt, 1999). Como consequência, a visão de segurança de um Estado dependerá do processo de identificação de si próprio e do outro, no qual esse processo pode, às vezes, assumir formas hobbesianas (Wendt, 1999). Assim, isso não significa que os Estados irão sempre assumir uma identidade egoísta e enxergar o outro como uma possível ameaça a sua sobrevivência, pois a construção dessa identidade e da visão de um ator sobre o outro depende de muitos fatores endógenos, não determinados exclusivamente pela estrutura na qual se encontram. " Se Estados começarem a pensar como "Realistas" então é isso o que eles vão ensinar um para o outro, e esse é o tipo de anarquia que eles vão criar" (Wendt, 1999, p. 332, tradução nossa)[38].

Em linha com a visão construtivista para as relações internacionais, a teoria da segurança ontológica relaciona a segurança com a percepção que um ator possui de si mesmo com o mundo ao seu redor. A teoria da segurança ontológica nasceu com o sociólogo britânico

[37] Texto original: The forms of identity and interest that constitute such dilemas, however, are themselves ongoing effects of, not exogenous to, the interaction; identities are produced in and through "situated activity".

[38] Texto original: If states start out thinking like ``Realists" then that is what they will teach each other to be, and the kind of anarchy they will make

Anthony Giddens em 1991, quando se referiu a segurança como ‘sendo’ e não como ‘sobrevivência’ (Kinnvall; Mitzen, 2016). Diferente da concepção tradicional de segurança, a segurança ontológica leva em consideração diferentes dinâmicas da situação e relação entre os atores para compreender os motivos pelos quais esses atores entram ou não em rotas de conflito e violência. Nesse sentido, a segurança ontológica tem como enfoque as incertezas, ansiedades e capacidades dos atores no sistema internacional (Kinnvall; Mitzen, 2016).

Isso significa que essa teoria busca investigar as razões pelas quais indivíduos, grupos e Estados experienciam a insegurança a partir do entendimento da concepção de identidade desses atores, de forma a compreender os sentimentos e sensações que os levam a se comportar de determinada maneira. Isso porque, para a segurança ontológica, é preciso considerar o estado psicológico e até emocional no qual o ator se encontra, visto que esse fator subjetivo influencia as tomadas de decisão e os comportamentos adotados.

> Um enfoque na segurança ontológica coloca ênfase no que está nas histórias ou narrativas que contamos para nós mesmos sobre nossas relações com os outros. É uma chamada para investigar as razões cognitivas e afetivas do por que indivíduos, grupos e até Estados experienciam a insegurança e a ansiedade existencial e para explorar as respostas emocionais a esses sentimentos (Kinnvall; Mitzen, 2016, p. 3, tradução nossa)[39].

Como consequência, a ordem e a estabilidade não são vistas como algo estático, mas como aspectos da segurança que estão em constante mudança por serem o produto da auto percepção do ator e da sua interação com os demais (Freire, 2020). Nesse sentido, o aumento da percepção de incerteza e insegurança pode aprofundar os conflitos no mundo político (Kinnvall; Mitzen, 2016). E, seguindo a mesma lógica, se a percepção dos atores é de confiança e de previsibilidade, interpreta-se que a sensação de segurança e estabilidade irá prevalecer entre os atores envolvidos. Além disso, como as percepções sobre si e os outros não são dadas pela estrutura e sim construídas socialmente, o que hoje é visto como inofensivo ou que não gera preocupações para um ator, pode se tornar uma ameaça amanhã e vice-versa.

A segurança ontológica, portanto, tem um olhar sobre a habilidade dos atores em preservarem as suas identidades, pois diferente da segurança física, que se importa somente com a sobrevivência, a segurança ontológica diz respeito ao ser (Lupovici, 2023). Dessa forma, as emoções também são levadas em consideração, como questões que envolvem confiança,

[39] Texto original: A focus on ontological security puts the emphasis on what goes into the stories or narratives we tell ourselves about ourselves and our relations to others. It is a call to investigate cognitive and affective reaseons why individuals, group and even states experience insecurity and existential anxiety and to explore the emotional responses to these feelings

orgulho, visto que a insegurança produz emoções contrárias como desconfiança, frustração, humilhação, entre outros (Lupovici, 2023). Assim, projetando as perspectivas construtivistas e da segurança ontológica para um nível macro, entende-se a segurança internacional como um processo de confecção de estabilidade e redução de ameaças entre os principais atores do sistema internacional, os Estados, a partir da construção das suas identidades e da sua interação de modo a prevenir conflitos e promover relações pacíficas.

Já no que tange ao ciberespaço, interpreta-se que os atores nesse domínio ainda estão em uma fase inicial de compreensão do que efetivamente representa a segurança no ambiente cibernético e como podem lidar com as ameaças possibilitadas por ele. Isso significa que estamos em um momento inicial do processo de construção das identidades e dos interesses dos atores nesse espaço, em que a sua exploração e total concepção das suas capacidades está em uma fase de descobrimento e desenvolvimento (De Rê, 2021). Isso porque o entendimento dos Estados sobre o ciberespaço e como protegê-lo difere, gerando múltiplas interpretações e conceitos sobre o espaço cibernético e o que configura a sua segurança e defesa. Nesse sentido, a própria securitização do ciberespaço é um produto de como os atores, especialmente estatais, enxergam esse espaço e as possibilidades positivas e negativas que ele pode proporcionar nas diferentes áreas econômicas, políticas, culturais e sociais.

Como coloca Amir Lupovici (2023), pensar a segurança e a defesa cibernética a partir das lentes da segurança ontológica fornece importantes compreensões por conta de três aspectos principais. Primeiro, porque as tecnologias cibernéticas desafiam as habilidades dos Estados em manter as suas narrativas e senso de casa, algo que está diretamente relacionado com o estado de insegurança ontológica; segundo, as incertezas criadas pelas tecnologias cibernéticas dificultam os Estados em prover um ambiente estável para que os indivíduos possam realizar suas rotinas; terceiro, as tecnologias cibernéticas desafiam os Estados em monopolizar o papel de fornecedor da segurança ontológica para a população, pois elas criam meios alternativos para os indivíduos buscarem as suas necessidades para se sentirem seguros (Lupovici, 2023).

Ademais, todas as interpretações, identidades, entendimentos e interesses que os atores possuem em relação ao ciberespaço podem variar conforme o significado social que os atores atribuírem para esses aspectos, sendo que o que pode ser um motivo de ansiedade e insegurança para determinado Estado em relação ao espaço cibernético, pode não ser para outro. Em um exemplo hipotético, a criação de um sofisticado *spyware* por Israel pode gerar uma grande tensão para a Palestina, ao mesmo tempo que pode ser visto com neutralidade pelos Estados Unidos, que pode até mesmo ter o interesse em adquirir tal tecnologia.

Atualmente, por não existir uma convenção internacional reconhecida pelas nações sobre o ciberespaço, os Estados são os principais responsáveis por confeccionar documentos governamentais estratégicos sobre o ciberespaço e a segurança e a defesa cibernética. Esses documentos podem ser considerados como a fonte primária da expressão dos Estados sobre o entendimento que possuem sobre esse domínio. Além disso, elucidam sobre quais são as medidas e ações consideradas estratégicas pelos países para garantir a proteção do seu espaço cibernético. Ocorre que cada país possui sua própria concepção sobre esse domínio e, assim, são enxergadas diferentes possibilidades, tanto para projeção de poder, quanto para manter a estabilidade e a ordem interna, que esse domínio pode proporcionar.

Dessa forma, a adoção de determinada concepção, identidade e interesse sobre e para o ciberespaço por um país, pode gerar ansiedades e incertezas para outro, já que a concepção e interpretação deste pode diferir do primeiro. Sendo assim, emerge a importância de olhar para como o direito internacional afeta e pode ser aplicado ao domínio cibernético, de forma a observar como os dispositivos atuais respondem às necessidades das interações entre os atores estatais no que diz respeito ao ciberespaço, bem como avaliar como o cenário da falta de uma convenção ou tratado internacional para o espaço cibernético pode produzir incertezas e levantar questionamentos entre os atores.

3.4 A AUSÊNCIA DE UMA REGULAMENTAÇÃO INTERNACIONAL PARA O CIBERESPAÇO

O direito internacional contemporâneo tem como seu fundamento a Carta das Nações Unidas, elaborada em 1945 pela comunidade internacional. Desde a sua criação, desafios e obstáculos foram emergindo nas relações internacionais de forma que os Estados foram sendo compelidos a aprimorar as normas internacionais. Assim, diversos tratados foram firmados ao longo do século XX, como as Convenções de Genebra de 1949 e seus Protocolos Adicionais, e início do século XXI, como a Convenção para Proteção de Todas as Pessoas contra os Desaparecimentos Forçados de 2007, abordando sobre temas específicos e construindo regulamentações e dispositivos para estabelecer padrões de conduta e boas práticas para os Estados. Nesse intervalo de tempo, como visto anteriormente, o ciberespaço foi criado e seu uso disseminado por meio das TICs. E, por se tratar de um ambiente capaz de possibilitar as ameaças e os danos comentados, bem como de afrontar princípios tradicionais como o da soberania, surge, por consequência, o questionamento da aplicabilidade do direito internacional para o espaço cibernético.

Essa indagação está diretamente ligada com o impacto das operações cibernéticas no mundo atual em conjunto com a percepção do ciberespaço como uma “terra sem lei” no que tange ao âmbito internacional, já que as normas e regras vigentes no direito internacional não abordam especificamente sobre o espaço cibernético e as suas particularidades. Talvez o primeiro questionamento que surge diz respeito à jurisdição e territorialidade, visto serem os elementos nos quais o Estado tem a prerrogativa de estabelecer o seu controle e autoridade.

O problema em relação ao ciberespaço é justamente definir a sua jurisdição sobre a dimensão não-física, onde dados e informações fluem de forma a ignorar a existência de fronteiras físicas. E essa característica da extraterritorialidade do ciberespaço acaba sendo um problema ainda maior, na questão da jurisdição, quando pensamos no uso da computação em nuvem, já que não há nenhuma localização física para os dados, que podem cruzar barreiras nacionais e serem processados em diversos Estados simultaneamente, levantando dúvidas sobre qual Estado seria responsável se um crime cibernético fosse cometido através da computação em nuvem (Kittichaisaree, 2017).

O ponto trazido aqui é como o direito internacional pode e consegue lidar em uma situação hipotética como essa e quais premissas deveriam ser utilizadas. Como expressa François Delerue (2019), um obstáculo em relação à aplicabilidade das normas internacionais para o espaço cibernético - e as operações que ocorrem nele e por causa dele – é a dificuldade dos Estados em discutir e acordar sobre esse assunto. Um exemplo empírico dessa dificuldade está na criação e nos trabalhos dos sucessivos Grupos de Especialistas Governamentais da ONU (GGE) estabelecidos sobre o assunto nos anos de 2004, 2010, 2013, 2015, 2017 e 2021. Nem todos os GGEs produziram relatórios finais, o que já indica a complexidade de consenso entre os participantes.

Os relatórios produzidos em 2013 e 2015 foram significativos por terem sidos os primeiros a reconhecerem a aplicabilidade do direito internacional e da Carta das Nações Unidas para o ciberespaço (Delerue, 2019). Esses relatórios possuem apenas caráter recomendatório, mas demonstram o interesse de um grupo de Estados que o ciberespaço seja compreendido como um domínio que precisa ser regulado de alguma forma, mesmo que pelas regras já existentes. No entanto, o reconhecimento da aplicabilidade não responde às perguntas sobre como as regras devem ser aplicadas e se elas são capazes de abranger as especificidades e as complexidades que o ciberespaço propicia nas relações internacionais. Ou seja, isso significa que a interpretação das normas vigentes entra em jogo e não parece ser um consenso fácil de ser atingido pelos atores estatais.

O aspecto da interpretação foi o motivo pelo qual o GGE de 2017 não produziu um relatório final, pois os participantes não conseguiram acordar sobre o parágrafo 34, que detalhava sobre como o direito internacional deveria ser aplicado pelos Estados no uso de TICs, demonstrando a inabilidade dos participantes em encontrar concordância nas especificidades das normas para a sua implementação ao setor cibernético (Delerue, 2019). A declaração do especialista governamental de Cuba ilustra bem o porquê do posicionamento contrário adotado por alguns países.

> Eu devo registrar nossa séria preocupação sobre a pretensão de alguns, refletida no parágrafo 34 do rascunho do relatório final, de converter o ciberespaço em um teatro de operações militares e de legitimar, nesse contexto, ações de força punitivas unilaterais, incluindo a aplicação de sanções e até ações militares por Estados que reivindicam serem vítimas do uso ilícito de TICs (Cuba, 2017, s.p, tradução nossa)[40].

Além disso, ele enfatiza que:

> Estabelecer como precedente essa perigosa reinterpretação das normas do direito internacional e da Carta das Nações Unidas seria um golpe fatal para a segurança coletiva e a arquitetura da manutenção da paz estabelecida na Carta das Nações Unidas. A "Lei da Selva" não pode ser imposta, em que os interesses dos Estados mais poderosos prevaleceriam sempre em detrimento dos mais vulneráveis. (Cuba, 2017, s.p, tradução nossa)[41].

Fica claro, a partir dessa declaração, que a posição cubana é de reconhecimento de que normas precisam existir e serem aplicadas ao ciberespaço, mas normas específicas que levem em considerações as particularidades desse domínio. Isso porque na visão cubana, simplesmente implementar as normas internacionais tradicionais seria estabelecer a "lei da selva" para o espaço cibernético, onde basicamente cada um poderia fazer o que bem entendesse e, por consequência, os mais fortes teriam vantagens para impor as suas vontades. Entretanto, o GGE de 2017 não chegar ao consenso não significa automaticamente um fracasso, mas sim uma demonstração que a comunidade internacional tem debatido sobre o tema e que um processo de negociação e adaptação está em desenvolvimento (Delerue, 2019).

---

[40] Texto original: I must register our serious concern over the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs.

[41] Texto original: To establish as a precedent this dangerous reinterpretation of the norms of international law and the Charter of the United Nations would be a fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations. The "Law of the Jungle" cannot be imposed, in which the interests of the most powerful States would always prevail to the detriment of the most vulnerable.

Como consequência, em 2019 mais um GGE sobre o tema teve início, produzindo um relatório final no ano de 2021. O Grupo foi intitulado como Grupo Governamental de Especialistas sobre a Promoção do Comportamento Responsável do Estado no Ciberepsçao no contexto da Segurança Internacional, tendo como objetivo principal dar continuidade aos estudos e à negociação para promover um entendimento comum e medidas cooperativas no que tange à esfera do ciberespaço no âmbito da segurança internacional. O relatório reafirma que as normas, regras e princípios do direito internacional devem valer para o espaço cibernético, de modo a refletir no estabelecimento de um padrão de comportamento responsável dos Estados nesse domínio (Organização das Nações Unidas, 2021).

Dessa forma, no entendimento do Grupo, o uso de TICs por parte dos atores estatais deve seguir - e estar vinculado com - diretrizes e regras para que conflitos sejam prevenidos e comportamentos que promovem a paz e a estabilidade sejam tomados (Organização das Nações Unidas, 2021). Assim, o relatório atualiza as normas estabelecidas no ano de 2015, estabelecendo, por exemplo, que os Estados devem cooperar no desenvolvimento e uso das TICs; que não devem permitir conscientemente que seu território seja utilizado para ações cibernéticas internacionais hostis; que devem respeitar os princípios dos direitos humanos no âmbito cibernético, entre outros (Organização das Nações Unidas, 2021).

A relevância dos relatórios produzidos pelas Nações Unidas nos últimos anos está tanto na reafirmação da aplicabilidade dos princípios das responsabilidades do Estado perante o direito internacional no contexto cibernético, quanto no reconhecimento da aplicabilidade do direito internacional para o ciberespaço (Wang, 2021). Contudo, para além dessa reafirmação e de apontar a importância da validade dos princípios da Carta das Nações Unidas, o relatório de 2021 também expressa a importância de um debate mais aprofundado sobre como adotar de forma apropriada esses princípios para o âmbito cibernético. Sendo assim, o Grupo manifesta:

> Sem prejuízo para o direito internacional existente e para o desenvolvimento adicional do direito internacional no futuro, o Grupo reconhece que a discussão continuada e o compartilhamento de visões pelos Estados, coletivamente nas Nações Unidas sobre como especificamente regras e princípios do direito internacional são aplicáveis para o uso de TICs pelos Estados é essencial para o aprofundamento de entendimentos comuns, evitando desentendimentos e aumentando a previsibilidade e a estabilidade. Tais discussões podem ser informadas e apoiadas em compartilhamentos de visões bilaterais e regionais entre os Estados (Organização das Nações Unidas, 2021, p. 18, tradução nossa)[42].

[42] Texto original: Without prejudice to existing international law and to the further development of international law in the future, the Group acknowledged that continued discussion and exchanges of views by States, collectively at the United Nations on how specific rules and principles of international law apply to the use of ICTs by States is essential for deepening common understandings, avoiding misunderstandings and increasing

Indiretamente, isso acaba sendo um reconhecimento da comunidade internacional de que ainda há dúvidas pelos Estados sobre como determinar exatamente a aplicabilidade das regras e princípios já existentes, atestando que na prática há a ausência de uma regulamentação internacional para lidar especificamente com o ciberespaço e os seus efeitos sobre a segurança internacional. Consequentemente, ações cibernéticas internacionais podem ficar sem respostas simplesmente pelos atores estatais não saberem e não possuírem uma estrutura normativa para se apoiarem. Um exemplo prático foi o vazamento de documentos do partido Democrata nos EUA perpetrados por hackers russos no ano de 2015 e 2016. Ocorre que as ações realizadas parecem ficar em um limbo sem respostas, em que não se tem definição se representaram uma violação da soberania estadunidense, ou uma intervenção ilegal sob o direito internacional, sendo que até mesmo atribuir responsabilidade por parte do governo russo pelos atos é algo dificultado (Schmitt, 2017).

Interpreta-se, portanto, que a ausência de regulamentação internacional para o ciberespaço permite a existência de uma espécie de zona cinzenta no direito internacional, em que as relações interestatais ocorridas e/ou afetadas pela utilização do espaço cibernético não possuem diretivas nem preceitos específicos a serem seguidos. Consequentemente, algumas questões se tornam vagas ou abstratas, como a já discorrida violação da soberania, em que fica claro que uma ação cibernética, de um Estado para outro, que tem consequências físicas e causa danos materiais configura um desrespeito à soberania. Esse esclarecimento está presente também no Manual de Tallinn 2.0 (2017), documento elaborado por especialistas da OTAN que versa sobre o ciberespaço no âmbito do direito internacional. Agora, quando se trata de uma ação em que há apenas a alteração de dados ou sistemas, que pode afetar o funcionamento de operações digitais, não se tem uma definição clara se isso configura uma violação de soberania.

Dessa forma, a interpretação dos atores acaba sendo o fator definidor sobre como determinada ação ou ataque se caracteriza e qual deve ser a resposta utilizada por quem sofre a agressão. Com isso, operações cibernéticas hostis, que não causam danos físicos e não são destrutivos, conduzidos dentro do território de outro Estado são beneficiadas pelas incertezas que cercam o conceito legal de violação da soberania (Schmitt, 2017). Outro ponto que fica sem resposta objetiva é a responsabilização de um ato, visto que há uma grande dificuldade em saber e encontrar quem realizou determinada ação cibernética. Isso ocorre em vista da facilidade

predictability and stability. Such discussions could be informed and supported by regional and bilateral exchanges of views between States.

do anonimato no mundo virtual e da possibilidade do envolvimento de múltiplos atores, que acaba criando obstáculos para a real identificação de quem realmente está por trás de um ataque ou incidente cibernético. Sendo assim, há também uma zona cinzenta no que diz respeito à atribuição, sob o direito internacional, da responsabilidade estatal para ações cibernéticas, especialmente quando essas ações são conduzidas por atores não-estatais, mas que de alguma forma são ligadas à figura do Estado (Schmitt, 2017).

Esse problema também acaba se estendendo para como um Estado deve reagir e utilizar o uso da força em casos de operações realizadas no ciberespaço. Isso porque como coloca o Artigo 2 da Carta das Nações Unidas, os Estados devem evitar se utilizar da força contra a integridade territorial e independência política de outro, sendo que em casos de agressões os Estados possuem o direito de se defenderem individualmente ou coletivamente, conforme expressa o Artigo 51 da Carta (Organização das Nações Unidas, 1945). Dessa forma, ataques cibernéticos que causam danos físicos e que há a identificação do agressor, conseguem ser enquadrados como atos que violam as normas internacionais estabelecidas e, assim, o uso da força como resposta da vítima pode ser legitimado.

No entanto, se as ações no ciberespaço forem de roubo ou alterações de dados e informações, espionagem e/ou sabotagem de sistemas digitais em que não há danos materiais diretos, e, mais do que isso, se não for possível atribuir responsabilidade, tem-se um cenário no qual a vítima não tem amparo legal para responder com o uso da força. Ou seja, pode-se dizer que a situação atual é que a comunidade internacional aceita que o direito internacional seja aplicado ao espaço cibernético, mas quais princípios e regras específicas devem ser reivindicadas e como elas devem ser implementadas requer um acordo adicional dos Estados (Wang, 2021). Como consequência, a questão do uso ou não uso da força também recai para um aspecto interpretativo por parte dos atores. Como expressa Michael Schimitt (2017, p. 15, tradução nossa)[43]:

> [...] a chave para entender o direito de autodefesa no contexto cibernético é o significado do termo "ataque armado", que é indefinido no direito internacional. A visão prevalecente é que, enquanto todos os ataques armados são necessariamente usos da força, nem todos os usos da força são qualificados como ataques armados.

Dessa forma, a aplicabilidade do direito internacional para o domínio cibernético enfrenta desafios, talvez desafios semelhantes – em suas devidas proporções e particularidades

[43] Texto original: [...] the key to understanding the right of self-defense in the cyber context is the meaning of the term "armed attack" which is undefined in international law. The prevailing view is that, while all armed attacks are necessarily uses of force, not all uses of force qualify as armed attacks.

– dos enfrentados quando os domínios aéreos e espaciais se tornaram palco para a realização de operações militares e civis com consequências destrutivas entre atores. Para esses dois domínios, contudo, foram criadas convenções pela comunidade internacional sobre como os atores devem se portar e conduzir suas ações no ar e no espaço, de forma a respeitar regras e princípios que visam ordenar e regular as atividades nesses domínios. Sendo assim, levanta-se o questionamento se o ciberespaço também necessita de uma regulamentação internacional própria, de forma a construir uma governança com preceitos e diretrizes apropriadas para as especificidades que o ciberespaço possui. E é isso que será abordado de forma mais aprofundada nos próximos capítulos.

3.5 CONSIDERAÇÕES DO CAPÍTULO

Este capítulo serviu para abordar sobre o ciberespaço de maneira mais aprofundada, de forma a entender que as suas características produzem diferentes efeitos nas relações internacionais. Por se tratar de um domínio, o espaço cibernético tem a capacidade de possibilitar a projeção de poder pelos atores, mas por ser diferente dos domínios tradicionais, essa projeção não se baseia majoritariamente em *hard power*, mas também em *soft power*, já que as capacidades cibernéticas permitem que o fluxo de dados e informações consigam influenciar na tomada de decisões dos atores. E não apenas por isso, mas também pelo ciberespaço se mostrar ser um ambiente no qual a coerção e a dissuasão não são as estratégias mais eficazes de demonstração de poder e fazer com um ator constranja outro a fazer aquilo que tem interesse.

Sendo assim, se é possível projetar poder por meio do ciberespaço, emerge a necessidade de ter meios para se proteger ciberneticamente, de forma a atenuar as ameaças e as ações hostis que podem ser perpetradas nesse domínio. Com isso, a segurança e a defesa cibernética são postas como de grande relevância para a segurança e a defesa nacional pelos Estados, compreendendo a necessidade de criar diretrizes e mecanismos para se protegerem no âmbito cibernético, cada vez mais interdependente com as infraestruturas e sistemas vitais para o ordenamento social de uma nação. Contudo, por ser algo novo, esses atores ainda estão em fase de assimilação sobre o que a segurança e a defesa cibernética efetivamente significam e como podem conceituá-las.

Essa dificuldade de entendimento comum reverbera para o contexto global, em que há a ausência de uma regulamentação internacional para tratar sobre o ciberespaço e os seus efeitos sobre a segurança internacional. Foi possível perceber que essa ausência é um reflexo da

divergência entre os Estados sobre como o ciberespaço deve ser regido pelo direito internacional, em que as particularidades desse domínio, especialmente no que diz respeito à sua dimensão não física, acabam desafiando a aplicabilidade de princípios e normas internacionais. Dessa forma, interpreta-se o cenário atual como de incertezas e urge a necessidade de avaliar se o estabelecimento de um modelo de governança tem a capacidade de diminuir essas incertezas e criar padrões normativos e de comportamento para serem seguidos pelos Estados, que hoje tomam as suas ações cibernéticas sem o receio de punições.

4 A GOVERNANÇA GLOBAL PARA O CIBERESPAÇO

A ausência da governança global do espaço cibernético propicia que caminhos ou certos modelos possam ser pensados e/ou aplicados na sua construção e implementação. Na realidade, existem atores, como no caso dos Estados Unidos, que enxergam a situação atual como uma espécie de governança. Porém, ela se dá de maneira descentralizada e envolvendo múltiplos atores com relevância e atribuições distintas. Dessa forma, é preciso entender quais modelos de governança global estão sendo discutidos pela comunidade internacional e pela academia para serem estabelecidos, de modo a identificar as suas características para posteriormente ser possível realizar uma análise crítica sobre os seus fenômenos.

Por isso, este capítulo apresenta os dois principais modelos em voga hoje nas discussões sobre a governança global do ciberespaço: o modelo *multistakeholder* e o modelo multilateral. Serão expostas as características e as particularidades de cada modelo, elucidando sobre os atores que os compõe e a forma de governar de ambas, de modo a esclarecer as suas distinções e semelhanças. Em segundo momento, este capítulo irá explicitar as posições e as concepções de Estados Unidos, China e Rússia quanto aos modelos mencionados. Para isso, serão analisados os principais documentos governamentais desses países que mencionam sobre o assunto, selecionados com base nas suas relevâncias em termos estratégicos e na constatação de que versam sobre o tema. Isso significa que outros documentos governamentais de grande importância estratégica foram deixados de lado na análise, por não tratarem sobre a governança global do ciberespaço em suas disposições.

Além disso, serão evidenciados discursos e declarações de autoridades e chefes de Estados que expressam as suas visões sobre o assunto, demonstrando a correlação entre as declarações e aquilo que está exposto nos documentos. Ressalta-se que o objetivo deste capítulo é somente apresentar o que esses três países expressam sobre o assunto, revelando as suas considerações e posicionamentos frente ao fenômeno da governança global do espaço cibernético, deixando para que uma análise crítica seja feita no capítulo seguinte.

4.1 OS MODELOS “MULTISTAKEHOLDER” E “MULTILATERAL” DE POSSÍVEL GOVERNANÇA DO CIBERESPAÇO

Novos graus de complexidades foram incoporados na política internacional, muito por conta do ciberespaço, especialmente por causa da Internet. Junto com isso, emergiu uma pergunta nas discussões internacionais: quem governa a Internet? Estamos em um momento em

que essa pergunta ainda não possui uma resposta objetiva, mesmo com a enorme relevância que essa ferramenta tem para a economia mundial e para a sociedade internacional. Ao fim e ao cabo, não existe um único ator que controla a Internet, e o ciberespaço, de maneira integral, sendo que por desenho e estrutura, há uma multiplicidade de redes controladas por organizações privadas e públicas que compõem esse controle (Sahel, 2016).

Isso significa que há uma descentralização, pelo menos em teoria, sobre o comando do domínio cibernético em nível global, resultando na ausência de uma autoridade central ou uma regulamentação internacional, como visto nos capítulos anteriores. Dessa forma, há o envolvimento de múltiplos atores na coordenação de recursos e políticas para o ciberespaço global, em especial a Internet, fazendo que com muitos autores enxerguem isso como um modelo *multistakeholder* de governança (Calderaro, 2021; Canabarro; Gonzales, 2018; Raymond; Denardis, 2015; Hofmann, 2020). Esse tipo de arranjo se caracteriza pela participação de atores não-estatais e estatais, públicos e privados, em que cada um possui funções e responsabilidades específicas na condução de funções técnicas e processos que mantém a operacionalidade do espaço cibernético.

Como expressa Mark Raymond e Laura DeNardis (2015), o modelo *multistakeholder* consiste em classes de atores engajados em uma governança comum no que diz respeito a questões de natureza pública e que se configura por relações de autoridade poliárquicas compostas por certas regras de procedimento. Dessa forma, o *multistakeholderism* abrange uma gama de atores que possuem certa autoridade em processos políticos globais, em que atores não estatais como entidades privadas, sociedade civil, empresas, organizações não-governamentais atuam de maneira deliberada e paralelamente ao Estado (Jongen; Scholte, 2021).

Sendo assim, se tratando especificamente da Internet, os conteúdos e os dispositivos de computação na qual nós, usuários, temos acesso e estamos expostos são apenas a superfície de uma grande rede de infraestruturas, serviços e instituições que deixam a Internet operacional, em que apesar da natureza privada e as vezes autônoma desses componentes de rede, uma coordenação global é necessária para manter a funcionalidade dessa ferramenta (DeNardis; Raymond, 2013). Como consequência, os atores que afetam esse arranjo de coordenação e controle podem ser caracterizados como possuindo a capacidade de constranger e/ou permitir comportamento no ambiente virtual e a capacidade de produzir efeitos intencionais (Domanski, 2013). Ou seja, os atores podem ser considerados como "governantes" ao serem responsáveis pelas tomadas de decisão na construção e na implementação de políticas e diretrizes no ambiente cibernético.

Nesse caso, uma pergunta mais pertinente do que quem controla a Internet é como ela deveria ser controlada (Sahel, 2016). A primeira vez que o modelo *multistakeholder* foi citado e, de certa forma, reconhecido no âmbito internacional em relação à Internet, foi no primeiro Grupo de Trabalho sobre a Governança da Internet da ONU (WGIG), que produziu um relatório publicado no ano de 2005. No documento, o Grupo define a governança *multistakeholder* da Internet como "[...] o desenvolvimento e a aplicação por governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios, normas, regras e processos de tomadas de decisão e programas compartilhados que moldam a evolução e o uso da Internet" (WGIG, 2005, p. 4, tradução nossa)[44].

Na prática, o *multistakeholderism* muitas vezes é elevado mais como um valor do que uma abordagem para atingir objetivos de interesse público, como manter a estabilidade e a segurança da Internet, visto que para manter a operacionalidade da Internet são necessárias diversas tarefas de coordenação e elaboração de políticas e não necessariamente os *stakeholders* envolvidos são os mais apropriados para cada função de manutenção dessa operacionalidade (DeNardis, Raymond, 2013). Ademais, com a participação de diversos atores, é possível também questionar o aspecto da legitimidade deles ao ter as suas atribuições no gerenciamento da principal ferramenta do ciberespaço global. Nesse sentido, é importante olhar quem são esses atores e o que eles representam.

Mas antes, é preciso enfatizar que, neste trabalho, argumenta-se que esse modelo não corresponde a uma forma de governança global. Esse ponto será discutido de maneira mais profunda e crítica no capítulo seguinte, mas por enquanto, destaca-se que o conceito tradicional de governança definido por Rosenau (1992) prevê a construção de uma conformidade e uma ordem, sendo que apesar de o modelo *multistakeholder* englobar organizações e estruturas formais e informais, emitindo diretivas, fazendo demandas e até mesmo determinando certas regras ou limitações, elas se concentram no âmbito técnico, em que regras no âmbito político sobre o comportamento dos Estados, por exemplo, continuam sem uma regulamentação formal específica.

Outra premissa que o conceito tradicional de governança exige é a legitimidade, mesmo que de forma indireta, sendo que, como veremos mais adiante, algumas entidades reguladoras da Internet hoje são questionadas em relação isso. Isso ocorre porque não é possível ignorar o elemento do interesse das entidades envolvidas, privadas ou não, que tem suas próprias

[44] Texto original: [...] the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

motivações e que, consequentemente, tendem a criar narrativas sobre como é importante manter o modelo *multistakeholder*, para que seja visto e entendido como uma solução para os desafios complexos que existem para governar a Internet (Hofmann, 2020).

Dessa forma é preciso olhar para quem são esses atores, capazes de influenciar e, de certa forma, modelar o espaço cibernético a partir de suas ações ou decisões, sejam elas integradas ou autônomas. Assim, toda a estrutura e a arquitetura política do ciberespaço deve ser levada em consideração, isso porque estamos falando de um ambiente criado a partir da existência e do funcionamento de tecnologias e equipamentos. Dessa forma, fatores como a infraestrutura, os protocolos técnicos, os sistemas digitais, tanto *hardware* quanto *software*, e a sua aplicação impactam na lógica de funcionamento, no controle, no domínio e na forma de utilização do ciberespaço, que pode ser tendenciada a partir dos interesses dos grupos de atores que possuem autoridade e influência sobre esse espaço.

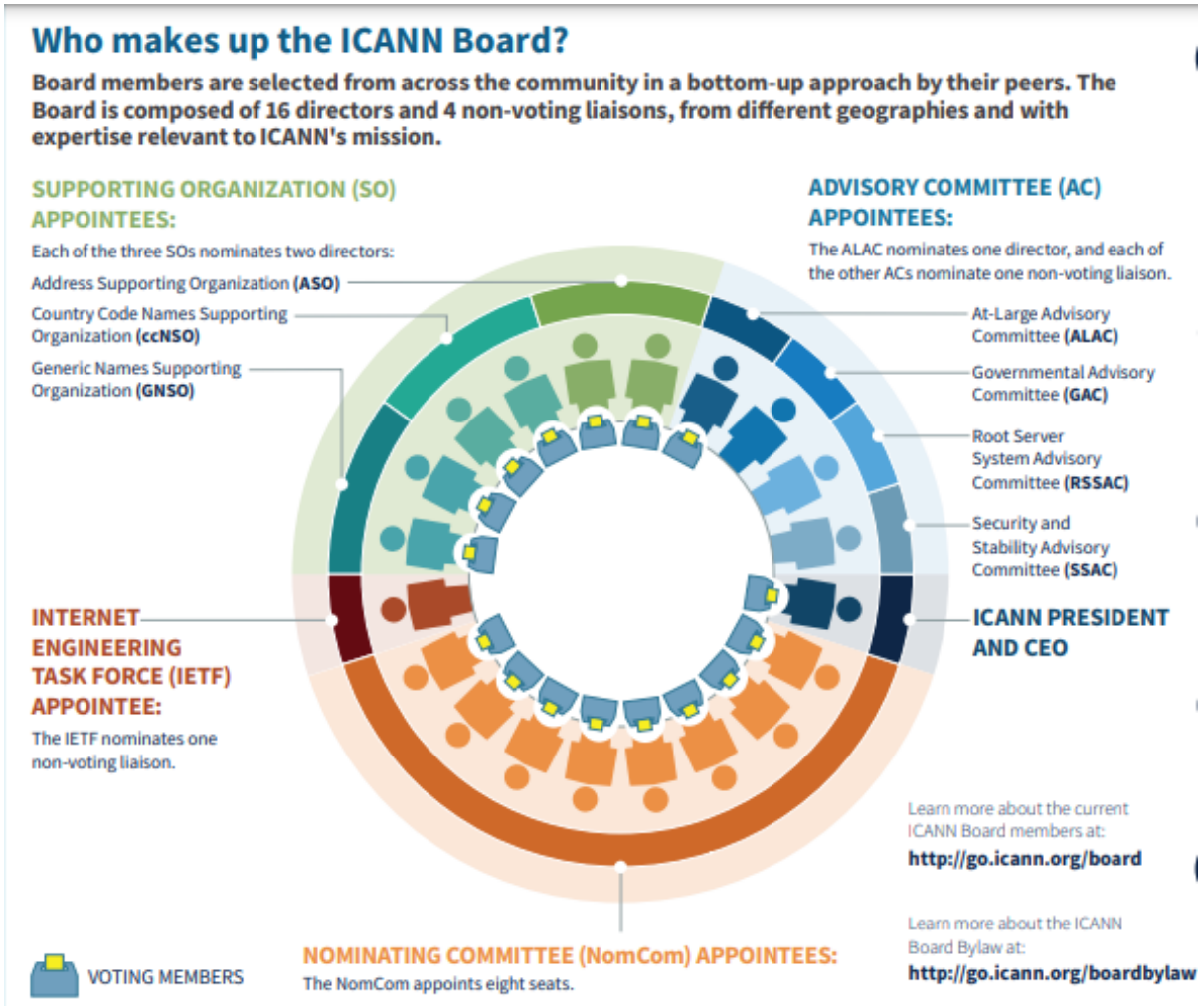
Como colocam Raymond e DeNardis (2015), o ecossistema de gerenciamento da Internet pode ser dividido em seis áreas: (i) controle dos recursos críticos; (ii) estabelecimento de padrões; (iii) coordenação de acessos e interconexões; (iv) governança da cibersegurança; (v) papel político dos intermediários das informações e (vi) aplicação de direitos de propriedade intelectual. Sendo assim, existem distintas camadas e funções que englobam a coordenação e a administração dessa ferramenta, em que muitas vezes a ligação do caráter técnico exigido com o caráter político da tomada de decisões levantam indagações sobre aspectos como prestação de contas, transparência e supervisão da ampla gama de organizações e empresas que participam ativamente desse ecossistema (Raymond; DeNardis, 2015).

Dentro dessas seis áreas, variados atores executam as suas ações e este trabalho não tem a pretensão de se estender nas atividades específicas que cada um realiza. Contudo, alguns acabam tendo maior destaque por conta das atribuições de grande relevância e influência que possuem, como é o caso da Corporação da Internet para a Atribuição de Nomes e Números (ICANN) e a Força-Tarefa de Engenharia de Internet (IETF). A IETF é uma organização internacional composta por indivíduos e organizações que atuam com o objetivo de desenvolver padrões e propor soluções relacionados à utilização da Internet, de forma a aprimorar essa ferramenta. A ICANN, por sua vez, é uma das principais entidades no que concerne ao gerenciamento da Internet em nível global, por ser responsável por determinar e atribuir o Sistema de Nomes e Domínios (DNS). Assim, a organização tem a autoridade de governar a raiz da Internet, incluindo funções como a coordenação da atribuição dos nomes e domínios, dos endereços de protocolos, da porta de protocolo e números de parâmetros, a coordenação da

operação e evolução do sistema do servidor de nomes raiz do DNS e das políticas de desenvolvimento (Becker, 2019).

O DNS pode ser considerado como um elemento chave na estrutura do ciberespaço global, já que é responsável pela identificação de sítios na web, como por exemplo o ".net" ou o ".br", sendo que ele serve como um sistema de indexação hierárquico em que o topo é chamado de raiz (Canabarro; Gonzales, 2018). Além disso, a ICANN também contém diferentes comitês consultivos, que não possuem autoridade legal e têm como função realizar recomendações a partir dos estudos e descobertas realizados pelos membros dos comitês (Becker, 2019). A figura a seguir, disponibilizada pela própria ICANN, mostra como a estrutura da organização está desenhada, em relação aos diferentes setores e o peso de participação dos atores dentro da organização.

Figura 2 – Estrutura do quadro de diretores da ICANN



Fonte: ICANN (2020). Disponível em: https://www.icann.org/en/system/files/files/get-to-know-the-icann-board-31dec20-en.pdf. Acesso em: 10 de dezembro de 2023

A partir da figura nota-se que nem todos os membros possuem voto na mesa dos diretores, indicando uma desigualdade em relação à deliberação e definição das políticas e diretrizes desenvolvidas pela organização. Nesse caso, os membros da área técnica de grande relevância para a arquitetura da Internet, como o *Adress Supporting Organization* (ASO), o *Country Code-Names Supporting Organization* (ccNSO) e o *Generic Names-Supporting Organization* (GNSO), possuem duas cadeiras votantes cada, enquanto os membros dos comitês consultivos não possuem direito ao voto. Dentre os não votantes, encontra-se o *Governmental Advisory Committee* (GAC), comitê formado por representantes de governos nacionais que podem apenar fazer recomendações à ICANN.

Sendo assim, o GAC é o representante dos Estados dentro da ICANN e só se tornou um órgão da organização depois de 2002, com as mudanças estruturais em seu estatuto, tornando o GAC um órgão sem direito a voto, mas com papel recomendatório (Becker, 2019). Isso significa que na estrutura de comando da principal entidade de gerenciamento da Internet, os países não possuem uma participação ativa de influência, não sendo diretamente os tomadores de decisão sobre como a Internet deve operar e sob quais princípios ela deve ser regida. Apesar disso, por ter o envolvimento de diversos atores de diferentes áreas em seu quadro, a ICANN pode ser vista como um exemplo de validação do modelo *multistakeholder*. Dessa forma, a ICANN compartilha valores e princípios previstos pelo modelo, como transparência, diversidade, representatividade e uma Internet aberta (Sahel, 2016).

Esses princípios foram reivindicados e fortalecidos especialmente após a organização ter sido separada do governo dos Estados Unidos. Isso porque até o ano de 2016, a ICANN era vinculada ao Departamento de Comércio dos EUA e, como expressa Becker (2019), quando o governo estadunidense anunciou que não renovaria o contrato e deixaria de exercer controle, requisitou que o design institucional da ICANN fortalecesse o modelo *multistakeholder*, de forma a manter a estabilidade, segurança, resiliência e abertura da Internet. Como consequência, há certas contestações em relação a esse modelo. Na verdade, a própria desvinculação do governo estadunidense com a ICANN, tornando ela uma entidade privada para regular a Internet, ocorreu após um processo de pressão externa e internacional, especialmente após as revelações de Edward Snowden sobre a espionagem estadunidense contra outros países, como Brasil e Alemanha, que passaram a questionar a conduta dos EUA como “regente” da Internet global (Becker, 2019).

Ocorre que muitos atores estatais, que acabam tendo uma participação periférica nas tomadas de decisões e na capacidade de influenciar na arquitetura e nos debates sobre como a Internet deve ser regida e operacionalizada, se tornaram cada vez mais deliberativos e a se

posicionarem pelo estabelecimento de um modelo diferente do *multistakeholder*, com um papel mais proeminente dos Estados (Calderaro, 2021). Essa alternativa consistiria em um modelo voltado ao multilateralismo. Os principais críticos do *multistakeholderism* enfatizam que, na prática, esse modelo favorece a desigualdade entre os atores, em que os poderosos e privilegiados são favorecidos (Haggart; Scholte; Tusikov, 2021). Nesse sentido, uma opção baseada em um formato multilateral é colocada à mesa, consistindo em uma espécie de transferência de responsabilidades da governança do espaço cibernético global para órgãos em que os Estados teriam maior proeminência, como a União Internacional de Telecomunicações (UIT) da ONU (Haggart; Scholte; Tusikov, 2021).

Já os defensores do modelo *multistakeholder*, além de destacar que esse modelo preza pelos princípios da transparência, do livre acesso e livre fluxo de informações, também argumentam que o Estado possuir maior envolvimento e influência no gerenciamento da Internet, e na governança do ciberespaço global como um todo, pode servir como uma ferramenta para o autoritarismo (Haggart; Schoelte; Tusikov, 2021). Isso significa que podemos considerar que há duas grandes abordagens sobre como o ciberespaço deve ser administrado e governado.

> A primeira é uma abordagem técnica, que pode ser descrita como a fusão do mercado com a sociedade, bem como um arranjo espontâneo baseado em um consenso aproximado. De uma perspectiva técnica, a Internet ainda é a continuação do experimento ARPANET criado pela Agência de Projetos de Pesquisa Avançada de Defesa dos EUA há mais de 30 anos atrás. A outra uma abordagem regulatória na qual é centrada em governos soberanos, como o controle de atividades cibernéticas por leis domésticas e o poder discursivo relativo dos países na governança global (Cuihong, 2018, p. 56, tradução nossa)[45].

Isso significa que há uma divergência entre os atores, especialmente entre os Estados, em relação a qual modelo deve ser implementado, sendo que essas divergências envolvem o conhecimento e a prática no que concerne ao ciberespaço, ideologias, valores e interesses nacionais (Huang; Macák, 2017). A principal divergência nesse caso ocorre entre o Ocidente, centrado na figura dos EUA, e o Oriente, com destaque para a China e a Rússia, em que todos já expressaram as suas preferências e possuem as suas posições quanto ao modelo que deve ser implementado para o ciberespaço (Huang; Macák, 2017). Dessa forma, pela posição desses

[45] Texto original: One is the technical approach, which can be described as a fusion of the market and society, and also a spontaneous arrangement based on rough consensus. From a technical point of view, the Internet is still a continuation of the experimental ARPANET created by the U.S. Defense Advanced Research Projects Agency more than 30 years ago. The other is the regulatory approach which is centered on sovereign governments, such as the control of cyber activities by domestic law and the relative discourse power of countries in global governance.

países em relação à governança global do ciberespaço, em conjunto com a relevância que possuem no cenário geopolítico internacional, será analisado quais são as concepções e as posições adotadas por EUA, China e Rússia nesse quesito a partir de documentos governamentais oficiais que expressam sobre o assunto, bem como de declarações unilaterais e em fóruns internacionais.

4.2 ESTADOS UNIDOS

Como já comentado brevemente, os Estados Unidos foram os responsáveis pela criação e elaboração da Internet, que por muito tempo ficou sendo governada pelo governo estadunidense. Nesse sentido, não é de hoje que o setor cibernético possui uma grande relevância no país em termos do que ele pode proporcionar para as relações socioeconômicas e também securitárias. Não à toa que desde 2003, com a publicação do documento "*The National Strategy to Secure Cyberspace*", os EUA reconhecem que o domínio cibernético é fundamental não só para o desenvolvimento e a prosperidade da nação, mas também para a proteção do país contra as ameaças no mundo virtual que ganharam cada vez mais destaque no século XXI.

Dessa forma, diversos documentos governamentais que abordam ou citam o espaço cibernético foram elaborados e publicados pelo país norte-americano nos últimos anos. No entanto, neste trabalho serão analisados somente uma parcela desses documentos, pois para fins de pesquisa, apenas os documentos que mencionam ou abordam sobre a governança global do ciberespaço são válidos para serem analisados. Com isso, após pesquisar e ler os principais documentos estratégicos de segurança nacional, defesa nacional, segurança cibernética e defesa cibernética dos EUA, chegou-se aos seguintes documentos para serem analisados:

Tabela 4 – Documentos governamentais dos EUA

Nome	**Data**	**Órgão responsável**
International Strategy for Cyberspace	2011	The White House
National Cyber Strategy of the United States of America	2018	The White House
Recommendations to the President on Protecting	2018	Office of the Coordinator for Cyber Issues

American Cyber Interests through International Engagement		
National Cybersecurity Strategy	2023	The White House

Fonte: Elaborado pelo autor

Para além desses documentos oficiais, será analisado a "Declaração para o Futuro da Internet (DFI)", documento que conta com a participação de 60 países, mas que teve os Estados Unidos como figura central na sua articulação e elaboração. Ademais, discursos e declarações por representantes do governo estadunidense também serão levados em consideração e trazidos nessa seção.

O primeiro documento estratégico estadunidense a mencionar sobre a governança global do ciberespaço foi o "*International Strategy for Cyberspace*", publicado no ano de 2011, pela então administração de Barack Obama. Esse documento reconhece que o espaço cibernético possui o potencial de afetar o mundo inteiro e, então, políticas que guiem e fortaleçam os EUA nesse domínio, tanto em nível interno quanto externo, são necessárias (Estados Unidos, 2011). Dessa forma, o país norte-americano estabelece os princípios nos quais a sua estratégia internacional será estruturada, que são a liberdade fundamental, a privacidade e a livre circulação de informações.

O documento se refere à liberdade fundamental como a habilidade de procurar, receber e transmitir informações e ideias através do espaço cibernético; a privacidade fica consistida na obrigação de proteger os dados e a vida privada dos usuários, em que os indivíduos devem saber e entender como os seus dados são utilizados; por fim, o princípio da livre circulação de informações refere-se à não utilização de sistemas de segurança para suprimir a liberdade de expressão e associação dos indivíduos, sendo que os EUA se comprometem com iniciativas internacionais que prezem pelo livre comércio e livro fluxo de informações (Estados Unidos, 2011).

Sendo assim, o país expressa que tem como objetivo trabalhar em nível internacional para promover uma infraestrutura de informação e comunicação que seja aberta, interoperável, segura e confiável (Estados Unidos, 2011). Esses princípios vão ao encontro do que o modelo *multistakeholder* preza, em que a não intervenção na forma como o espaço cibernético e a Internet foram fundados se mostra como o melhor caminho para o desenvolvimento e para as relações entre os múltiplos atores no domínio cibernético. Como consequência, o documento

enfatiza que a garantia da estabilidade no ciberespaço global para os Estados ocorre por meio de normas de comportamento, mas que essas normas precisam seguir padrões técnicos que melhor preservam a funcionalidade global das redes (Estados Unidos, 2011). Nesse ponto, o modelo *multistakeholder* aparece como um item essencial para que o cenário mencionado seja real. Conforme o documento, uma governança *multistakeholder* prevê que: "Esforços para a governança da Internet não podem ser limitados por governos, mas devem incluir todas as partes interessadas apropriadas" (Estados Unidos, 2011, p. 10, tradução nossa)[46].

Dessa forma, o documento enfatiza que para promover estruturas de governança da Internet que sirva as necessidades de todos os usuários é necessário promover e aprimorar o *multistakeholderism* como modelo a ser implementado. É exposto que a arquitetura da Internet possui em si um modo organizacional descentralizado, cooperativo e em camadas, sendo que esse modo deve ser fortalecido já que permite a liberdade de expressão, o desenvolvimento social e político e a funcionalidade das democracias ao redor do mundo (Estados Unidos, 2011). Com isso, o governo estadunidense expressa que

> Os Estados Unidos permanecem firme na nossa convicção que quando a comunidade internacional se reunir para discutir sobre questões que abrangem a governança da Internet, essas discussões devem ocorrer de uma maneira *multistakeholder*; nós vamos continuar a apoiar locais de sucesso como o Fórum de Governança da Internet, no qual incorpora a natureza aberta e inclusiva da Internet em si mesmo ao permitir que atores não governamentais contribuam para a discussão em pé de igualdade com os governos (Estados Unidos, 2011, p. 22, tradução nossa)[47].

Isso significa que o primeiro documento estratégico dos EUA no âmbito da construção e implementação de diretrizes internacionais a serem tomadas pelo país, já previa a defesa e a promoção do modelo *multistakeholder* como um fator importante no desígnio das suas políticas e ações em âmbito internacional. Interpreta-se, assim, que desde esse período, o modelo *multistakeholder* e a sua aplicação prática é visto pelos EUA como algo que vai ao encontro dos seus interesses e objetivos.

Em concordância, no ano de 2018, com a publicação do "*National Cyber Strategy of the United States of America*", pela administração de Donald Trump, os Estados Unidos continuaram a defender essa via de "governança" para o ciberespaço em nível global. O

[46] Texto original: Internet governance efforts must no be limited to governments, but should include all appropriate stakeholders.

[47] Texto original: The United States stands firm in our conviction that when the international community meets to discuss the range of Internet governance issues, these conversations must take place in a multi-stakeholder manner; we will continue to support successful venues like the Internet Governance Forum, which embodies the open and inclusive nature of the Internet itself by allowing nongovernment stakeholders to contribute to the discussion on equal footing with governments.

documento é dividido em 4 pilares fundamentais para que a segurança cibernética seja efetiva no país, sendo eles: (i) proteger a população, o território e o estilo de vida estadunidense; (ii) promover a prosperidade estadunidense; (iii) preservar a paz por meio da força e (iv) avançar a influência dos EUA (Estados Unidos, 2018a). Neste quarto e último pilar, a promoção de uma Internet aberta, interoperável, confiável e segura é posto como o elemento fundamental para que o objetivo de avanço da influência do país seja alcançado.

O documento expressa que o mundo inteiro olha para os Estados Unidos, por ser referência e líder em questões cibernéticas (Estados Unidos, 2018a). Dessa forma, é visto como estratégico para o país manter essa postura e avançar a sua influência para além das suas fronteiras, a partir de colaborações e alianças, de modo que os interesses dos Estados Unidos sejam reforçados (Estados Unidos, 2018a). Sendo assim, diversos pontos e ações são trazidos para que esse objetivo, de manter os EUA como uma referência para os demais, seja mantido e implementado.

Dentre esses pontos, o governo estadunidense enfatiza a necessidade de manter a Internet funcionando e sendo administrada da maneira como ela é nos dias de hoje, em que há o envolvimento de múltiplos atores e os princípios da liberdade de expressão e do livre fluxo de informações sejam protegidos. Essa ênfase ocorre devido à visão dos EUA sobre o que representa para eles manter uma Internet aberta e administrada aos moldes atuais.

> O governo dos Estados Unidos conceitua a liberdade na Internet como o exercício online dos direitos humanos e liberdades fundamentais – como a liberdade de expressão, associação, reunião pacífica, religião ou crença, privacidade de direitos online – independente de fronteiras ou meio. Por extensão, a liberdade na Internet também apoia a livre circulação de informações online que aprimoram o comércio, fomenta a inovação e fortalece tanto a segurança nacional quanto a internacional (Estados Unidos, 2018a, p. 24, tradução nossa)[48].

Nesse sentido, a manutenção da estrutura e arquitetura da Internet nos moldes criados pelos EUA são tidos como a exaltação e a garantia de valores nos quais o país preza. Como consequência dessa concepção, o documento expressa de maneira explícita que é necessário promover um modelo de governança da Internet que seja *multistakeholder*. Fica colocado que os Estados Unidos irão continuar a participar em esforços globais que garantam que o modelo *multistakeholder* prevaleça contra outro modo de gerenciar e administrar a Internet,

[48] Texto original: The United States Government conceptualizes Internet freedom as the online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium. By extension, Internet freedom also supports the free flow of information online that enhances international trade and commerce, fosters innovation, and strengthens both national and international security.

especialmente contra tentativas de criação de estruturas de governança centradas na figura do Estado, que poderiam acabar a Internet livre (Estados Unidos, 2018a). Sendo assim, esse documento é mais direto ao expressar que não é do interesse dos EUA que o ciberespaço seja governado de uma maneira diferente da estrutura organizacional existente. E não apenas isso, mas que o país norte-americano irá minar as tentativas que vão contra o modelo *multistakeholder* (Estados Unidos, 2018a).

Como justificativa, o governo dos EUA esclarece que o *multistakeholderism* é caracterizado pela transparência, pelo consenso nas tomadas de decisões e pelo envolvimento de vários atores que garantem o teor técnico necessário para operar o domínio cibernético (Estados Unidos, 2018a). Dessa forma, a defesa e o fomento desse modelo é apontado como uma ação prioritária para que o país possa continuar a expandir a sua área de influência no mundo (Estados Unidos, 2018a). Consequentemente, interpreta-se que a implementação prática do modelo *multistakeholder* favorece o país norte-americano, tanto no sentido do seu desenvolvimento, quanto da sua segurança e capacidade cibernética.

Foi também no ano de 2018 que o "*Office of the Coordinator for Cyber Issues*", escritório alocado dentro do Departamento de Estado responsável por cuidar dos assuntos cibernéticos no âmbito da diplomacia global, elaborou o documento "*Recommendations to the President on Protecting American Cyber Interests through International Engagement*". Esse documento serve como uma orientação ao Presidente dos EUA sobre o cenário e a importância do setor cibernético para as variadas áreas do desenvolvimento socioeconômico, bem como sobre ações e diretrizes que devem ser tomadas para justamente estabelecer práticas que contribuam para a prosperidade do país na dinâmica internacional no que concerne ao domínio cibernético.

Assim, o documento alerta que os Estados estão cada vez mais conscientes da importância do setor cibernético para a atividade econômica e política e, por conseguinte, se importando e se comprometendo com a regulamentação e controle da Internet (Estados Unidos, 2018b). Nesse sentido, é esclarecido que muitos Estados estão assumindo que uma Internet aberta e a abordagem *multistakeholder*, defendida pelos EUA, são uma ameaça para as suas estabilidades domésticas e são um meio para proteger os interesses Ocidentais (Estados Unidos, 2018b).

Com isso, são recomendadas que sejam tomadas ações no nível internacional que fortaleçam a visão e os interesses do país. Dentre essas ações, é destacado a importância de coalisões e parcerias multilaterais com países que defendam uma Internet aberta, que preserve o livro fluxo de informações e proteja os direitos humanos por meio de coordenação diplomática

(Estados Unidos, 2018b). Além disso, é posto como essencial que o papel de atores não estatais na governança do ciberespaço seja mantido, expressando precisamente que é preciso "promover o sistema existente de governança *multistakeholder* da Internet para gerenciar recursos-chave da Internet e se opor a novos mecanismos de cima para baixo ou intergovernamentais para a governança da Internet" (Estados Unidos, 2018b, p. 3, tradução nossa)[49].

Isso significa que a recomendação do escritório é que o país tenha um engajamento internacional voltado a defender o modelo *multistakeholder*. Interpreta-se, portanto, que esse modelo é capaz de beneficiar os EUA a atingir os seus objetivos de política externa no que concerne ao setor cibernético, aumentando a capacidade do país em fazer valer as suas vontades e maximizar a sua influência na dinâmica internacional. Não por coincidência, ao final do documento é indicado que as orientações estratégicas visam contribuir para a efetividade dos EUA no seu engajamento internacional em assuntos cibernéticos (Estados Unidos, 2018b).

Já recentemente, em 2023, sob a administração de Joe Biden, os Estados Unidos publicaram uma nova estratégia de cibersegurança, atualizando o documento de 2018. Entitulado de "*National Cybersecurity Strategy*", ele tem como objetivo principal construir um ecossistema protegido e resiliente para o país, fazendo com que nem incidentes nem erros possam se tornar uma catástrofe com consequências sistêmicas (Estados Unidos, 2023). O documento é dividido em 5 pilares essenciais para que esse ecossistema cibernético seja uma realidade, sendo eles: (i) defesa das infraestruturas críticas; (ii) romper e desmantelar atores da ameaça; (iii) moldar forças do mercado para guiar para a segurança e a resiliência; (iv) investir em um futuro resiliente e (v) formar parcerias internacionais para perseguir objetivos conjuntos (Estados Unidos, 2023).

Dentro de cada um desses pilares, há objetivos tidos como fundamentais para que eles possam ser assegurados. Assim, dentro do quarto pilar, sobre investir em um futuro resiliente, é posto o objetivo estratégico de garantir a fundação técnica da Internet. Nesse sentido, o documento preza pela preservação e expansão de uma Internet livre, aberta, global e confiável, em que os padrões técnicos sejam garantidos, visto que se enxerga que há regimes autocráticos que querem alterar a fundação *multistakeholder* da Internet e permitir um maior controle governamental (Estados Unidos, 2023). Além disso, no quinto pilar, sobre construir parcerias internacionais para perseguir objetivos conjuntos, o governo estadunidense estabelece o

[49] Texto original: Promoting the existing multistakeholder Internet governance system to manage key Internet resources and oppose new top-down or intergovernmental mechanisms for Internet governance

objetivo estratégico de construir coalisões para combater ameaças ao seu ecossistema digital e, dentro desse objetivo, o modelo *multistakeholder* é mencionado.

Fica expressado que realizar parcerias com diversos *stakeholders*, de forma a incluir o setor privado e organizações da sociedade civil é um elemento fundamental para lidar com problemas sistêmicos (Estados Unidos, 2023). Nesse sentido, o governo estadunidense aponta que

> Nós vamos aproveitar essas parcerias para habilitar colaborações operacionais efetivas para defender nosso ecossistema digital compartilhado. Nós iremos também apoiar e ajudar a construir, como necessário, novas e inovadoras parcerias – como no caso da internacional Iniciativa Contra-Ransomware – que traz junto coleções únicas de atores para lidar com novos e emergentes desafios de segurança cibernética (Estados Unidos, 2023, p. 30, tradução nossa)[50].

Isso significa que, para o governo estadunidense, manter o modelo *multistakeholder* possibilita que os padrões técnicos do ciberespaço global sejam mantidos e que parcerias estratégicas com atores de interesse sejam realizadas em favorecimento do país norte-americano. O documento de 2023 é mais sucinto e menos direto do que a estratégia de 2018 em expressar explicitamente que o modelo *multistakeholder* deve ser promovido no âmbito da governança global do ciberespaço. No entanto, não deixa de mencionar como esse modelo está alinhado aos valores dos EUA e mantê-lo é visto como o melhor caminho para a funcionalidade regular da Internet sob os princípios da liberdade e transparência.

Como comentado anteriormente, para além dos documentos governamentais, no caso dos EUA será analisado também a DFI, divulgada em 2022, visto que o país norte-americano foi quem liderou o seu processo de elaboração e publicação. A declaração é inspirada na visão e no sentimento de que a Internet é uma ferramenta com a capacidade de promover o bem-estar e a prosperidade, bem como garantir direitos fundamentais, e, por isso, deve ser protegida. Nesse sentido, é expressado que a operação estável e segura dos sistemas da Internet tem sidos governada, desde a sua criação, por uma abordagem *multistakeholder* de forma a evitar uma fragmentação e isso precisa ser preservado no mundo (DFI, 2022).

O documento enfatiza que esse modelo está sendo ameaçado ultimamente e isso é um risco para a defesa de princípios de liberdade. Dessa forma, os signatários do documento têm a visão de que devem garantir que o uso de tecnologias digitais reforce a democracia e o respeito

[50] Texto original: We will leverage these partnerships to enable effective operational collaboration to defend our shared digital ecosystem. We will also support and help build, as needed, new and innovative partnerships – as in the case of the international Counter-Ransomware Initiative – that bring together unique challenges of stakeholders to address new and emerging cybersecurity challenges.

aos direitos humanos, oferecendo oportunidades de inovação (DFI, 2022). Como consequência, a declaração enfatiza que a Internet precisa operar de maneira descentralizada, por uma abordagem *multistakeholder* em que governos atuam em parceria com a academia, a sociedade civil, o setor privado e a comunidade técnica para lidar com o gerenciamento global da Internet (DFI, 2022).

Nesse sentido, como uma ação a ser tomada pelos países apoiadores da declaração, é relatado que devem:

> Proteger e fortalecer o sistema *multistakeholder* de governança da Internet, incluindo o desenvolvimento, implementação e gerenciamento dos seus principais protocolos técnicos e outros padrões e protocolos relacionados. Abster-se de minar a infraestrutura técnica essencial para a disponibilidade e integridade geral da Internet (DFI, 2022, p. 3, tradução nossa)[51].

Por fim, a declaração argumenta que os princípios, diretrizes e ações expostas em seu conteúdo, assinado por 60 países, sirva de guia e sejam levados em consideração em processos e debates multilaterais como na ONU, G7, G20, Organização para a Cooperação e Desenvolvimento Econômico (OCDE), Organização Mundial do Comércio (OMC), entre outros (DFI, 2022).

Para além dos documentos, os Estados Unidos também defendem o modelo *multistakeholder* em declarações unilaterais e multilaterais. No ano de 2014, por exemplo, no Encontro Multissetorial Global sobre o Futuro da Governança da Internet, também chamado de NETmundial, realizado no Brasil, o país norte-americano submeteu algumas contribuições para o evento. Dentre essas contribuições, se encontra o tópico de princípios para a governança da Internet. Nesse tópico, o governo estadunidense expressa que é preciso que os atores tenham compromisso com a abordagem *multistakeholder*, de modo a envolver múltiplos atores e ocorrer de maneira transparente, além de promover o acesso não discriminatório à Internet (Estados Unidos, 2014).

Ademais, no ano de 2023, o governo dos EUA divulgou a Declaração da Cúpula para a Democracia, reforçando o compromisso do governo com os princípios democráticos e reconhecendo a importância da sua valorização. Na declaração, o governo dos EUA reitera que

---

[51] Texto original: Protect and strengthen the multistakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols. Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.

promover o acesso à Internet contribui para a democracia, mas para isso as companhias de tecnologia precisam se comportar de maneira responsável, de modo a proteger os dados e informações de privacidade dos usuários, bem como atuar com transparência (Estados Unidos, 2023b). Além disso, expressa que a manutenção do *multistakeholderism* colabora com os princípios democráticos, enfatizando o seu compromisso com esse modelo.

> Nós somos guiados pelo compromisso de fortalecer a abordagem *multistakeholder* de governança para a Internet e uma mais robusta cooperação entre governos e autoridades em política públicas relevantes referentes ao ecossistema digital de modo a atingir soluções inclusivas, compreensivas, coerentes e duradouras (Estados Unidos, 2023b, s.p, tradução nossa)[52].

4.3 CHINA

A República Popular da China tem enfatizado a importância de proteger o ciberespaço como um aspecto da sua segurança nacional desde a década passada. Dessa forma, elaborou e publicou documentos referentes ao ciberespaço e à segurança cibernética de modo a estabelecer a sua estratégia frente a esse novo domínio. Como já explicitado brevemente, a China possui uma concepção sobre o ciberespaço que difere da concepção estadunidense e da considerada visão ocidental tradicional para esse ambiente, visto que o país asiático enxerga esse ambiente como um espaço em que a soberania nacional deve prevalecer para que as oportunidades de desenvolvimento socioeconômico e a sua segurança sejam garantidas (China, 2016a).

Como consequência de ter um olhar distinto para o espaço cibernético, a China também tem a sua própria consideração sobre como a governança global para o ciberespaço deve se dar. Por isso, são analisados os principais documentos governamentais estratégicos sobre o ciberespaço publicados pela China que permeiam e/ou comentam sobre a posição chinesa frente a esse assunto. Ao contrário dos EUA, o país asiático conta com poucos documentos sobre o espaço cibernético e, assim, todos foram analisados nessa pesquisa. Além disso, discursos de autoridades chinesas também são levados em consideração nesta seção. A tabela a seguir indica os documentos chineses analisados neste trabalho.

Tabela 5 – Documentos governamentais da China

[52] Texto original: We are guided by a commitment to a strengthened multistakeholder approach to Internet governance and more robust cooperation among governments and authorities on relevant public policies issues pertaining to digital ecosystems in order to achieve inclusive, comprehensive, coherent, and enduring solutions.

Nome	Data	Órgão responsável
Estratégia Nacional de Segurança do Ciberespaço[53]	2016	Cyberspace Administration of China
Lei de Segurança Cibernética da República Popular da China[54]	2016	Office of the Central Cyberspace Affairs Commission
Estratégia Internacional de Cooperação para o Ciberespaço[55]	2017	Cyberspace Administration of China

Fonte: Elaborado pelo autor

O primeiro documento chinês a mencionar sobre a governança global do ciberespaço foi a "Estratégia Nacional de Segurança do Ciberespaço", publicado no ano de 2016. Na realidade, o governo chinês expressa que esse documento tem como intenção fazer com que seja possível a implementação dos quatros princípios de promoção de uma reforma do sistema de governança global da Internet, proposto pelo presidente Xi Jinping no ano anterior, em 2015, em seu discurso na segunda Conferência Mundial da Internet, realizada na China. Nesse discurso, o governante chinês destaca que o aprofundamento da multipolaridade no mundo, da globalização econômica e da aplicação de tecnologias da informação, fez com que a Internet ganhasse um papel fundamental no progresso da humanidade (China, 2015).

Como consequência, a importância do setor cibernético é evidenciada, mas é manifestado que problemas como desenvolvimento desigual, regras inadequadas e uma ordem não-equitativa são características da Internet em nível mundial. Xi Jinping então alega que há uma lacuna entre os países e, que as regras existentes sobre o ciberespaço global raramente refletem os desejos e os interesses da maioria dos países (China, 2015). Sendo assim, o presidente chinês realça quatro princípios que a China, e os demais países, deveriam seguir para transformar o sistema de governança global da Internet em um sistema mais seguro, democrático e transparente, sendo eles: (i) respeito pela soberania cibernética; (ii) manutenção da paz e da segurança; (iii) promoção da abertura e da cooperação; (iv) cultivo de uma boa ordem (China, 2015).

[53] Texto original: 国家网络空间安全战略

[54] Texto original: 中华人民共和国网络安全法

[55] Texto original: 网络空间国际合作战略

Para o primeiro princípio, relacionado à soberania, argumenta-se que, com base na Carta das Nações Unidas, a soberania deve ser aplicada também ao espaço cibernético já que ela é um elemento basilar das relações internacionais e cobre todos os aspectos das interações interestatais. Dessa forma, Xi Jinping defende que todo e qualquer país deve ter o direito de escolher o seu caminho de desenvolvimento cibernético, estabelecer as políticas que lhe são convenientes e poder participar de maneira igualitária na governança internacional do ciberespaço (China, 2015). Além disso, enfatiza que nenhum país deve pretender a hegemonia cibernética e/ou interferir nos assuntos internos de outro país no que diz respeito ao setor cibernético (China, 2015).

Para o segundo princípio, sobre a manutenção da paz e da segurança, o presidente da China alega que o ciberespaço não deve se tornar um campo de batalha entre os países e muito menos ser um ambiente propício e confortável para o cometimento de crimes (China, 2015). Dessa forma, o discurso expressa que um ciberespaço seguro, confiável e próspero é de grande relevância para todos no mundo, sendo que os países devem trabalhar para que os crimes cibernéticos, sejam roubos comerciais ou ataques contra governos, sejam combatidos por meio de regras e convenções internacionais relevantes sobre o assunto, visto que, como coloca Xi Jinping: "Nós não podemos ter a segurança de um ou alguns países enquanto o resto é deixado com insegurança [...]" (China, 2015, s.p, tradução nossa)[56].

Sobre o princípio da promoção da abertura e da cooperação, o governante chinês alega que para que a governança global do ciberespaço seja aprimorada, é preciso que os conceitos de apoio mútuo, confiança mútua e benefício mútuo sejam seguidos, de forma que a mentalidade de soma zero seja rejeitada (China, 2015). Por conseguinte, o discurso coloca que a cooperação no ciberespaço deve ser fortalecida, em que mais pontos de convergência de interesses sejam criados para que mais pessoas e mais países sejam beneficiados com o desenvolvimento cibernético (China, 2015).

O último princípio levantado por Xi Jinping, sobre o cultivo de uma boa ordem, expressa que ordem e liberdade também são essenciais no ciberespaço. Nesse sentido, o líder chinês argumenta que os direitos dos usuários devem ser respeitados ao mesmo tempo que uma boa ordem no ciberespaço deve ser construída por meio de leis e normas, que justamente protejam os direitos e o interesses legítimos das pessoas (China, 2015). "O ciberespaço deve ser governado, operacionalizado e utilizado de acordo com a lei, para que a Internet possa

[56] Texto original: We cannot just have the security of one or some countries while leaving the rest insecure [...]

aproveitar de um desenvolvimento sólido no âmbito da regra da lei" (China, 2015, s.p, tradução nossa)[57].

Ainda em seu discurso, Xi Jinping expõe cinco propostas práticas para que os princípios mencionados sejam estabelecidos. Dentre as propostas, está a construção de uma governança global para o ciberespaço que promova a justiça e a equidade. O líder chinês alega que o espaço cibernético em nível internacional deve ser governado por uma abordagem multilateral com uma múltipla participação dos atores, que deveria ser baseada na consulta entre todas as partes, aproveitando o papel de cada um, incluindo governos, organizações internacionais, empresas de Internet, comunidades de tecnologia, instituições não governamentais e cidadãos (China, 2015). Dessa forma, Xi Jinping esclarece que não deve haver unilateralismo no âmbito da governança global do ciberespaço, em que as decisões não devem ser feitas por um único ator ou um pequeno grupo, mas que todos os países precisam participar e construir regras para essa governança, de modo que reflita os interesses e aspirações da maioria (China, 2015).

É a partir do alicerce desse discurso, portanto, que a estratégia chinesa de segurança cibernética é elaborada e publicada. Isso significa que o documento segue a lógica de buscar estabelecer os aspectos e os pontos trazidos na fala do presidente da China. Assim, é mencionado como um elemento importante para a garantia da segurança cibernética nacional chinesa, que todos os países cooperem nas áreas de intercâmbio de tecnologia, sendo que um sistema de governança internacional para o ciberespaço que seja multilateral, democrático e transparente é tido como algo sólido e ideal (China, 2016a). Com isso, a China se propõe a participar ativamente na promoção de uma transformação no sistema de governança da Internet no intuito de salvaguardar a paz e a segurança no ciberespaço (China, 2016a).

O documento também determina como um dos seus pontos estratégicos o fortalecimento da cooperação internacional no ciberespaço, sendo que é defendido um modelo multilateral de governança global para o ciberespaço. O governo chinês enxerga que a ONU deveria ter um papel central nesse modelo, de forma a promover o desenvolvimento de regras internacionais universalmente aceitadas para o ciberespaço, aprofundando padrões e normas a serem seguidas pelos países (China, 2016a). Isso significa que o país asiático acredita que o estabelecimento de um modelo multilateral de governança favorece não somente a sua própria segurança, mas também favorece que os interesses de atores menores e menos relevantes sejam levados em consideração.

[57] Texto original: Cyberspace must be governed operated and used in accordance with law, so that the Internet can enjoy sound development under the rule of law.

O segundo documento governamental da China analisado neste trabalho refere-se à "Lei de Segurança Cibernética da República Popular da China", publicado no ano de 2016. Tal documento consiste em regras, diretrizes e princípios a serem seguidos pela China e a sua população para que a segurança cibernética seja garantida no país. Dessa forma, ele possui como objetivo central assegurar que a soberania do ciberespaço seja protegida, que a segurança nacional, o interesse social público, os direitos dos cidadãos e o desenvolvimento socioeconômico sejam assegurados (China, 2016b).

Para o governo chinês, atingir tal objetivo perpassa por agir de maneira ativa no âmbito internacional nos assuntos que envolvem o ciberespaço. Sendo assim, o documento expressa que o Estado chinês irá promover um ciberespaço de paz, segurança, cooperação e aberto, contribuindo para estabelecer uma governança global multilateral que seja democrática e transparente (China, 2016b). Por se tratar de um documento mais voltado para os assuntos internos de segurança cibernética, como regras específicas para operadores de redes, cidadãos e instituições, essa é a única menção sobre a governança global do ciberespaço existente.

Já o terceiro documento governamental chinês, a "Estratégia Internacional de Cooperação para o Ciberespaço", publicado no ano de 2017, dá maior ênfase em ações e diretrizes que o Estado chinês deve tomar em nível internacional. O entendimento do país para a elaboração dessa estratégia é de que o ciberespaço é um bem comum da humanidade, em que os países estão interconectados pelo ambiente cibernético e, com isso, a comunidade internacional deve ter a responsabilidade de construir um ciberespaço confiável e de comum interesse para todos (China, 2017).

Isso porque governo chinês tem a concepção de que estamos vivendo uma nova era com a revolução da informação, que trouxe e permitiu que mudanças profundas ocorressem no modo de vida dos humanos, estimulando inovações no mercado, prosperidade econômica e desenvolvimento social (China, 2017). O ciberespaço, portanto, é tido como peça central nessa revolução, sendo o elemento que faz com que as oportunidades de desenvolvimento ocorram. Contudo, a China destaca que apesar do espaço cibernético ser um propulsor para as inovações e mudanças sociais, culturais e econômicas, existem problemas a serem superados que englobam o setor cibernético, como o desenvolvimento desigual de capacidades tecnológicas e da própria Internet, bem como a falta de regras sólidas no âmbito internacional, fazendo com que uma ordem irracional se tornasse proeminente (China, 2017).

Dessa forma, há o entendimento de que existe uma separação entre os países no que concerne ao desenvolvimento tecnológico e à utilização de capacidades tecnológicas para a prosperidade nacional. "A divisão digital entre países e regiões continua a aumentar.

Infraestruturas críticas de informação possuem riscos vitais. O sistema global de gerenciamento de recursos básicos da Internet tem dificuldade de refletir os desejos e interesses da maioria dos países" (China, 2017, p. 2, tradução livre)[58]. Um dos aspectos destacados no documento para a existência dessa divisão desigual é o comportamento distinto dos países, em que há o abuso do uso de TICs por determinados países que interferem nos assuntos internos de outros, sendo que esses comportamentos abusivos ocorrem devido à ausência de regras internacionais efetivas que regulem o comportamento dos atores no ciberespaço (China, 2017).

Com isso, a estratégia chinesa determina que o país preza pelo princípio da governança conjunta. Pois, é tido que devido ao ciberespaço ser um ambiente comum aos seres humanos, a construção de uma governança comum por todos os países deve ser realizada.

> Para a governança global do ciberespaço, nós precisamos primeiro aderir à participação multilateral. Todos os países, grandes ou pequenos, fortes ou fracos, ricos ou pobres, são membros iguais da comunidade internacional. Todos eles possuem o direito de participar na ordem e regras internacionais do ciberespaço através de plataformas e mecanismos de governança de redes internacionais para assegurar que o desenvolvimento futuro do ciberespaço seja compartilhado por todas as pessoas (China, 2017, p. 3, tradução livre)[59].

A China estima que os países devem fortalecer os seus laços no âmbito do ciberespaço, em que a comunicação, o compartilhamento de informações e o diálogo sejam aprimorados, para que possam conjuntamente formular regras internacionais para o espaço cibernético (China, 2017). Nesse cenário, o governo chinês expressa, mais uma vez, que a ONU deve ser a figura principal ao desempenhar o seu papel global de coordenar as posições de todas as partes e atuar para um consenso internacional (China, 2017). Além disso, o documento estratégico enfatiza que o estabelecimento de um modelo multilateral de governança global do ciberespaço deve ocorrer em conjunto com uma distribuição igualitária dos recursos da Internet, contribuindo para uma governança transparente e de compartilhamento responsável (China, 2017).

Um elemento recorrente nos documentos chineses e que também é enfatizado nessa estratégia de 2017 é o elemento da soberania. Interpreta-se que o governo chinês enxerga a determinação e aplicabilidade da soberania para o espaço cibernético como peça chave não só

---

[58] Texto original: **国家和地区**间的"**数字**鸿沟"**不断拉大**. **关**键信息基础设施存在较大风险隐患。全球互联网基础资源管理体系难以反映大多数国家意愿和利益

[59] Texto original: **网**络空间国际治理，首先应坚持多边参与。国家不分大小、强弱、贫富，都是国际社会平等成员，都有权通过国际网络治理机制和平台，平等参与网络空间的国际秩序与规则建设，确保网络空间的未来发展由各国人民共同掌握。

para a sua segurança, mas também para promoção e manutenção de relações harmônicas entre os Estados no âmbito cibernético. Isso porque o país expressa que a ordem internacional está estruturada e sistematizada pelo princípio da soberania nacional. Consequentemente, esse princípio deveria ser também implementado e respeitado para o ciberespaço. Nesse sentido, a China se posiciona contra toda e qualquer interferência externa em assuntos internos dos países através da Internet, bem como que os países devem ter as suas leis e regras nacionais de segurança cibernética respeitadas por todos igualmente (China, 2017).

Como um espaço que deve ter a sua soberania respeitada, o governo chinês ressalta a importância e a necessidade da construção e desenvolvimento conjunto de regras e códigos de condutas internacionais para os Estados em relação ao ciberespaço, de forma que a cooperação seja promovida e a segurança seja mantida (China, 2017). A criação de regras internacionais comuns para a regulação do comportamento dos atores no espaço cibernético perpassa pela concepção de uma governança, com isso, é enfatizado de maneira explícita no documento que o país asiático é a favor da implementação de uma governança global multilateral para o ciberespaço. "A China defende a construção de um sistema de governança global para a Internet multilateral, democrático e transparente, através da participação igualitária e tomada de decisão conjunta pela comunidade internacional" (China, 2017, p. 5, tradução livre)[60].

Nesse caso, o governo chinês enxerga que os governos nacionais devem ter um papel mais proeminente nessa governança, especialmente em assuntos que envolvem política públicas e segurança, de forma a atingir uma participação conjunta, uma gestão científica e tomadas de decisões democráticas (China, 2017). O documento também prevê planos de ações estratégicas que a China deve tomar no âmbito internacional. Dentro dessas ações, destaca-se que o país deve participar ativamente nos processos internacionais que envolvem o ciberespaço, aprimorando o diálogo e a confiança internacional, tendo como objetivo estabelecer regras e normas internacionais aceitas por todos na constituição de uma governança global para o ciberespaço (China, 2017).

Sendo assim, como uma ação específica, a China coloca que irá realizar esforços que promovam a construção de uma ordem baseada em regras para o ciberespaço, atribuindo para a ONU a incumbência de formular essas regras (China, 2017). Além disso, como outra ação, o governo chinês expressa que irá atuar para que o Fórum de Governança da Internet (IGF) tenha seus mecanismos reformados, para que o fórum desempenhe um papel mais importante na

[60] Texto original: **中国主**张通过国际社会平等参与和共同决策，构建多边、民主、透明的全球互联网治理体系。

governança global da Internet (China, 2017). Dessa forma, o documento indica que é preciso fortalecer a capacidade do fórum em tomar decisões sobre questões que envolvem a governança, bem como promover recursos para que o fórum tenha um fundo estável (China, 2017).

Por fim, o documento enfatiza que a China irá atuar para fortalecer a cooperação internacional, de forma a estimular o compartilhamento ordenado de informações entre governos, indústria e empresas, fortalecendo a proteção de infraestruturas de informação fundamentais e dados importantes (China, 2017). Nesse sentido, o país deseja que uma cultura de cooperação no ciberespaço seja cultivada pelos países, em que a Internet seja utilizada por todas as nações, sendo uma plataforma para intercâmbios culturais, compreensão mútua e comunicação entre todas as pessoas (China, 2017).

Para além dos documentos governamentais, destaca-se o discurso do representante do governo chinês, o embaixador Nong Hong, no 10º Fórum Beijing Xiangshan, em 2023. A declaração do embaixador tinha como enfoque tratar sobre a implementação conjunta de uma segurança global, em linha com a *Global Security Initiative,* proposta pelo governo chinês no ano de 2022 com o objetivo de estabelecer um mundo pacífico para a humanidade. O embaixador enfatiza quatro principais áreas em que ações devem ser tomadas para que o progresso da segurança seja estabelecido. Uma dessas áreas é a reforma no sistema de governança global, em que a China expressa a intenção de continuar apoiando o papel central na ONU na segurança global e acredita que é preciso aprimorar a governança em áreas como o ciberespaço, inteligência artificial, dados, biossegurança, terrorismo e saúde pública (China, 2023).

Isso significa que o país asiático considera a questão da governança global do ciberespaço como um elemento da segurança internacional. Nesse caso, tem-se a visão de que o estabelecimento da governança, nos moldes mencionados pelo governo chinês em seus documentos oficiais, tende a promover relações mais harmônicas e cooperativas entre os países no âmbito do setor cibernético, já que é previsto a construção de normas que norteiem o comportamento e a conduta dos atores no ciberespaço. A implementação do modelo multilateral de governança global para o ciberespaço, portanto, é visto como benéfico para a China, tanto para si quanto para a comunidade internacional.

4.4 RÚSSIA

A Federação Russa pode ser considerada também como uma potência cibernética, reconhecendo o ciberespaço, ou espaço da informação como é mencionado em seus documentos, como um espaço capaz de afetar diretamente a segurança e o desenvolvimento do país. Como membro permanente do Conselho de Segurança da ONU e pela relevância regional e internacional que possui, as políticas russas e a sua posição possuem grande peso frente a comunidade internacional e a dinâmica de poder nas relações internacionais. Dessa forma, documentos governamentais russos que tratam sobre o ciberespaço são analisados nesta seção para compreender a sua concepção frente à governança global desse domínio.

Além disso, discursos e declarações de autoridades governamentais russas também são trazidas de forma a englobar a completude da posição russa. Diferentemente de EUA e China, a Federação Russa não menciona de maneira explícita o formato de governança global para o espaço cibernético que deseja que seja implementado. No entanto, muitos dos seus dispositivos e diretrizes estratégicas elucidam o caminho que o país deseja em termos do gerenciamento e governabilidade desse espaço, como, por exemplo, a sua regulamentação em nível internacional.

Sendo assim, a tabela abaixo indica os documentos governamentais russos analisados que tocam no assunto da governança global do ciberespaço, mesmo que indiretamente.

Tabela 6 - Documentos governamentais da Rússia

Nome	**Data**	**Órgão responsável**
Doutrina da Segurança da Informação da Federação Russa[61]	2016	Decreto Presidencial
Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030[62]	2017	Decreto Presidencial

[61] Texto original: ДОКТРИНАинформационной безопасности Российской Федерации

[62] Texto original: О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы

Comunicado de imprensa sobre a adoção de uma resolução russa sobre segurança da informação internacional na Assembleia Geral das Nações Unidas[63]	2018	Ministério das Relações Exteriores da Federação Russa
Estratégia de Segurança Nacional da Federação Russa[64]	2021	Decreto Presidencial
O Conceito da Política Externa da Federação Russa[65]	2023	Decreto Presidencial

Fonte: Elaborado pelo autor

O primeiro documento do governo russo analisado em questão é o seu primeiro documento voltado exclusivamente para a segurança cibernética, ou segurança da informação, termo utilizado pelo país para tratar sobre o assunto. Intitulado de "Doutrina da Segurança da Informação da Federação Russa" e publicado em 2016, ele se caracteriza por ser a doutrina oficial do sistema de segurança nacional russo no que concerne à esfera da informação, definida como a combinação da informação, objeto de informatização, sistemas da informação e websites, redes de comunicação, tecnologias da informação, entidades envolvidas no processamento de informações, bem como mecanismos de regulamentação das relações públicas nessa esfera (Rússia, 2016).

Dessa forma, o documento tem como objetivo traçar as diretrizes estratégicas para que a proteção do ciberespaço e a segurança nacional sejam garantidas, bem como um ambiente internacional seguro e confiável (Rússia, 2016). Isso porque o governo russo entende como de suma importância que o país seja um facilitador do desenvolvimento da segurança da informação em nível internacional, de forma a combater ameaças e usos de tecnologias que desestabilizem o cenário internacional, ao mesmo tempo em que protege a soberania do seu ciberespaço (Rússia, 2016).

[63] Texto original: О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности
[64] Texto original: О Стратегии национальной безопасности Российской Федерации
[65] Texto original: Концепция внешней политики Российской Федерации

Nesse contexto, é expressado que alguns países estrangeiros se utilizam de suas capacidades tecnológicas para influenciar a infraestrutura informacional para fins militares, operando serviços de inteligência para desestabilizar internamente outros países (Rússia, 2016). Como consequência, a doutrina alega que é preciso defender a soberania do ciberespaço da Rússia e combater ações inconsistentes com o direito internacional, visto que a segurança cibernética no âmbito da estabilidade estratégica é caracterizada pelo desejo dos Estados em utilizar a sua superioridade tecnológica para dominar o espaço cibernético (Rússia, 2016).

Dessa forma, a situação atual em que há uma desigual distribuição dos recursos em nível global em relação à Internet e seu funcionamento estável, faz com que não seja possível que o gerenciamento do espaço da informação ocorra de forma justa e baseado na confiança (Rússia, 2016).

> A ausência de normas jurídicas internacionais que regulem as relações interestatais no espaço da informação, bem como os mecanismos e procedimentos para a sua aplicação que levaria em conta as especificidades das tecnologias da informação, torna difícil a formação de um sistema internacional de segurança da informação arquitetado para atingir uma estabilidade estratégica e uma parceria estratégica equitativa (Rússia, 2016, p. 6, tradução livre)[66].

Com isso, o governo russo enxerga como fundamental a defesa da sua soberania, o estabelecimento de um sistema internacional de segurança da informação capaz de regular e combater ações que utilizem tecnologias da informação e violem o direito internacional, bem como a construção de mecanismos jurídicos internacionais específicos para tratar sobre o ciberespaço e tecnologias da informação de modo a prevenir conflitos entre os Estados nesse espaço (Rússia, 2016). De modo a promover a sua posição, o documento expressa que o país deve defender e estimular a sua concepção em organizações internacionais na busca por uma cooperação benéfica mutuamente entre os atores na esfera da informação (Rússia, 2016).

No ano de 2017, o governo russo elaborou e publicou a "Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030". Assim, trata-se de um documento que prevê orientações, ações e procedimentos para serem tomados pelo país, no âmbito nacional e internacional, para a formação de uma sociedade consciente em um mundo cada vez mais digitalizado. A Rússia reconhece que as TICs promoveram mudanças

[66] Texto original: Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

significativas na forma como o ser humano realiza suas atividades e interações, sendo que considera importante que a sociedade russa tenha capacidade de utilizar as novas tecnologias, garantir a eficiência de uma economia digital e se proteger contra possíveis ataques e ações maliciosas no setor cibernético (Rússia, 2017).

Uma das justificativas para a elaboração dessa estratégia é de que não foram estabelecidos mecanismos jurídicos internacionais que permitam a defesa da soberania dos Estados sobre o ciberespaço, que acabam sendo forçados a determinar uma regulamentação estatal sobre questões que envolvem as TICs conforme as circunstâncias do mundo exigem (Rússia, 2017). Assim, como o cenário global do ciberespaço e da Internet acaba influenciando os cenários internos dos países, o governo russo reconhece que para desenvolver uma boa infraestrutura cibernética nacional, precisa realizar atividades e ações no nível internacional.

Dentre as ações, destacam-se defender o direito soberano do Estado russo em determinar as suas políticas para a Internet; trabalhar para que a Internet não seja utilizada para fins militares; contribuir para o desenvolvimento de normas de regulamentação internacional da Internet, incluindo questões de jurisdição, participação igualitária da comunidade internacional na gestão do ciberespaço global e seus recursos (Rússia, 2017). Nesse sentido, interpreta-se que a Federação Russa não vê com bons olhos a ausência de regras internacionais específicas que tratem sobre o espaço cibernético e as relações interestatais dentro dele. Como indica o documento, o país considera que essa ausência possibilita uma maior vulnerabilidade da sua soberania sobre o ciberespaço em âmbito nacional, dificultando a sua defesa.

Já no ano de 2021, o governo russo divulgou a sua nova "Estratégia de Segurança Nacional da Federação Russa", atualizando a versão anterior publicada em 2015. O documento é responsável por determinar os planos estratégicos, objetivos e as prioridades nacionais para garantir a segurança nacional do país. Dessa forma, essa estratégia concentra a maioria dos seus dispositivos para ações e diretrizes voltadas ao âmbito interno, com base em políticas nacionais. No entanto, encaminhamentos para o âmbito internacional também são mencionados, inclusive para o setor cibernético. O documento identifica o espaço cibernético como um ambiente de suma importância para a estabilidade e a prosperidade russa. Assim, dedica uma seção do documento para tratar sobre a segurança cibernética.

Fica exposto que o uso das TICs tem se expandido no mundo, mas que a sua utilização também está servindo para interferir nos assuntos internos dos países por outros e representar uma ameaça para a paz e a segurança internacional (Rússia, 2021). O governo russo alega que isso, bem como ataques cibernéticos e ações hostis como propagandas ilegais e desinformação, ocorrem por conta da falta de fundamentos jurídicos e legais no direito internacional para lidar

com o ciberespaço (Rússia, 2021). Além disso, essa ausência também é apontada como capaz de viabilizar a consolidação dos monopólios das corporações transnacionais no controle e gerenciamento dos recursos da Internet, possuindo poder para determinar bloqueios e censuras em plataformas alternativas de Internet (Rússia, 2021).

Por isso, o documento expressa que para atingir a sua meta de assegurar a segurança cibernética no país é preciso implementar políticas como fortalecer a cooperação da Rússia com parceiros externos na área de segurança cibernética, com o propósito de estabelecer um regime legal internacional de segurança no uso de tecnologias da informação (Rússia, 2021). Ademais, o governo russo aponta que os objetivos de política externa do país no âmbito da segurança dependem da realização de diversas ações, dentre elas, atuar para o desenvolvimento de uma cooperação internacional para a formação de um ciberespaço global equitativo e seguro para todos (Rússia, 2021).

Ainda na linha da área da política externa, o governo russo elaborou no ano de 2023 o "Conceito da Política Externa da Federação Russa". Tal documento estratégico trata da visão sistêmica do país no âmbito da política externa, estabelecendo os princípios, objetivos e ações prioritárias para garantir os interesses nacionais russos nessa área. O desenvolvimento de um ciberespaço seguro e a garantia da proteção da sociedade russa contra informações destrutivas estão determinados como objetivos de interesse nacional, sendo que a consolidação da posição russa no ciberespaço internacional é posta como uma ação estratégica (Rússia, 2023).

Dessa forma, na seção do documento destinada ao fortalecimento da paz e da segurança internacional, é expressado a importância de assegurar uma segurança internacional da informação, de forma a combater ameaças e fortalecer a soberania russa no ciberespaço global (Rússia, 2023). Assim, o governo russo entende que deve dar prioridade para algumas ações, como estimular e aprimorar um regime internacional legal para a prevenção de conflitos interestatais e regulamentação de atividades no ciberespaço; construir e moldar uma estrutura jurídica internacional para combater a utilização de TICs para crimes; assegurar uma Internet global segura com base na participação equitativa de todos no seu gerenciamento; e adotar políticas e medidas diplomáticas para que o ciberespaço e as TICs não sejam utilizadas como armas e para fins militares (Rússia, 2023).

Ademais, o governo russo dedica uma seção inteira somente à questão da influência da informação para a política externa do país. Nela, além de ser enfatizado que o país irá combater propagandas e informações maliciosas no cenário internacional que tenha a intenção de difamar a Federação Russa e desestabilizar a sua sociedade, é também mencionado a importância de uma regulamentação internacional para o espaço cibernético. Sendo assim, é apontado que a

Rússia deve facilitar a disseminação de informações que promovam a paz internacional e o entendimento entre os Estados, em que o aprimoramento de mecanismos e normas internacionais de regulamentação e proteção de informações e mídias de comunicação é estratégico para a disseminação de informações e o livre acesso (Rússia, 2023).

Para além dos documentos estratégicos, ainda em 2018, o Ministério das Relações Exteriores divulgou uma nota para a imprensa manifestando a adoção pela Assembleia Geral da ONU de uma resolução proposta pelo governo russo. A resolução é denominada de "Desenvolvimentos na áera da informação e telecomunicações no contexto da segurança internacional", tratando sobre questões que envolvem a segurança cibernética em âmbito internacional para os Estados. Sendo assim, a nota informa que a proposta russa incluía um documento com uma lista provisória de 13 regras internacionais, normas e princípios de comportamento responsável para os Estados na esfera do ciberespaço (Rússia, 2018).

Nesse sentido, é manifestado que o documento proposto consistiria no primeiro código de conduta para os Estados na esfera digital, tratando sobre questões como soberania, utilização responsável de TICs, ações de manutenção da segurança, papel de liderança da ONU na promoção da segurança internacional do ciberespaço, entre outros (Rússia, 2018). A resolução serviu para a criação de um grupo de trabalho voltado para esse assunto, envolvendo diversos países. No entanto, a nota informa que os países ocidentais não deram suporte para a criação desse grupo e votaram coletivamente contra as ideias propostas na resolução (Rússia, 2018). Além disso, a nota também acusa que esse comportamento demonstra ser um indicativo de que os países ocidentais são preocupados em promover uma atmosfera de desconfiança na esfera da informação (Rússia, 2018).

Como um todo, os documentos russos alegam sobre a necessidade de construir uma regulamentação internacional para o ciberespaço, alegando que a ausência de normas específicas para o domínio cibernético não é benéfica para o país e para a comunidade internacional em termos de segurança. As menções sobre esse assunto nos documentos governamentais são feitas de maneira não tão incisivas e diretas. Já algumas posições adotadas pelo governo russo em declarações são mais firmes e categóricas. O principal exemplo é a declaração dada no ano de 2014 pelo presidente da Rússia, Vladmir Putin, que expressou em uma conferência de mídia que a Internet foi construída como um "projeto da CIA" e serve para beneficiar os interesses estadunidenses (MacAskill, 2014).

Essa declaração vai ao encontro das intenções expostas nos documentos estratégicos, que argumentam a vontade e a posição russa em reformar o modo como a Internet global opera e construir mecanismos de regulamentação em nível internacional. Dessa forma, interpreta-se

que, apesar do governo russo não utilizar a expressão governança global, o país apoia que mecanismos de governança sejam criados para que regras específicas e uma ordem seja estabelecida no que diz respeito ao ciberespaço. Para a Federação Russa, portanto, atualmente existe uma ausência de governança global para o espaço cibernético, sendo que a ONU deve liderar o desenvolvimento de uma regulamentação com a participação equitativa de toda a comunidade internacional.

4.5 CONSIDERAÇÕES DO CAPÍTULO

A apresentação dos dois modelos de governança global mostrou as suas especificidades e esclareceram como os atores possuem os seus papéis em cada um deles. Nesse sentido, o modelo *multistakeholder* demonstra dar ênfase para as entidades privadas que já possuem um maior controle sobre o gerenciamento do ciberespaço, prezando pela participação de outros atores e pela manutenção da interoperabilidade da Internet e a sua abertura nos moldes atuais construídos pelos EUA. Já o modelo multilateral, de maneira sucinta, dá ênfase para o envolvimento igualitário dos governos nacionais na administração e gerenciamento do ciberespaço, em que a participação ativa da comunidade internacional é tida como um pressuposto.

Além disso, este terceiro capítulo apresentou as posições de EUA, China e Rússia no que se refere à governança global do ciberespaço. Com base nos documentos governamentais, e nas declarações de autoridades, entende-se que os Estados Unidos é o único dos três a defender a manutenção do modelo *multistakeholder*, com a premissa de que a sua aplicabilidade garante uma Internet livre e transparente. E não só isso, mas que o *multistakeholderism* assegura que o gerenciamento do ciberespaço fique nas mãos principalmente de entidades privadas e, com isso, que esse espaço não seja subjugado pelo controle estatal.

Já a China tem uma posição clara e direta na defesa do modelo multilateral de governança global, argumentando que a situação atual, em que o *multistakeholderism* prevalece, faz com que haja uma desigualdade na distribuição de capacidades e poder de tomada de decisão no âmbito do controle e da governabilidade da Internet e do ciberespaço. Sendo assim, o governo chinês enxerga com bons olhos o estabelecimento de um modelo que garanta uma distribuição e uma participação mais igualitária entre os países do mundo em assuntos que tratam sobre a arquitetura e gerenciamento da Internet. Para a China, a ONU deveria ter um papel central na implementação dessa governança, determinando as regras e princípios a serem seguidos por todos.

A Rússia, por sua vez, não menciona de maneira explícita em seus documentos a sua posição especificamente em relação à governança global do ciberespaço. No entanto, o governo russo deixa claro a sua concepção, de que a situação atual de ausência de regulamentação internacional para o domínio cibernético é desfavorável tanto para a sua segurança nacional quanto para a segurança internacional. Sendo assim, expressa que tem a intenção de contribuir para a construção de uma regulamentação internacional para o ciberespaço, por meio da elaboração de normas internacionais específicas para esse domínio que guiem o comportamento dos Estados e promova relações pacíficas no espaço cibernético.

Dessa forma, com as posições desses três países expostas, o próximo capítulo irá focar em uma análise crítica tanto sobre os dois modelos comentados, quanto sobre os posicionamentos de cada país, de forma a tecer comentários sobre os interesses envolvidos. Para além disso, irá tratar também da relação dos modelos de governança com a segurança internacional, na busca por responder à pergunta de partida e confrontar a hipótese da pesquisa, na intenção de sua validação ou falseamento.

5 A APLICABILIDADE E IMPLEMENTAÇÃO DA GOVERNANÇA GLOBAL DO CIBERESPAÇO

Entendido as características dos modelos, neste capítulo será feito uma análise crítica tanto em relação a eles, quanto em relação às posições adotadas por EUA, China e Rússia, de forma a compreender quais são as motivações que levam esses países a terem tal postura sobre a governança global do ciberespaço. A análise terá como enfoque os possíveis impactos que a implementação dos modelos possui para as relações internacionais. No caso do *multistakeholderism*, em que a administração da Internet e do ciberespaço prevalece sob o domínio de entidades transnacionais, muitas delas privadas, que tem como pretexto a garantia da qualidade técnica para exercer suas funções, significa manter o *status quo*, no qual a participação dos governos nacionais é limitada.

No caso do modelo multilateral, os governos nacionais ganhariam maior destaque, com a confecção e estabelecimento de um conjunto de normas internacionais para o ciberespaço, de forma que os Estados participem ativamente não só dessa construção, mas também do respeito e reconhecimento mútuo das normas criadas. Dessa forma, com base no conceito de governança visto ao longo do trabalho e à luz da segurança ontológica, neste capítulo será ponderado sobre as reverberações que esses modelos causam para a segurança internacional, de modo a responder à pergunta de partida e de verificar a hipótese de pesquisa.

5.1 MULTISTAKEHOLDER X MULTILATERALISMO: OS EFEITOS PRÁTICOS DAS SUAS APLICAÇÕES

Conforme mencionado no primeiro capítulo deste trabalho, o espaço cibernético pode ser entendido como um bem público global, já que seus arranjos e utilização são não excludentes, possuindo um valor social. Isso porque, ao olharmos para a Internet, temos que o seu valor social pertence ao seu papel de permitir que outros bens públicos e direitos sejam distribuídos e usufruídos, como conhecimento, educação, segurança, liberdade de expressão, liberdade de associação, entre outros (Canazza, 2018). Como consequência, o ciberespaço se mostra como um domínio e uma ferramenta tecnológica de grande capacidade para o compartilhamento de conhecimentos e informações, elementos fundamentais para a garantia de uma vida com dignidade.

Sendo assim, interpreta-se que o acesso à Internet deveria ser universal. Alguns países estabeleceram iniciativas para possibilitar o acesso para a sua população em cidades

metropolitanas. Contudo, na realidade prática do mundo, a desigualdade sobre o uso dessa tecnologia é evidente. O mercado de fornecimento de Internet, assim como o mercado de telecomunicações, apresenta características que tendem ao monopólio, como altos custos de entrada, necessidade de grande investimento em infraestrutura, um limitado número de fornecedores, concentração de competição e custos marginais que tendem a zero (Canazza, 2018). Dessa forma, assim como qualquer outro nicho de mercado, o fornecimento desse recurso acaba sendo restringido e, em âmbito global, os países mais pobres e com menores níveis de desenvolvimento econômico e tecnológico acabam sendo os mais afetados pela falta de acesso à Internet.

Essa desigualdade não se limita somente ao uso dessa tecnologia e do ciberespaço como um todo, mas ocorre também em termos de capacidade de influência, controle, gerenciamento e tomada de decisão sobre a sua arquitetura e forma de uso. Geralmente, no campo econômico, para corrigir ou mitigar certos efeitos negativos produzidos por um mercado, os governos atuam de forma a compensar a oferta ou a demanda, estabelecendo leis, taxações e regulações para chegar a uma solução benéfica para as partes (Canazza, 2018). No caso de como a Internet global está estruturada hoje, as disparidades entre os países, principalmente no que tange ao poder de decisão e influência, são evidentes e, assim, levanta-se o questionamento se por acaso deveria ser construído um mecanismo pelos governos, para regulamentar o controle dos recursos e a maneira de administrar essa tecnologia.

Isso porque, como já sabido, o ciberespaço hoje é gerido e conduzido por múltiplos atores em um modelo de *multistakeholders* por conta da própria criação e formação da Internet ao longo das últimas décadas. Ocorre que esse modelo enfrenta obstáculos na sua implementação, principalmente em relação a uma possível cooptação por interesses particulares no caso de não ser estruturado apropriadamente (Hofmann, 2016). Dessa forma, é fundamental olhar para as consequências e os efeitos que a manutenção do modelo *multistakeholder* produz no que diz respeito as relações interestatais em assuntos de governança do ciberespaço.

Não é questionável o fato de que esse modelo permite que atores de grande relevância e expertise, no ramo da administração técnica do ciberespaço, estejam envolvidos no processo de gestão desse espaço, no sentido de auxiliar na condução de uma melhor elaboração de diretrizes e procedimentos. Mas é importante questionar a sua validade e sucesso em outros critérios, não apenas técnicos, já que ele deve (ou pelo menos deveria) garantir que esse espaço, que representa um bem público global, tenha seus recursos geridos de maneira que verdadeiramente atendam os interesses dos usuários ao redor do mundo (Sahel, 2016).

Assim como expressado na Cúpula Mundial sobre a Sociedade da Informação, realizada em 2005, os princípios que devem orientar a governança da Internet são a abertura, transparência, inclusão, colaboração e igualdade, sendo princípios vistos como presentes no modelo *multistakeholder*. Isso significa que esses valores são transpassados para esse modelo, que acaba servindo como uma espécie de guardião. No estatuto da ICANN, por exemplo, que é figura central na implementação e preservação do *multistakeholder*, está presente os seguintes dispositivos na seção 1.2 sobre comprometimentos e valores fundamentais:

> (b) (ii) Buscar e apoiar uma participação ampla e informada refletindo a diversidade funcional, geográfica e cultural da Internet em todos os níveis de desenvolvimento de políticas e tomadas de decisões para assegurar que o processo de desenvolvimento de políticas de baixo para cima e *multistakeholder* seja usado para determinar o interesse público e que esses processos sejam responsáveis e transparentes; (a) (v) Tomar decisões aplicando políticas documentadas consistentes, neutras, objetivas e justas, sem destacar qualquer parte específica para tratamento discriminatório (ou seja, fazendo uma distinção injustificada e prejudicial entre diferentes partes; (a) (vi) Continuar prestando contas para a comunidade da Internet através de mecanismos definidos neste estatuto que aprimore a efetividade da ICANN. (ICANN, 2023, s.p, tradução nossa)[67]

Isso demonstra que o modelo *multistakeholder* está alinhado com princípios e valores liberais de abertura, livre circulação, transparência e prestação de contas, enfatizando até mesmo a defesa de uma neutralidade na determinação de políticas e tomadas de decisão. Essa neutralidade estaria vinculada com a intenção de elaborar e executar ações que foquem em questões técnicas e que sejam benéficas para a comunidade da Internet. Como consequência, a legitimidade atribuída à ICANN, ou ao sistema *multistakeholder* de tomada de decisão, está ligada com a expectativa de se obter políticas de alta qualidade (Hofmann, 2016). E essa expectativa ocorre justamente por conta dos princípios embutidos no modelo.

Como coloca Hortense Jongen e Jan Aart Scholte (2021), a ICANN tem promovido concertadamente o modelo *multistakeholder* e moldou a si mesma como um exemplo a ser seguido, em que uma grande quantidade de recursos, energia e tempo é dispendida para vender a ideia da ICANN. O que precisa ser observado, portanto, é se na prática esses princípios são

---

[67] Texto original: Seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet at all levels of policy development and decision-making to ensure that the bottom-up, multistakeholder policy development process is used to ascertain the global public interest and that those processes are accountable and transparent; Make decisions by applying documented policies consistently, neutrally, objectively, and fairly, without singling out any particular party for discriminatory treatment (i.e., making an unjustified prejudicial distinction between or among different parties); Remain accountable to the Internet community through mechanisms defined in these Bylaws that enhance ICANN's effectiveness.

seguidos e como isso reflete para os países e as suas relações no âmbito do setor cibernético, de forma a tecer uma análise sobre as vantagens e desvantagens que o sistema *multistakeholder* produz. Um fator que fica evidenciado é a relevância e preponderância de atores do Norte Global nos mecanismos de tomada de decisão e com participação ativa, muito em vista do histórico de construção da Internet e do modelo *multistakeholder*, em que esses atores puderam desenvolver uma maior experiência e conhecimento institucional e técnico sobre questões que envolvem o ciberespaço e suas tecnologias (Sahel, 2016).

Dessa forma, novos atores ou atores que foram excluídos historicamente no processo de formação do espaço cibernético e da Internet global não possuem a mesma força e capacidade de participação. Ou seja, interpreta-se que, de certo modo, os atores do Sul Global, tanto estatais quanto não-estatais, acabam não sendo incluídos de maneira igualitária em todo o processo de desenvolvimento de políticas e do gerenciamento do ciberespaço global, marcando um *gap* quando comparado com os países centrais. Até mesmo a organização e participação da sociedade civil em países no Sul Global passa por maiores dificuldades.

> Particularmente em países onde a desigualdade econômica e social é muito preponderante, a contínua participação de grupos locais da sociedade civil é difícil de atingir. Enquanto o discurso *multistakeholder* enfatiza a autoridade gerada por meio de processos pluripartidários, estudos empíricos apontam assimetrias de poder inerentes como a causa do fracasso (Hofmann, 2016, p. 33, tradução nossa)[68].

Sendo assim, há esforços por parte dos defensores do modelo *multistakeholder* para provar e assegurar de que se trata de um sistema inclusivo, diverso e transparente, capaz de lidar com os desequilíbrios e conflitos de interesse entre os atores (Hofmann, 2016). No entanto, a assimetria e o desequilíbrio fazem parte da realidade prática desse modelo, construindo um cenário no qual países que adotaram a Internet tardiamente e se mantiveram em uma posição periférica nos estágios de discussão sobre a governança da Internet estão se tornando vocais e se posicionando internacionalmente (Calderaro, 2021). Na prática, é possível observar esse desequilíbrio, por exemplo, nas contribuições e participações em debates e consultas públicas na ICANN.

Conforme estudo feito por Vítor M. de Oliveira (2019), foi verificado que há uma discrepância entre países e regiões em relação as suas atuações e envolvimento, de forma que os países periféricos realizam menos propostas e menos participações nas consultas públicas.

---

[68] Texto original: Particularly in countries where social and economic inequality are very pronounced, continuous participation by local civil society groups is difficult to achieve. While the multi-stakeholder discourse emphasises the authority generated through pluripartite processes, the empirical studies point out inherent power asymmetries as a cause of failure.

A pesquisa analisou todas as consultas públicas realizadas na ICANN no ano de 2018, sendo que de um total de 593 contribuições, 245 foram realizadas por EUA e Canadá, representando um percentual de 41,31% (Oliveira, 2019). Isso significa que somente dois países representam quase metade das contribuições realizadas na ICANN. Se olharmos por blocos regionais, 57,84% das contribuições foram feitas pela América do Norte e Europa juntas, sendo que a África teve um percentual de 14,70% e a América Latina e Caribe somente 5,2% (Oliveira, 2019).

A divergência evidencia que há uma concentração de capacidade de influenciar as diretivas e os rumos a serem tomados a partir da estrutura *multistakeholder*, no âmbito da gestão da Internet global. O baixo percentual de participação do bloco africano e latino americano demonstra que mesmo essas regiões possuírem uma quantidade numérica maior de países, elas não conseguem ter um envolvimento e uma intervenção direta em assuntos de governança do ciberespaço como as regiões que englobam os países do considerado Norte Global. Dessa forma, se atualmente a ICANN representa a principal organização de gerenciamento da Internet e do modelo *multistakeholder*, interpreta-se que os princípios de participação igualitária, diversidade e a busca por representar o interesse público não são alcançados na experiência prática.

Como consequência, podemos dizer que não é o interesse de todos que prevalece no estabelecimento de políticas para a Internet, mas sim de um grupo de instituições e governos localizados nos considerados países ricos. Mas, com o crescimento da influência que a Internet produziu nos diversos setores da vida, os governos querem estar cada vez mais envolvidos no conteúdo e acesso dessa ferramenta, o que faz com que alguns países estejam questionando o modelo *multistakeholder* (Towers, 2014). Ocorre que os padrões de governança da Internet, envolvendo as políticas e o controle de recursos, não conseguiram acompanhar, ou ficaram para trás, dos avanços tecnológicos, o que passou a incitar preocupação à atores globais (Towers, 2014).

Sendo assim, em uma perspectiva ampla, é possível considerar que a forma como o modelo funciona permite certos caminhos invisíveis, nos quais as infraestruturas e arquiteturas institucionalizam e normalizam formas particulares de conhecer e governar (Epstein; Katzenbach; Musiani, 2016). Nesse sentido, o poder não reside somente em pontos de controle, mas também é exercido de maneira mais sútil, de forma a direcionar e constranger o comportamento online, por exemplo, através de formas específicas de websites ou estruturas de desenvolvimento de aplicativos digitais (Epstein; Katzenbach; Musiani, 2016). Com isso, como coloca Ashwin J. Mathew (2016), a Internet pode até parecer uma ferramenta descentralizada

quando pensamos na sua dimensão de comando e controle, mas em termos práticos ela é apenas um sistema distribuído, com centros de concentração de poder, sendo que existem, em regiões e países, várias redes dominantes provendo trânsito para a Internet global.

Como já mencionado no segundo capítulo, um exemplo prático da concentração de poder em relação às redes dominantes é a localização dos servidores-raiz da Internet, que se localizam em grande parte nos EUA. Mais uma vez, isso mostra o desequilíbrio global existente entre as principais ferramentas e redes de gerenciamento da Internet e, entende-se que isso produz efeitos que afetam a geopolítica e a balança de poder entre os Estados no sistema internacional. Consequentemente, o próprio modelo *multistakeholder* serve em grande medida para reforçar e manter as relações de poder existentes, sendo que os atores que possuem maiores influências e capacidades têm os seus interesses privilegiados, em que a agenda estadunidense possui maior predominância (Carr, 2015).

Se olharmos para esse contexto sob uma perspectiva de hegemonia, é possível interpretar que o ciberespaço global, a partir da Internet, foi sendo moldado a partir da visão ocidental de mundo, com base na promoção dos valores liberais estadunidenses. O entendimento trazido aqui sobre hegemonia remete ao conceito formado por Antônio Gramsci (1971), que elucida sobre o controle de narrativas e o estabelecimento de diretrizes ou da agenda a ser seguida, na busca pela construção de consenso para que a hegemonia seja determinada. Consenso não no sentido de que é elaborado, escolhido e aceito pela maioria, mas no sentido de ser seguido pela maioria por ser imposto e exportado pela figura hegemônica para o restante, indo ao encontro do seu interesse exclusivo.

Como aponta Robert Cox (1993), a hegemonia gramsciana pode ser expressada como a combinação de uma estrutura social, política e econômica determinada pela classe dominante do país central hegemônico, em que há a expansão externa dessas estruturas por meio de instituições, sejam elas sociais, culturais e tecnológicas. Assim, a percepção de hegemonia de Gramsci leva em consideração o papel de instituições como a igreja, o sistema educacional, a imprensa; isto é, todas as instituições que de certo modo atuam para a formação de um padrão de comportamentos e expectativas sobre a ordem social. Dessa forma, argumenta-se que a Internet, e o ciberespaço como um todo, se enquadram como uma nova instituição capaz de impactar esse padrão comportamental na ordem social.

Sendo assim, a implementação dessa hegemonia através do ciberespaço pode ser utilizada para influenciar o comportamento dos indivíduos, ou até mesmo para aculturar o maior número possível de indivíduos internacionalmente (Lobastova, 2020). Nesse sentido, pode ser compreendido que há uma hegemonia no ciberespaço global, pela maneira na qual ele foi e está

arquitetado, assim como pela maneira na qual funciona como uma ferramenta de propagação de elementos hegemônicos. Além disso, se aspectos como modo de produção e as relações sociais são facilitadas pela estrutura do ciberespaço, o interesse hegemônico por trás dessa estrutura exerce incidência sobre outros atores, sendo que essa incidência ocorre justamente pelo envolvimento desse interesse, representando uma consequência (Halvordsson, 2012).

Essa consequência direta impacta principalmente os países periféricos e atores com menores capacidades de projeção de poder no espaço cibernético, visto que, como expressa Cox (1993), a expansão externa dos interesses hegemônicos, ou seja, a exportação desses interesses, atinge os países mais vulneráveis, que não passaram pelo mesmo processo de transformação social e não possuem o mesmo desenvolvimento econômico do país central. Essa é a diferença e a conexão, como elucida Madeline Carr (2015), entre os produtores de regras e os tomadores de regras, em que o primeiro grupo elabora os preceitos por ter capacidade para isso e o segundo grupo somente segue esses preceitos por não conseguir fazer valer as suas próprias vontades.

Ao levar essa relação para o âmbito da governança global do espaço cibernético, a autora expressa que:

> 'Produtores de regras' e 'tomadores de regras' na governança global da Internet estão ligados por um entendimento comum de uma ideologia política e um conjunto de reivindicações normativas sobre o que a Internet "deveria" ser. Ao promover um certo modelo de governança o mais compatível com normas amplamente ressonantes como 'liberdade', 'privacidade', 'democracia', 'igualdade' e 'auto determinação política', a oposição ao modelo de *multistakeholders* se torna sinônimo de oposição a essas normas e deixa pouco espaço para visões alternativas (Carr, 2015, p. 642, tradução nossa)[69].

Essa relação entre produtores e tomadores de regras na governança global da Internet – necessário para a manutenção do modelo atual - vai ao encontro dos conceitos de condições materiais e ideias de Cox (1981), em que as condições materiais (capacidades organizacionais e tecnológicas) e as ideias (noções compartilhadas que perpetuam expectativas de comportamento) possuem uma vinculação. Isso porque, no caso do ciberespaço, as condições materiais representam o domínio dos equipamentos tecnológicos e o controle das infraestruturas; e as ideias, a ideologia e os valores políticos por trás das diretrizes estabelecidas

[69] Texto original: 'Rule makers' and 'rule takers' in global Internet governance are bound together by a shared understanding of a particular political ideology and set of normative claims about what the Internet 'should' be. By promoting a certain governance model as most compatible with widely resonant norms like 'freedom', 'privacy', 'democracy', 'equality' and 'political self-determination', opposition to multistakeholderism becomes synonymous with opposition to those norms and leaves little room for alternative views.

para a governança do espaço cibernético, sendo que em conjunto elas moldam a forma de operar desse espaço, bem como a forma de agir e de se comportar do usuário ao utilizá-lo.

Ao fim e ao cabo, a estrutura global do ciberespaço está organizada de maneira não equitativa, em que os recursos e as relações de poder são assimétricos, de maneira que quem detém as tecnologias e a capacidade de tomada de decisão consegue fazer valer os seus interesses. Nesse processo de dominação ocidental, centrado na figura estadunidense, as entidades privadas e as organizações internacionais foram cruciais, visto que entidades privadas, como a ICANN, serviram para determinar e implementar o gerenciamento e a operação do ciberespaço; e as organizações internacionais serviram como validadoras das diretrizes estabelecidas, já que nunca confrontaram o *multistakeholderism*. O IGF, por exemplo, que proporciona que múltiplos atores debatam os desafios da governança, acaba tendo a sua agenda voltada para discussões sobre procedimentos do modelo já estabelecido (Calderaro, 2021).

Sob essa perspectiva, a voz dos *stakeholders* com pouca influência, ou mais fracos, sobre a governança global do ciberespaço tem pequenas chances de impactar de maneira efetiva o resultado final de negociações ou discussões, apesar da narrativa ou falsa percepção da influência descentralizada (Calderaro, 2021), que apenas em tese coloca todos no mesmo patamar de participação e ingerência. Todo esse contexto demonstra que não é sem motivo ou sem fundamento que os EUA defendem a manutenção do *multistakeholderism* em seus documentos governamentais, prezando que o direito internacional contemporâneo é suficiente para lidar com questões e/ou adversidades que abrangem o espaço cibernético. Essa defesa ocorre pelo país norte-americano compreender que o modelo construído e executado nos dias de hoje favorece a sua posição e os seus interesses.

Essa visão não é exclusiva dos EUA, mas é presente em vários importantes países ocidentais, como Reino Unido, Canadá e membros da União Europeia (Huang; Macák, 2017). Nesse sentido, a promoção do *multistakeholderism* é feita com base nos ideais e nos valores liberais, que visam uma Internet democrática com participação e acesso plurais. No entanto, na prática essa posição funciona mais para defender os interesses estadunidenses do que os valores em si que são pregados, resultando em um cenário no qual o discurso ideológico serve para dar suporte à projeção de poder dos EUA no ciberespaço global (Deibert; Pauly, 2019).

Não é sem motivo também certa contestação por parte de alguns atores, entre eles, China e Rússia, como visto nos documentos governamentais analisados no capítulo anterior, que demonstram críticas e certo descontentamento sobre a situação atual do ciberespaço global. Dessa forma, parece ter se criado uma nova dinâmica geopolítica sobre a questão cibernética,

que tem trazido desafios diplomáticos sobre aspectos da governança da Internet, em que o papel de liderança das democracias liberais do Ocidente está sendo questionado (Calderaro, 2021). Ocorre que a descentralização sobre quem governa o ciberespaço deu espaço para que gigantes da tecnologia e atores com maiores recursos, *know-how* e capacidade dominassem não apenas o setor técnico de operabilidade da Internet e do setor cibernético, mas dominassem também a dimensão da tomada de decisões e estabelecimento de políticas para esse domínio.

A contradição do modelo *multistakeholder*, portanto, em prezar pela participação igualitária e por princípios democráticos, mas na prática não dar tanto espaço e voz para atores menores e menos relevantes é o que faz com que alguns países questionem tal modelo. Como coloca Madeline Carr (2015), um dos motivos pelo qual o arranjo de Bretton Woods perdurou foi a sua capacidade de ter mecanismos para lidar com os interesses de diversos atores, de forma a balanceá-los. No entanto, no caso da governança global do espaço cibernético, observa-se que esses interesses estão desbalanceados, em que determinados atores obtém maiores vantagens em detrimento de outros, sendo que, por conseguinte, isso tem gerado incômodos e descontentamentos.

Conforme Saeme Kim (2022) indica em seu estudo ao analisar casos de países como Singapura e Coreia do Sul, os países considerados potências médias conseguem de maneira limitada participar e fazer valer as suas intenções na dinâmica da governança cibernética global. Isso porque, segundo o autor, apesar de tentarem atuar ativamente e realizarem iniciativas, sofrem constrangimentos geopolíticos, bem como limitações devido às suas capacidades no âmbito cibernético. Nesse sentido, existir uma contestação e uma intenção, por certos Estados, de ter uma maior relevância na área da governança do ciberespaço não parece ser algo ilógico, ou algo que foge da premissa de esses atores realizarem esforços para fazer valer seus interesses e objetivos no sistema internacional.

Isso porque, se a manutenção do *status quo* beneficia determinado ator ou grupo, nesse caso os países ocidentais do Norte Global, em especial os EUA, o seu rompimento ou remodelação pode trazer vantagens para outros.

> O livre movimento global de informações (assim como a livre navegação das marinhas e satélites, e em um menor grau, aeronaves) serve ao poder hegemônico global, não porque os formuladores de políticas dos EUA acreditam no ideal dos bens comuns abertos (apesar de que alguns possam acreditar) mas porque sustentar uma posição de dominância depende na habilidade de mover bens, serviços, informações e capacidades através do ciberespaço (Deibert; Pauly, 2019, p. 84, tradução nossa)[70]

[70] Texto original: The free movement of information globally (just as with free navigation of navies and satellites, and to a lesser degree, aircraft) serves global hegemonic power, not because US policymakers believe in the ideal

Conforme mencionado sucintamente no capítulo anterior, é possível considerar que as contestações desse modelo se intensificaram após as revelações de Edward Snowden, no ano de 2013, que mostrou ao mundo que o governo estadunidense se utilizava de ferramentas cibernéticas para realizar espionagens em países. Snowden teve acesso a documentos e registros secretos por trabalhar na Agência de Segurança Nacional (NSA) dos EUA e tomou a decisão de tornar muitas dessas informações públicas, sendo que uma das revelações foi a confirmação da espionagem que o governo dos EUA realizava, em que dados de outros países, como o Brasil, eram vigiados e coletados pelo governo estadunidense (Pohle; Audenhove, 2017).

Ao tornar as informações públicas, houve uma reação política, acadêmica e da sociedade civil não apenas sobre como a Internet operava e como estava estruturada, mas também sobre o comportamento dos EUA no ciberespaço e na utilização de TICs (Pohle; Audenhove, 2017). Até mesmo alguns países da UE passaram a desacreditar do modelo *multistakeholder* após as revelações, dando certa atenção para o modelo multilateral, que tradicionalmente tem sido apoiado por países como China, Rússia e Irã (Liaropoulos, 2016). Como foi observado nos documentos oficiais de China e Rússia, existe uma desconfiança não apenas com o *multistakeholderism* e a atuação dos EUA, mas também com as entidades privadas que detém grande controle e influência na dimensão cibernética. Conforme expressa Julien Nocetti (2015), esses Estados já observavam e tinham a visão de que as políticas de privacidade adotadas por empresas como Google, Facebook e Twitter podiam servir como uma potencial ameaça a sua segurança nacional.

Assim, o modelo multilateral ganhou forças nos últimos anos como a possibilidade de ser uma via para a governança global para o espaço cibernético. Os defensores desse modelo, ou aqueles que se opõe ao *multistakeholderism*, declaram que um multilateralismo intergovernamental para lidar com a governança cibernética no mundo daria mais voz à países periféricos e melhor proteção aos interesses públicos globais (Haggart; Scholte; Tusikov, 2021). Nesse sentido, a ideia por trás do modelo multilateral, como expressado no capítulo anterior, consiste em dar mais relevância aos governos na dinâmica do gerenciamento e operacionalidade do ciberespaço, bem como nas determinações de políticas para esse domínio.

No entanto, existe a indagação de que transferir um maior poder de decisão aos governos nacionais, poderia abrir brecha para que o autoritarismo prevalecesse, em que determinados

---

of the open commons (although some very well might) but because sustaining a position of dominance depends on the ability to move goods, services, information, and capabilities across cyberspace.

Estados poderiam tirar proveito para estabelecer políticas mais duras de censura, bloqueios nos fluxos de dados e informações, etc. Mauro Santaniello (2021) expressa que um modelo multilateral voltado para uma estrutura hierárquica de comando, em que a aplicação de leis e a construção de diretrizes estivesse voltado somente à figura do Estado, se caracteriza pelo princípio da soberania digital, apoiado geralmente por governos mais autoritários. Sendo assim, seria importante que o processo de estabelecimento de uma governança global do ciberespaço, com base no multilateralismo, ocorresse com uma abordagem democrática e um processo de constitucionalização, com a limitação dos poderes de entidades privadas e o constrangimento do poder público (Santaniello, 2021).

Carol M. Glen (2014) argumenta que o modelo multilateral pode ter dois arquétipos, o repressivo e o aberto. O modelo repressivo teria a sua atenção voltada para governos que não buscam apenas fortalecer a sua própria segurança, mas possuem a intenção de transferir a responsabilidade da governança da Internet para algum órgão intergovernamental, como a UIT (Glen, 2014). Esses governos apoiam aquilo que foi proposto na Contribuição 27 na Conferência Mundial sobre Telecomunicações Internacionais (WCIT), realizada em 2012, que tinha como intenção alterar as Regulações Internacionais de Telecomunicação. A proposta em questão afrontava o formato de funcionalidade da ICANN e foi submetida por Rússia, China, Arábia Saudita, Argélia, Sudão e Egito, trazendo pontos que tratavam sobre o direito de soberania no ciberespaço, maior controle nacional sobre questões cibernéticas e igualdade entre os Estados para lidar com aspectos como nomes e domínios, endereçamento e identificação de recursos (Glen, 2014).

Já o modelo multilateral aberto seria baseado na internacionalização da governança da Internet, mas sem ter como motivação questões de controle doméstico, sendo que, nesse caso, o multilateralismo seria o princípio central a ser seguido (Glen, 2014). Esse modelo estaria ligado aos países com pouco poder na hierarquia global e que enxergam o multilateralismo como uma forma de aumentar a sua influência mundial, sendo que na WCIT de 2012 suas preocupações estavam voltadas aos aspectos de prestação de contas e não discriminação (Glen, 2014). Portanto, esses países periféricos não voltavam a sua atenção à reivindicação da soberania no ciberespaço, mas sim à desigualdade existente na gestão do ciberespaço global, na qual esses países acabam sendo excluídos ou não tendo os seus interesses representados de maneira ideal.

> Esses países procuraram internacionalizar a governança da Internet, e eles desafiaram o papel dominante da ICANN de um modo que é similar ao modelo multilateral repressivo. No entanto, para além disso, eles pressionaram para que disposições

> fossem incluídas e o tratado garantisse um acesso não discriminatório (Glen, 2014, p. 649, tradução nossa)[71].

Seja qual for o modo multilateral, supõe-se que os seus pontos de convergência são a transferência de responsabilidades e papel de dominância de um grupo de atores, estatais e não estatais, para uma maior pluralidade de participações com o ganho de relevância de outros atores; maior importância e poder de influência dos Estados em decisões de determinação de políticas para o ciberespaço global; e possibilidade de construção de normas internacionais específicas para o domínio cibernético. Dessa forma, pode-se dizer que a aplicação de um modelo multilateral de governança global para o espaço cibernético tem capacidade para alterar a dinâmica geopolítica atual em relação ao ciberespaço. Principalmente se houver a elaboração e aplicação de normas internacionais direcionadas para esse domínio, visto que algumas normas podem criar obrigações que prescrevem, proíbem ou permitem determinadas atividades e ações, ou criam direitos para os atores (Finnemore; Hollis, 2016).

Nesse sentido, ponderar e realizar uma análise crítica sobre o estabelecimento de uma governança global para o ciberespaço a partir do modelo multilateral – já que ele se sobressai como alternativa ao formato *multistakeholder* – é uma necessidade em termos das relações internacionais, especialmente nos efeitos que isso pode produzir para a segurança internacional.

5.2 A REVERBERAÇÃO DE UMA GOVERNANÇA GLOBAL PARA O CIBERESPAÇO NA SEGURANÇA INTERNACIONAL

Antes de adentrar nas reverberações do estabelecimento de uma governança global para o ciberespaço, com a finalidade de responder à pergunta de partida e verificar a hipótese proposta neste trabalho, é preciso argumentar porquê o modelo *multistakeholder* não é compreendido aqui como um modelo de governança, ao contrário do que é exposto por outros autores e instituições. O *multistakeholderism* não se encaixa como um sistema de governança global visto que não atende a todos os critérios expostos tradicionalmente por Rosenau (1992), apresentados no primeiro capítulo deste trabalho.

Isso ocorre especialmente pelo modelo *multistakeholder* não definir um sistema de regras e normas a serem seguidos pelos atores. Como pudemos ver ao longo do que foi exposto

---

[71] Texto original: These countries sought to internationalize Internet governance, and they challenged the dominant role of ICANN in a way that is similar to the repressive multilateral model. However, in addition, they pressed for provisions to be included in the treaty that would guarantee non discriminatory acess

neste trabalho, não existem normas e/ou convenções internacionais que tratam sobre o ciberespaço e regulem esse domínio, sendo que apesar da comunidade internacional aceitar a aplicação do direito internacional contemporâneo para o espaço cibernético, ainda há questionamentos e incertezas sem respostas. Isso significa que o *multistakeholderism* não consegue – e parece nem ter a pretensão de - determinar uma regulamentação específica que norteie as ações dos Estados no ciberespaço, deixando para que as normas internacionais tradicionais sejam utilizadas para isso.

Dessa forma, questões como a aplicação do princípio da soberania fica sem respostas claras e objetivas, em que a reivindicação desse princípio por parte de um Estado se torna mais um aspecto de interpretação sobre uma situação específica do que de cumprimento de regra. Essas dúvidas deixadas, ou não resolvidas, pelo modelo *multistakeholder* fazem com que se tenha a compreensão de que ele não é capaz de assegurar uma característica fundamental exposta por Rosenau (1992), que é a ordem. A governança está diretamente ligada com a construção de uma ordem, sendo interativas em vista dos arranjos e da regulamentação estabelecida a partir do sistema de regras previsto pela governança. Assim, se não há um sistema de regras e um arranjo de diretrizes e políticas que configure uma ordem a ser seguida, tanto no nível ideacional, quanto comportamental e político, isso significa que não há governança. E, se o *multistakeholderism* não consegue prover esses elementos, por conseguinte, significa que ele não consegue estabelecer uma governança.

Importante enfatizar que a descentralização presente no modelo *multistakeholder*, bem como a forte presença de atores não estatais e/ou privados, não são os motivos pelos quais esse modelo não representa uma governança, já que como expõe Rosenau (1992), a governança pode ser composta por uma coletividade tanto privada quanto pública, formal ou informal. O ponto é esse modelo não definir um conjunto de regras e diretrizes aceito e seguido por todos, ou pela maioria dos atores, de forma a gerar conformidade.

Além disso, outro fator que deve ser levado em consideração é a legitimidade, condição necessária para a existência de uma governança global. Os atores inseridos na governança devem reconhecer a autoridade das regulamentações estabelecidas e, consequentemente, aceitar seguir as suas disposições. No entanto, no modelo *multistakeholder*, algumas figuras centrais como a ICANN, acabam sendo questionadas ou confrontadas por outros atores. No caso da ICANN, importantes países na dinâmica de poder do sistema internacional, como China e Rússia a partir do que foi observado em seus documentos e declarações, contestam o formato de determinação de políticas e de participação que a entidade preza.

Com base no que foi alegado acima, conclui-se que o modelo multilateral seria o modelo responsável pelo estabelecimento de uma governança global para o espaço cibernético e, portanto, as implicações da sua possível implementação devem ser analisadas. Primeiramente, ele precisaria ser conduzido por uma organização internacional reconhecida por todos os Estados, para que assim a autoridade e a legitimidade das diretrizes não sejam descreditadas ou desrespeitadas pelos atores. Em segundo lugar, seria preciso construir, em comum acordo, regras particulares direcionadas ao ciberespaço em âmbito internacional, de forma que as dúvidas e incertezas existentes hoje, no que tange a como responder a um ataque cibernético, o que exatamente define um ataque cibernético e como reivindicar soberania no espaço cibernético, sejam respondidas e compreendidas entre os países. Em terceiro, o estabelecimento de acordos e regras comuns precisam ser respeitadas de modo a afetar o comportamento dos atores no ciberespaço. Com isso, os níveis ideacional, comportamental e político seriam atendidos.

Para isso, os países precisariam olhar para o ciberespaço como um bem público global, compreendendo que o seu usufruto não é limitado nem excludente e, por isso, deve servir ao interesse comum e não aos interesses particulares. Como bem visto, o *multistakeholderism* preza pela valorização do interesse comum, mas não consegue aplicar esse princípio na realidade prática. Sendo assim, interpreta-se que a existência de uma governança global para o ciberespaço perpassa pela consolidação do interesse comum como um norte a ser seguido, já que como lembra Kaul (2013), a melhor forma de gerir um bem público global é por meio da tomada de decisões políticas em conjunto.

No entanto, talvez essa seja a maior dificuldade a ser superada na política internacional quando o assunto é o ciberespaço, que é o alinhamento de definições e concepções entre os Estados. A comunidade internacional ainda não definiu oficialmente, por exemplo, se o Direito Internacional Humanitário é aplicável aos conflitos cibernéticos e à guerra cibernética (Guterres, 2018). É possível dizer até mesmo que não se tem uma ideia oficial e aceita internacionalmente sobre o que configura uma guerra cibernética, e o que seria capaz de ocasioná-la. Se levarmos em consideração que a aceitação do direito internacional vigente para operações no ciberespaço favorece aqueles com melhores capacidades, de modo a manter o *status quo* (Malagutti, 2022), pode-se argumentar que o conflito de interesses sobre o domínio cibernético é um obstáculo para se alcançar o consenso.

Dessa forma, manter a inexistência de regulamentos pode indicar que certos Estados podem preferir a ambiguidade que as normas internacionais tradicionais geram para o ciberespaço, em que aspectos como uso da força e dificuldade de atribuição podem ser

utilizados estrategicamente (Malagutti, 2022). Ocorre que justamente a ambiguidade e as incertezas geradas tendem a construir um cenário de desconfiança entre os Estados, visto que promove certa imprevisibilidade tanto em relação às ações cibernéticas quanto às reações. Aliás, reações essas que, nos moldes atuais, não excluem a possibilidade de serem cinéticas. Sendo assim, sob a luz da segurança ontológica, interpreta-se que o cenário atual corrobora para uma situação em que os Estados, ao não saberem como o outro irá se portar ou reagir em determinado caso ou incidente, possuem maior ansiedade e suspeita sobre a conduta do outro.

Algumas tentativas já foram feitas na intenção de criar diretrizes comuns aos Estados para regulamentar suas ações no ciberespaço. Para além dos GGEs já mencionados, as principais delas ocorreram nos anos de 2011 e 2015, com a proposta de criação do Código de Conduta Internacional para a Segurança da Informação pelos países da *Shanghai Cooperation Organization* (SCO). A primeira proposta foi enviada em 2011 para a ONU como resolução para ser aprovada pela Assembleia Geral, sendo submetida por China, Rússia, Tajiquistão e Uzbequistão. O texto reconhecia a importância das TICs no mundo e como elas colocavam desafios para a estabilidade e a segurança internacional, sendo que por conta disso, esses países enxergavam como necessário construir um código de conduta internacional com normas e regras a serem seguidos pelos Estados (Organização das Nações Unidas, 2011).

Dessa forma, era mencionado que os Estados deveriam seguir as disposições da Carta das Nações Unidas e respeitar a soberania e integridade de cada país, bem como os direitos humanos e as normas internacionais, sendo que as TICs não deveriam ser utilizadas para propósitos que desrespeitassem os preceitos mencionados e ameaçassem a segurança internacional (Organização das Nações Unidas, 2011). O Código também indicava que os Estados tinham a responsabilidade de proteger o seu espaço cibernético e infraestruturas críticas, bem como respeitar os direitos e liberdades do outro, de forma a promover uma Internet global democrática, transparente e com acesso igualitário a recursos (Organização das Nações Unidas, 2011).

A proposta não foi aceita, especialmente por países ocidentais, como os EUA, devido ao argumento de que o documento poderia legitimar práticas controversas, já que havia uma ênfase pela soberania no ciberespaço e autoridade nacional sobre a Internet (Bader, 2018). Com isso, no ano de 2015 o documento sofreu uma atualização e foi submetido novamente para a Assembleia Geral da ONU para ser debatido pela comunidade internacional. Diferente do documento anterior, o Cazaquistão e o Quirguistão também participaram da submissão em conjunto com os demais 4 países. De maneira geral, a proposta mantém grande parte dos elementos trazidos na primeira versão, reclamando pela construção de regulamentos para o

comportamento dos Estados em vista da magnitude e importância da segurança cibernética no mundo.

Dessa forma, ainda foi colocado que os países não deveriam usar TICs para interferir nos assuntos internos de outro, de modo que a soberania do ciberespaço seja respeitada e os princípios e responsabilidades expressos no direito internacional sejam garantidos (Organização das Nações Unidas, 2015). No entanto, é acrescentado que os direitos de um indivíduo no mundo material e *offline* deveriam ser os mesmos no ambiente virtual, em que os Estados seriam incumbidos de proteger e respeitar os direitos e liberdade fundamentais (Organização das Nações Unidas, 2015). Outro ponto adicionado na segunda proposta foi que todos os Estados precisariam participar de maneira igualitária e responsável da governança internacional da Internet, promovendo mecanismos de governança multilaterais, transparentes e democráticos de forma a assegurar uma distribuição equitativa de recursos (Organização das Nações Unidas, 2015).

Além disso, o documento expressava que a construção de um código de conduta serviria para desenvolver confiança entre os Estados, aumentando a previsibilidade e diminuindo a probabilidade de desentendimentos, bem como contribuiria para auxiliar países periféricos em seus esforços para desenvolver capacidades cibernéticas e diminuir a desigualdade digital existente no mundo (Organização das Nações Unidas, 2015). Contudo, a segunda versão também foi rejeitada. Observa-se, portanto, uma dificuldade em se atingir um consenso entre os Estados em relação ao ciberespaço, como ele deve ser gerido e como ele deve ser regulamentado internacionalmente. Superar esse obstáculo talvez seja o maior desafio para que a governança global do ciberespaço seja concretizada.

Atualmente, o único documento multilateral, aceito por diversos países, é a Convenção de Budapeste, elaborado originalmente pelo Conselho da Europa em 2001, que trata sobre crimes cibernéticos. Nesse sentido, a grande maioria dos países signatários são europeus, mas nos últimos anos vários países adotaram o documento internamente, como no caso do Brasil, com o objetivo de ampliar a cooperação internacional no combate ao crime cibernético. No entanto, esse tratado aborda somente sobre crimes cibernéticos, no qual aspectos como violação de dados, acesso ilegal, fraudes, direitos autorais, entre outros, são regulamentados em seus dispositivos (Conselho da Europa, 2001). Isso significa que não há como considerar esse documento uma convenção que rege sobre o comportamento dos Estados e a governança do espaço cibernético em nível internacional.

Contudo, a Convenção de Budapeste serve para mostrar que instrumentos comuns sobre o setor cibernético podem ser criados e podem ter adesão pelos países. Nesse caso, Julia Bader

(2018) levanta algumas hipóteses sobre quais países estariam mais propensos a aceitar uma regulamentação internacional para o ciberespaço, representando um rompimento com o modelo *multistakeholder*. A primeira hipótese seria que países mais autoritários teriam maior probabilidade de aceitar, para conseguirem ganhar maior influência sobre recursos e mecanismos de governança do espaço cibernético e, então, estabelecerem políticas mais repressivas (Bader, 2018). A segunda diz respeito aos países periféricos e com pouca penetração de Internet, em que o estabelecimento de uma governança multilateral poderia contribuir para esses atores ganharem maior relevância e notoriedade, conseguindo proteger os seus interesses que agora são ignorados (Bader, 2018).

A terceira indica que países menos liberais, não necessariamente autoritários, seriam mais propensos por reconhecer que existe uma hegemonia estadunidense no ciberespaço global e, assim, gostariam de não sofrerem tanto a influência hegemônica material, se opondo ao molde atual (Bader, 2018). Por último, a quarta hipótese seria que não importa o regime político ou situação do país, mas que seriam a favor de uma regulamentação por questões de segurança, comércio ou auxílio e, assim, estariam mais propensos a se alinhar ou com os moldes liberais dos EUA ou com a China a depender das suas estratégias (Bader, 2018). No fim, a autora não conseguiu encontrar evidência suficiente para comprovar que os Estados se alinhariam ou com os modelos defendidos por EUA ou pela China exclusivamente para terem a proteção dessas potências, mas não fica excluída a possibilidade de um país ser a favor da regulamentação internacional do ciberespaço por questões securitárias.

A presença de países com regimes políticos mais autoritários, no conjunto de atores que enxergam o modelo multilateral de governança global para o ciberespaço como um melhor caminho, causa uma certa suspeita a outros Estados, especialmente ocidentais e liberais, em relação não só as intenções desses países, mas também às possíveis práticas e políticas repressivas que podem ser executadas ao modelo multilateral permitir que esses países autoritários ganhem maior relevância na dinâmica de poder do ciberespaço global. Mark Raymond e Justin Sherman (2023) expressam que, devido a esse contexto, um certo multilateralismo autoritário poderia estar em vias de implementação. Uma das características desse tipo de multilateralismo é a tendência a dar vantagens e permissões para grandes potências, em que o comprometimento com o princípio de que todos têm direitos iguais é enfraquecido (Raymond; Sherman, 2023).

Outra característica é a rejeição das noções liberais de moralidade nos propósitos do Estado, em que os Estados que almejam um multilateralismo autoritário tendem a ter propósitos morais mais ligados ao coletivo, prezando pela estabilidade social e a harmonia (Raymond;

Sherman, 2023). No caso específico do ciberespaço, entende-se que o receio consiste em essas características resultar em políticas de controle do fluxo de informações, com base especialmente na determinação da soberania do ciberespaço, algo reivindicado e mencionado principalmente pela China em seus documentos oficiais. Dessa forma, aspectos como esse dependem se mudanças substanciais no multilateralismo liberal forem feitas, mas pode-se entender também que a China manifesta questões como a de soberania de modo a almejar um respeito coletivo à autodeterminação no espaço cibernético frente aos desequilíbrios existentes, e não para constituir uma autonomia Westfaliana absoluta (Hong; Harwit, 2020).

Nesse sentido, se a razão chinesa de substituir o modelo *multistakeholder* pelo multilateralismo é aumentar as capacidades estatais para que o país asiático ganhe maior legitimidade para influenciar o formato da Internet e o seu desenvolvimento (Raymond; Sherman, 2023), isso não quer dizer, necessariamente, que o governo chinês visa como objetivo maior determinar políticas de repressão no seu ciberespaço e fechamento total. No entanto, para Raymond e Sherman (2023), os esforços chineses não deixam de ser um indicativo de que o país gostaria de moldar a arquitetura global de governança do ciberespaço para um modo multilateral autoritário.

> Os esforços chineses para avançar o multilateralismo autoritário não apenas com organizações multilaterais tradicionais, mas também por minar e minimizar o papel do legado do sistema *multistakeholder* da governança da Internet estão enraizados na rejeição da concepção liberal moderna do propósito moral do Estado e do propósito moral da governança global, bem como dos compromissos relacionados a transparência e a participação independente da sociedade civil na governança global que são centrais para as práticas do multilateralismo liberal (Raymond; Sherman, 2023, p. 19, tradução nossa)[72]

Contudo, é possível argumentar que, a partir dos documentos governamentais chineses analisados no capítulo anterior, o país não expressa a intenção de rejeitar ou minar a participação da sociedade civil e acabar com a transparência dos processos que envolvem a administração da Internet e do ciberespaço global. Pode-se interpretar que, ir contra a concepção liberal moderna do propósito moral do Estado, apenas indica que a China tem uma posição de não compactuar com a forma não coletiva e de segregação na qual o espaço cibernético é gerido atualmente, enxergando que esse proposito moral liberal tende a beneficiar

[72] Texto original: Chinese efforts to advance authoritarian multilarism not only within traditional multilateral organizations but also by undermining and minimizing the role of the multistakeholder legacy system of Internet governance are rooted in rejection of the modern liberal conception of the moral purpose of the state and the moral purpose of global governance, as well as the related commitments to transparency and independent civil society participation in global governance that are central to contemporary practices of liberal multilateralism.

um grupo seleto de atores. E como foi perceptível ao longo do exposto neste trabalho, mesmo o modelo *multistakeholder* propagandear que defende uma abertura e uma participação igualitária, na prática a assimetria de poder e, por consequência, a exclusão, acabam sendo evidentes.

Dessa forma, se o governo chinês afirma nos documentos que preza por uma governança global do ciberespaço transparente e com maior participação dos Estados, não é factível simplesmente certificar que suas ações práticas não iriam condizer com os princípios explícitos devido ao seu regime político interno. Até porque criticar uma possível contradição para defender um modelo que ao fim e ao cabo é contraditório, como o *multistakeholder*, não parece ser uma crítica fundamentada. Todos esses pontos precisam ser levados em consideração na avaliação e ponderação sobre a governança global do ciberespaço porque, como bem coloca Raymond e Sherman (2023), a criação de regras e a interpretação da governança da Internet e da segurança cibernética tem o potencial para afetar questões como os direitos humanos nas tecnologias digitais e indiretamente afetar até mesmo a ordem global.

O que os Estados consideram e expressam, portanto, possuem um grande peso para a definição de políticas concretas que darão rumo as suas relações. Nesse caso, as identidades que assumem sobre si, sobre os outros e o mundo ao seu redor contribuem para a definição dessas políticas e para a elaboração de narrativas sobre como o mundo opera e sobre como deveria operar. Especificamente no caso da dimensão cibernética, enxerga-se que há duas grandes narrativas, uma voltada à manutenção do *status quo* em um molde liberal e outra mais centrada na figura do Estado, no respeito à soberania do ciberespaço como princípio norteador. As visões de mundo dos atores são elementos intrínsecos na articulação das suas políticas específicas (Barrinha; Turner, 2023), sendo que as suas interações e até sentimentos relacionados a segurança, confiança, cooperação e parcerias são influenciadas por essas visões.

No caso de China e Rússia, com base nos documentos analisados, observa-se uma confrontação contra cenário atual da Internet e do ciberespaço global por conta dos desequilíbrios e da assimetria de poder em relação ao gerenciamento de recursos, coordenação de políticas e participação. Mas em nenhuma parte os documentos chineses ou russos remetem ao estabelecimento de uma regulamentação que esteja fora da alçada da Carta das Nações Unidas e do direito internacional em geral. A crítica chinesa é mais incisiva, alegando que não se pode existir uma hegemonia cibernética, visto que isso gera apenas segurança para um ou poucos países enquanto a insegurança acaba sendo predominante para o restante.

A defesa da ONU como a organização líder na definição da governança global do ciberespaço também é outro ponto presente, no qual levanta o questionamento se a visão desses

países realmente fundamenta um possível multilateralismo autoritário, já que a ONU representa a maior entidade multilateral sob os princípios liberais no mundo. Essa defesa é justificada nos documentos pela legitimidade da organização e pela possibilidade de participação mais igualitária, visto que em documentos como a "Estratégia Internacional de Cooperação para o Ciberespaço", da China, há a ênfase que a divisão desigual faz com que haja um comportamento distinto dos países e um certo abuso pelos países com maiores capacidades (China, 2017).

Compartilhando de uma visão similar, a Rússia aponta que a ausência de normas que regulem o comportamento dos Estados no espaço cibernético é um aspecto que permite a atual desigualdade e, se seguirmos a mesma lógica, podemos argumentar que acaba permitindo comportamentos abusivos denunciados pela China, que podem contribuir para situações de instabilidades entre os Estados. Na realidade, a Rússia acusa até mesmo a falta de regulamentação possibilitar a existência de monopólios por parte das corporações transnacionais detentoras do gerenciamento técnico da Internet. Os dois países justificam as suas visões não somente na importância de se estabelecer relações menos desiguais entre os países no âmbito do ciberespaço, mas também na segurança que uma regulamentação para o espaço cibernético poderia produzir.

É claro não se pode excluir a possibilidade de esses dois países, apesar de criticarem, realizarem ações consideradas abusivas no âmbito cibernético. E, para além disso, a justificativa securitária também é utilizada como pretexto para o principal ponto que causa o receio e a preocupação dos atores ocidentais no que concerne ao autoritarismo desses dois países, que é o fator da soberania. Ambos dão destaque para esse fator nos documentos e têm em suas posições a perspectiva de que o ciberespaço deveria operar em uma lógica similar aos demais domínios, já que ele também é um domínio de poder. No entanto, as perspectivas de China e Rússia vão além por considerar que as características do espaço cibernético exigem que normas específicas de respeito à soberania do ciberespaço sejam elaboradas. Nesse sentido, é possível ponderar que esses países clamam por normas que definam como aplicar a soberania no espaço cibernético por acreditarem que a reivindicação nos moldes dos domínios tradicionais gera instabilidades entre os Estados.

Como também já comentado, essa perspectiva difere da visão estadunidense, que deixa claro em seus documentos que considera que o direito internacional, da forma como está estabelecido, é suficiente para lidar com os atritos e/ou desavenças que ocorram no domínio cibernético. Ocorre que o direito internacional contemporâneo, com base na Carta das Nações Unidas, prevê o respeito à soberania e integridade dos Estados, sendo que então isso deveria ser aplicado também ao espaço cibernético. Como consequência, isso gera a indagação de, por

quais motivos exatamente, construir normas internacionais específicas para tratar sobre a soberania no ciberespaço é visto por muitos como uma tentativa autoritária de controle, e manter as regras atuais não, sendo que estas também preveem o princípio soberano.

Como também já comentado neste trabalho, a governança e a soberania podem interagir tanto de maneira a fortalecer o princípio da soberania, como de modo a enfraquecê-lo, dependendo da forma na qual a governança será implementada e quais as regras de conduta que serão seguidas pelos atores. Ao assumir que os governos nacionais possuem seus poderes limitados pela realidade complexa do mundo interconectado atual (Benvenisti, 2016), a governança por meio de um sistema de regras pode ter a capacidade de proteger a soberania de atores mais vulneráveis que acabam sendo prejudicados pela assimetria de poder existente no sistema internacional. Sendo assim, levando esse raciocínio para o âmbito do ciberespaço, temos que a ausência de governança e regulamentação, que permite comportamentos arbitrários por parte de quem tem maior poder de influência e controle sobre o ciberespaço global, reflete um cenário de desconsideração da soberania dos Estados mais fracos. O caso Snowden, por exemplo, pode ser visto como um reflexo prático dessa desconsideração.

Consequentemente, a elaboração de regras específicas para tratar sobre a soberania no espaço cibernético poderia beneficiar o respeito e o reconhecimento da autodeterminação dos países, tanto no que tange à elaboração de políticas de segurança e defesa cibernética quanto nas interações entre os Estados nesse ambiente, especialmente em relação a ações hostis e de agressão. Isto é, a identificação de uma ação como agressiva e a possível resposta a ela seria facilitada com dispositivos que indicassem exatamente o que representa ou não uma violação de soberania no espaço cibernético a partir das suas particularidades não-físicas.

Sendo assim, a reivindicação da soberania por Rússia e China não necessariamente representa uma tentativa autoritária de controle de recursos e imposição de políticas repressivas em nome da segurança, mas pode também representar uma tentativa de estabelecer entendimentos comuns entre os Estados sobre o que as ações e condutas cibernéticas significam nas relações internacionais. Um problema a ser discutido quanto a isso é o aspecto do controle do fluxo de informações e dados, visto que esse fluxo poderia sofrer interferências pelos Estados com base na legitimidade da sua soberania. Sendo assim, questões como campanhas de desinformações, utilização de Inteligência Artificial para disseminação de informações malicionas, entre outros, teriam que ser pensadas para serem resolvidas.

Dessa forma, interpreta-se que o fundamental não é simplesmente a elaboração e implementação de um conjunto de regras internacionais que regulem o comportamento dos Estados no ambiente cibernético, mas sim de que modo essas regras serão elaboradas e como

elas vão ser aceitas pela comunidade internacional. Isso porque, como podemos perceber, o regime multilateral tem outros objetivos que diferem do regime *multistakeholder*, como reger sobre a soberania estatal, promover o desenvolvimento e limitar a disseminação de conteúdos e ações ilegais através de leis, políticas e estabelecimento de normas (Oever, 2021). Nesse sentido, por estar em um estágio inicial, em que a formulação do sistema de regras e coordenação de políticas que podem compor esse regime se encontra em uma fase de idealização, a relevância da maneira em como isso pode ser construído é potencializada.

A emergência do modelo multilateral por países como China e Rússia, se concentra principalmente no aspecto de que o regime privado de múltiplos atores falha em incorporar considerações sobre o impacto social que suas deliberações e tecnologias proporcionam (Oever, 2021). Dessa forma, o modelo *multistakeholder* tem como preocupação maior promover um panorama em que a interconexão e interoperabilidade das redes no âmbito cibernético sejam aprimoradas e garantidas, sendo que o modelo multilateral de governança preza por alinhar e conciliar questões técnicas de infraestrutura e operabilidade, com questões sociais, políticas e normativas (Oever, 2021).

Um exemplo prático comentado por Niels ten Oever (2021), em sua pesquisa, para ilustrar esse conflito de interesse entre os dois modelos foi o caso do protocolo WHOIS ocorrido na última década. Nos anos de 2006 e 2007 a Comissão Europeia requisitou da ICANN alterar o acesso a informações privadas de registros em websites por meio do registro WHOIS disponível publicamente, sendo que esse registro consiste em um serviço no qual é possível acessar dados e informações de contato de usuários, incluindo o endereço físico, que tenham registrado um nome de domínio (Oever, 2021). Para a Comissão Europeia, expor esses dados publicamente representava uma violação ao direito à privacidade, mas a ICANN nunca respondeu às requisições, até que a Comissão Europeia elaborou suas próprias normas, por meio da lei de segurança *The General Data Protection Regulation*, no ano de 2016, e então a ICANN iniciou um processo para criar uma alternativa ao WHOIS existente (Oever, 2021).

Esse exemplo demonstra que, na justificativa da tecnicidade e melhor operação das redes, entidade privadas como a ICANN tendem a não atender solicitações de regulamentação por parte dos Estados, mesmo que a forma como as tecnologias e sistemas operam corresponda a violação de direitos. Com isso, o Estado, como ente que tem a responsabilidade de garantir os direitos e a segurança dos indivíduos e grupos, acaba sendo compelido a atuar para efetivar a sua função estatal. Já a ICANN, ficou uma década sem responder e promover qualquer alteração por simplesmente não ter obrigação e nem ter que prestar contas para a Comissão Europeia, que teve que agir por conta própria. Assim, isso representa um contexto de instabilidade entre

organizações privadas transnacionais e governos nacionais em relação aos diferentes objetivos e interesses que possuem, sendo que, nesse caso, o regime privado acaba tendo maior poder decisório e controle sobre os mecanismos de funcionalidade do ciberespaço.

Dessa forma, a acomodação das entidades privadas que administram a Internet em resolver ou lidar com problemas como o citado acaba fomentando a pretensão dos Estados nacionais em estabelecer um modelo multilateral de governança (Oever, 2021).

> Isso mostra que os órgãos que compõem o regime privado de governança da Internet produzem interconexões e interoperações e apoiam normas favorecendo esses resultados. Os Estados, por sua vez, buscam introduzir limitações para ajustar a rede (e seus vieses normativos) aos seus regimes normativos particulares, no qual devem tratar sobre outras questões políticas para além da maximização da interconexão (Oever, 2021, p. 68, tradução nossa)[73].

É perceptível, portanto, que uma das questões políticas na qual os Estados têm maior preocupação é com a segurança, tanto nacional quanto internacional, sendo que essa preocupação reflete na busca pela determinação de ações que preservem a estabilidade interna e externa. A questão da privacidade de dados, do caso mencionado, corresponde a uma preocupação relacionada à segurança interna dos países europeus e sua busca pela garantia de direitos fundamentais. Nesse sentido, esforços por governos nacionais para lidar com a gestão da Internet tendem a ser direcionados a ajustar, ou compensar, os aspectos técnicos com os aspectos sociais e legais (Oever, 2021) e, se projetarmos isso para o âmbito internacional na determinação de políticas que guiem as relações interestatais, temos que os governos também vão ter a tendência de direcionar seus esforços para políticas que garantam a cibersegurança e a ciberdefesa.

Nesse ponto, se os Estados vão ter maior propensão a construir normativas legais que vão ao encontro da estabilidade e da proteção de garantias e princípios fundamentais, a forma na qual o consenso pode ser alcançado na definição dessas normativas é crucial. Isso porque, não é a regulamentação por si que irá fazer com que os Estados entrem em consenso sobre suas condutas no ciberespaço, mas sim o contrário, a convergência de intenções e objetivos é que pode resultar em uma regulamentação.

Se a situação da administração do ciberespaço global atual é de hegemonia, favorecida pelo modelo *multistakeholder*, podemos considerar que somente quem representa o poder

[73] Texto original: This shows that the bodies that make up the private internet governance regime produce interconnection and interoperation and support norms favouring these outcomes. States, rather, seek to introduce limitations to fit the network (and its normative biases) to their particular norm regimes, which must adress other policies issues beyond maximising interconnection

hegemônico e quem está alinhado a ele tem maior sensação de segurança. Como consequência, o restante que ou se opõe às premissas estabelecidas, ou não está automaticamente alinhado a elas, tende a ter maior desconfiança ou sensações de vulnerabilidade. Como visto, esse é o caso dos países que não se alinham com o *multistakeholderism*, sendo que no caso de muitos países do Sul Global, o alinhamento ocorre por não terem capacidade ou força para impor as suas vontades, sendo os tomadores de regras, e não os produtores (Carr, 2015).

Dessa forma, pela perspectiva da segurança ontológica, interpreta-se que a circunstância de desequilíbrio e desigualdade entre os Estados para lidar com o ciberespaço e suas ferramentas gera um estado emocional e cognitivo de ansiedade, em vista das incertezas sobre como um Estado pode ou vai se portar nesse domínio. A incerteza da responsabilização pelos seus atos, pela ausência de regulamentação e pela subjetividade que o direito internacional possui em relação ao ciberespaço, torna o cenário mais imprevisível, já que os Estados podem ter menos receio de retaliações por ações cibernéticas. Essas ações vão depender do processo de construção de identidades e interesses por parte dos atores estatais no domínio cibernético, sendo que a falta de uma governança global dificulta a compreensão e a caracterização das identidades entre os atores.

Isto é, por não haver uma materialização prática, por meio de uma convenção reconhecida por todos, e um diálogo aberto, torna-se mais difícil saber as intenções, interesses e concepções do outro em relação ao espaço cibernético. Como consequência, como a estabilidade é um produto da percepção do ator sobre si, os outros ao redor e as suas interações (Freire, 2020), enxerga-se que um contexto onde os atores têm maior dificuldade de conceberem as percepções que possuem dos outros é um contexto que não fomenta a estabilidade, e sim a insegurança.

Sendo assim, interpreta-se que manter o *status quo* de desigualdade de participação e influência dos atores sobre o gerenciamento e determinação de políticas para a Internet e o espaço cibernético, bem como de ausência de um sistema de regras que deixe explícito tanto as ideias que os Estados possuem para esse domínio, quanto os comportamentos que podem assumir, corresponde a um contexto internacional que propicia a insegurança por ser mais propenso a causar frustrações e dubiedades. Portanto, construir um outro regime – nesse caso o regime multilateral - que vise atender aos anseios de igualdade dos Estados, em sua maioria, em que os aspectos da cibersegurança e da ciberdefesa sejam promovidos, com base no respeito mútuo da integridade territorial, representa um caminho na diminuição das indefinições e imprevisibilidades que pairam o ciberespaço nas relações internacionais.

Mas a construção desse outro regime precisa ser centrada em satisfazer o interesse comum da comunidade internacional, no qual as regras elaboradas cumpram o papel de promover a segurança entre os Estados e sejam aceitos e seguidos pela maioria. Isso porque um modelo multilateral que favoreça apenas os objetivos securitários e estratégicos de um seleto grupo de países irá criar um cenário de desconfiança e incertezas que também resultará em insegurança para outros atores.

Autores como Wolfgang Kleinwachter (2021) acreditam que não há outra alternativa para gerenciar e governar a Internet que uma abordagem *multistakeholder*. Há um entendimento de que a segurança só pode ser atingida se todos os atores, estatais e não estatais, inseridos no modelo *multistakeholder*, contribuírem realizando os seus respectivos papéis (Kleinwachter, 2021). O argumento se baseia na ideia de que apesar do formato *multistakeholder* pela ICANN permitir que certas zonas de conflito apareçam, por uma questão natural de diferentes interesses envolvidos entre múltiplos atores, os procedimentos e os consensos estabelecidos por esse modelo criaram um sistema que tem demonstrado sustentabilidade (Kleinwachter, 2021).

Além disso, é alegado que abordagens que não prezem por múltiplos atores e não sejam multissetoriais correm um risco maior de serem reduzidas e/ou sequestradas por interesses e prioridades egoístas, sendo que se governos ganham maior relevância e excluem o setor privado, poderia haver um colapso na questão econômica, técnica e de desenvolvimento do setor cibernético (Kleinwachter, 2021).

> Nas crescentes batalhas geoestratégicas no ciberespaço, é grande o risco de que a abordagem *multistakeholder* seja espremida entre interesses políticos rígidos. Isso seria um grande erro. Se potências cibernéticas ignorarem a complexidade do ecossistema da governança da Internet, elas irão falhar em alcançar resultados sustentáveis e vão provocar jogos de soma-zero que não terão nenhum vencedor. Todas as partes interessadas irão perder (Kleinwachter, 2021, p. 12, tradução nossa)[74].

Para quem defende o modelo *multistakeholder*, portanto, uma alternativa que o substitua representa um rompimento com a busca pelo interesse comum, bem como uma ruptura com um sistema sustentável em termos técnicos, em que a proeminência do setor privado assegura melhores resultados e mostra ser mais capaz de articular toda a complexidade que a Internet, e o setor cibernético em geral, exige. O problema, ou falha, dessa argumentação consiste

[74] Texto original: In the growing geo-strategic battles in cyberspace, the risk is high that the multistakeholder approach will bee squeezed between hard political interests. This would be a big mistake. If cyberpowers ignore the complexity of the Internet governance ecosystem, they will fail to reach sustainable results and provoke zero-sum games that do not know any winners. All stakeholders will lose.

justamente em o *multistakeholderism* não conseguir garantir e implementar empiricamente o interesse comum, visto que o poder decisório e a participação dos atores são desiguais e assimétricos.

Ademais, o próprio pretexto de que aumentar o papel dos governos nacionais seria prejudicial, por diminuir a eficiência técnica da administração do espaço cibernético, não consegue ter fundamento na realidade prática já que, como exposto, a ICANN ficou sob a gerência do governo estadunidense até o ano de 2016. E não só isso, mas também é possível levantar a indagação de que esse controle por parte dos EUA poderia estar ocorrendo até os dias de hoje caso as críticas e as oposições de vários países não tivessem sido feitas. Nesse sentido, Kleinwachter (2021) parece não fazer, em seu argumento, uma ponderação sobre a segurança de outros atores que não os que mais se beneficiam com a preservação do *statuos quo*.

Até mesmo o argumento de que esse formato permite consensos que o torna sustentável é questionável. Isso porque ficou claro que a comunidade internacional ainda não conseguiu chegar a um consenso sobre o estabelecimento de uma governança global para o ciberespaço. Sendo assim, esse consenso mencionado não deve dizer respeito à maioria dos atores, ou todos eles, e sim a um grupo seleto que tem maior capacidade, influência e poder decisório nos aspectos que envolvem a gestão, controle e operacionalidade do ciberespaço em nível internacional. Como consequência, é possível dizer que o *multistakeholderism* privilegia interesses específicos e, então, ele acaba fazendo aquilo que seus defensores criticam quando se fala em criar uma alternativa ao seu modelo, que é ser conduzido por prioridades egoístas de certos atores em detrimento de outros.

Se o ciberespaço é reconhecido como um domínio de poder na política internacional, julga-se que ele deveria passar por um processo de regulamentação assim como os domínios tradicionais passaram. No ano de 1944, foi elaborada e assinada a Convenção sobre Aviação Civil Internacional, tratado internacional responsável por estabelecer os direitos e responsabilidades dos Estados na utilização do espaço aéreo, regulamentando aspectos como soberania, direitos de voos, serviços aéreos, tráfego, entre outros (ICAO, 1944). Ainda em seu preâmbulo, tem-se o reconhecimento de que a aviação pode contribuir para a cooperação e interação entre as nações, mas também pode ser utilizada para a ameaça e ser transformada em um perigo para a segurança internacional e, por isso, o tratado estava sendo firmado (ICAO, 1944).

Já no ano de 1967 foi elaborado o Tratado do Espaço Sideral sob os auspícios da ONU, que consiste no documento internacional que rege as atividades dos Estados no espaço sideral. O tratado reconhece a importância da exploração do espaço sideral para o desenvolvimento das

nações e expressa que os Estados devem tomar suas ações com base na paz, regulamentando, portanto, o comportamento desses atores nesse domínio de forma a prezar pela cooperação e pela segurança internacional (Organização das Nações Unidas, 1967). Dessa forma, o documento possui elementos que abordam as características específicas desse domínio, traçando diretrizes sobre as condutas apropriadas que os Estados devem ter nele.

Outro exemplo é a Convenção das Nações Unidas sobre o Direito do Mar, celebrado no ano de 1982 pela ONU para lidar sobre os atos praticados pelos Estados no espaço marítimo. Esse documento tem como premissa a visão de que os Estados devem navegar nos mares com responsabilidades para assegurar relações pacíficas, sendo que suas diretrizes regulamentam aspectos como soberania, comunicação, controle e gestão de recursos, limites dos territórios marítimos, navegação, comércio, guerra, entre outros (Organização das Nações Unidas, 1982). Dessa forma, compreende-se que a comunidade internacional realizou esforços para construir regras, princípios e diretrizes que representam um entendimento comum sobre como as nações devem conduzir suas atividades nesses domínios.

Esses esforços tiveram como base o objetivo de preservar relações pacíficas e a segurança internacional, servindo como referência para as relações interestatais de modo a conjecturar a previsibilidade de condutas. Como consequência, considera-se que as ansiedades e as preocupações das nações em relação a utilizar e frequentar tais domínios diminuíram, a ponto de aumentarem a confiança para realizar interações e, por conseguinte, contribuírem para a formação do mundo cada vez mais interconectado, interdependente e globalizado no qual vivemos hoje. Isso significa que a mesma lógica pode ser utilizada para o espaço cibernético, que está passando por um momento parecido com o que os domínios citados – mar, ar e espaço – passaram quando começaram a ser utilizados com propósitos estratégicos pelos Estados.

Nesse sentido, respondendo à pergunta de partida, temos que a implementação de uma governança global do ciberespaço pode ser capaz de impactar as relações entre os Estados de forma a criar ordem, em que a determinação de um sistema de regras específicas para lidar com o espaço cibernético induz a uma conformidade que guiará os comportamentos desses atores nesse domínio. Como visto, o direito internacional, da maneira na qual está convencionado, propicia indagações e subjetividades que fazem com que os Estados tenham diferentes interpretações sobre as ações tomadas no espaço cibernético. Não há definições e linhas claras quanto a isso, especialmente no que concerne à dimensão não-física do ciberespaço, em que a vagueza abre caminho para que cada um possa compreender da forma que lhe for benéfica.

Dessa forma, seguindo a lógica do conceito de governança e da perspectiva da segurança ontológica, construir um sistema de regras com a coordenação de políticas e diretrizes aceitas

pela maioria e reconhecido por uma autoridade legítima, faz com que haja o estabelecimento de uma ordem que tende a prevenir conflitos. Essa prevenção ocorre por conta do aumento de previsibilidade em relação a conduta dos atores que, por consequência, gera menos sentimentos de desconfiança, ansiedades e tensões, produzindo maior sensação de segurança para as atividades realizadas no ciberespaço em âmbito internacional.

Contudo, a constituição de uma regulamentação internacional, por meio da aplicação de um modelo multilateral que resultaria em uma governança global para o ciberespaço, teria capacidade para promover segurança entre os Estados somente se estes tiverem um alinhamento de perspectivas e entendimentos que tenham como objetivo final evitar desavenças, a partir da construção de identidades e interesses não egoístas no espaço cibernético. Isso perpassa por compreender o ciberespaço como um bem público global, em que a sua gestão compartilhada deve ser feita por todos e para todos. Com isso, a construção de entendimentos comuns sobre questões como ataques cibernéticos, guerra cibernética, crimes cibernéticos, soberania no ciberespaço, segurança cibernética, defesa cibernética, roubo de dados e informações, entre outras, precisa ser feita de modo que não instigue um jogo de perde e ganha entre os Estados, mas sim um cenário de cooperação em que o interesse comum, nesse caso a segurança e a paz, prevalece.

Como nos encontramos em um contexto no qual tais entendimentos comuns e consensos ainda não foram alcançados pela comunidade internacional quando o assunto é o domínio cibernético, podemos dizer que estamos em um momento crucial no qual isso pode ser feito a partir da vontade dos Estados na definição e construção dos seus interesses no ciberespaço. A concretização da implementação da governança global para o ciberespaço, hoje representada por um modelo multilateral que serve de alternativa ao *multistakeholder*, depende de debates e alinhamento de perspectivas e concepções por parte dos Estados, que devem prezar pela harmonia ao criar normas e orientações de conduta no espaço cibernético.

Sendo assim, a hipótese levantada neste trabalho se confirma caso a construção da governança global do ciberespaço atenda a certas condições, que são alcançar o consenso a partir de visões compartilhadas e identidades que propiciem relações harmônicas; respeito pelas regras, normas e princípios criados de forma a servirem como guias para as condutas dos atores; e assegurar o interesse comum sobre os interesses particulares de forma que a participação igualitária entre as nações seja celebrada. Com essas condições, interpreta-se que a confecção de uma governança global para o ciberespaço é capaz de promover a segurança internacional, de modo a regulamentar os comportamentos dos atores que hoje possuem poucos constrangimentos para agirem no espaço cibernético.

Ao mesmo tempo em que a hipótese se mostra verdadeira com o cumprimento de determinadas condições, ela não consegue ser comprovada somente com a implementação de uma governança global para ciberespaço. Pois, se essa implementação for feita a partir de uma regulamentação construída com base em interesses particulares e conflitantes e identidades negativas, o seu sistema de regras pode não ser capaz de constituir uma governança que leve à segurança, sendo marcada por uma ordem que não promove a confiança. Esse poderia ser o caso de um multilateralismo autoritário ou repressivo para o domínio cibernético, em que por mais que fosse aceito pela maioria, na prática poderia servir para atender interesses particulares e, por consequência, gerar tensões e animosidades entre os Estados.

Dessa forma, a governança global para o ciberespaço pode ser um mecanismo na promoção e manutenção da segurança internacional, em que a formação de padrões de condutas, normas internacionais específicas e compreensões compartilhadas têm a capacidade de produzir conformidade. Conformidade essa que não existe atualmente entre a comunidade internacional, em relação a aspectos particulares do ciberespaço, como jurisdição, respostas a agressões cibernéticas, soberania, e até mesmo sobre a definição e conceito desse espaço. Sendo assim, a implementação de uma governança global para o ciberespaço segue como um caminho para a resolução de discordâncias que podem escalar para um conflito, visto que hoje o domínio cibernético tem potencial para causar danos e instabilidades em escala mundial.

5.3 CONSIDERAÇÕES DO CAPÍTULO

O capítulo se debruçou em verificar e ponderar os impactos da implementação de ambos os modelos mencionados, com a finalidade de analisar os seus efeitos práticos. Assim, observou-se que, para além de não representar uma governança por não se encaixar nas características do conceito tradicional trazido por Rosenau (1992), o modelo *multistakeholder* é marcado pelo desequilíbrio e pela assimetria entre os atores. A sua manutenção, portanto, representa a preservação do *status quo* em que determinados atores possuem maiores vantagens e proeminência no que tange à tomada de decisões e definição de políticas para o espaço cibernético global.

Além disso, a sua manutenção representa a ausência de um sistema de regras, normas e princípios que constitua uma regulamentação internacional do domínio cibernético, propiciando um cenário de múltiplas interpretações aos Estados e falta de respostas objetivas para questões cruciais como a aplicabilidade do princípio da soberania ao espaço cibernético. Dessa forma, com base na perspectiva da segurança ontológica, interpreta-se que esse cenário

tende a fomentar desentendimentos que podem provocar ansiedades e animosidades nos Estados, em que a situação de imprevisibilidade pode provocar uma maior sensação de insegurança.

Sendo assim, foi possível perceber na análise realizada no capítulo, que o modelo multilateral representa um caminho para o estabelecimento de uma governança global para o ciberespaço, com a construção e determinação de normas internacionais específicas para lidar com as particularidades do ciberespaço assim como foi feito para os domínios tradicionais comentados quando se tornaram estratégicos para os Estados. Com isso, interpreta-se que a implementação de uma governança global para o ciberespaço pode ter a capacidade de atenuar os desequilíbrios entre os atores em relação ao seu poder de influência e participação na dinâmica de governança cibernética, bem como promover a segurança internacional ao aumentar a previsibilidade e gerar conformidade entre os Estados no que tange aos seus comportamentos no ciberespaço.

6 CONCLUSÃO

Abordar sobre a governança global do ciberespaço é discutir sobre um tema com um panorama dinâmico e complexo, visto que envolve, mesmo que indiretamente, diversas áreas sociais, econômicas e políticas, perpassando desde direitos de privacidade até segurança internacional. Dentro da gama de complexidades, se encontram os desafios globais emergidos pela relevância do reino digital no mundo, que tem criado dificuldades a serem superadas tanto pelo Estado, quanto pela sociedade civil. Sendo assim, por se referir a um conjunto de regras, normas e mecanismos que orientam interações no domínio cibernético, foi observado que a governança global do ciberespaço se mostra inexistente, justamente pela falta de uma estrutura unificada.

Isso ocorre em vista do modelo *multistakeholder*, que rege o ciberespaço global atualmente, não representar uma governança ao não satisfazer, de maneira integral, os aspectos fundamentais que configuram aquilo que a define no cenário global. Dessa forma, foi possível constatar que o envolvimento de múltiplos atores não-estatais, estatais e privados na dinâmica *multistakeholder* tem como premissa a defesa de um ciberespaço aberto, com livre fluxo de informações e dados e interoperável, de modo que a qualidade técnica e a interconexão das redes seja não apenas garantida, mas também aprimorada. Contudo, enxerga-se que ao primar pelo princípio da liberdade, em que cada ator deve desempenhar sua função conforme seu papel, esse modelo acaba provocando a segregação e a manutenção de um *status quo* de assimetria de poder na definição e coordenação de políticas e procedimentos para o ciberespaço.

Nesse sentido, foi observado que toda a construção da Internet resultou no estabelecimento de uma hegemonia estadunidense, incluindo o seu setor privado, no controle e domínio das estruturas essenciais para o funcionamento dessa ferramenta, em que os países do Sul Global acabam tendo as suas participações e vontades limitadas no arranjo de tomada de decisões e estabelecimento de diretrizes. E, como o domínio cibernético hoje possibilita a projeção de poder, esses atores acabam sendo compelidos a seguir os interesses que lhes são impostos. Como consequência, em organizações como a ICANN, esses países têm pouca voz e representação, se caracterizando como os tomadores de regras, como aponta Madeline Carr (2015).

Além disso, a falta de uma regulamentação internacional para o espaço cibernético, marcada pela situação atual, faz com que exista uma espécie de zona cinzenta no direito internacional, que não consegue preencher as lacunas e indagações geradas pelo ciberespaço por conta das suas características imateriais. A ausência de uma unificação tende a levar à

ambiguidade sobre o que constitui um comportamento aceitável ou não pela comunidade internacional, aumentando a dificuldade em lidar de maneira efetiva com as ameaças cibernéticas. Como consequência, entende-se que princípios como o da soberania nacional são desafiados e os Estados ficam sem respostas objetivas em relação à sua reivindicação, já que questões como fluxo de informações e dados, atribuição e proporção não são tratados de maneira específica e adequada pelas normas internacionais atuais.

Com isso, agressões e incidentes cibernéticos como os casos mencionados da Estônia, *NotPetya* e S*tuxnet* ficam sem resoluções definitivas. Além disso, o reconhecimento da soberania no ciberespaço acaba sendo um aspecto interpretativo dos Estados a partir de situações e incidentes particulares, já que não há um entendimento comum quanto a isso. Assim, esses questionamentos sem respostas fazem com que animosidades possam ser afloradas já que o ciberespaço se tornou um ambiente de disputa de poder entre os Estados, possibilitando ações que podem levar a um conflito. Contudo, utilizando os exemplos de EUA, China e Rússia, constatamos que os países divergem no que tange aos seus entendimentos sobre como o ciberespaço deve ser regulado em âmbito internacional.

Isso significa que, apesar de essa zona cinzenta no direito internacional existir para o ciberespaço e possibilitar cenários de desavenças entre os Estados, existe uma dificuldade de construir um consenso e uma unificação sobre questões que envolvem o ciberespaço. Essa dificuldade ocorre mesmo com alguns esforços internacionais já terem sido feitos, como no caso da tentativa de criação do Código de Conduta Internacional para a Sociedade da Informação, bem como os grupos de trabalho da ONU que já tocaram no assunto. Contudo, os países do Ocidente, em especial os EUA, mantém a posição de defender o modelo *multistakeholder*, com base no argumento de que esse modelo é capaz de proporcionar um ciberespaço livre, transparente e democrático.

Ocorre que, na prática, ao beneficiar o cenário hegemônico existente, esse modelo produz uma distribuição desigual de recursos e capacidade de influência sobre a arquitetura e estrutura do ciberespaço em âmbito global. Dessa forma, as nações não têm uma participação igualitária na construção de diretrizes para a governabilidade do ciberespaço, sendo que, como foi observado, a assimetria de poder gerada faz com que determinados grupos de atores sejam beneficiados em detrimento de outros em fazer valer as suas vontades e interesses. Nesse caso, enxerga-se que os EUA e o seu setor privado acabam sendo os atores mais favorecidos e, por isso, o país norte-americano defende em seus documentos estratégicos a promoção do modelo *multistakeholder* a partir dos princípios liberais, não vendo como necessário a construção de uma regulamentação internacional específica para o espaço cibernético.

Em contrapartida, a China e a Rússia entendem que a situação atual não é favorável aos Estados, que acabam tendo as suas ações e vontades limitadas em detrimento da capacidade de atores não estatais e privados, como a ICANN, quando o assunto é a governança global da Internet e do ciberespaço. Dessa forma, o governo chinês é mais resoluto em criticar o regime *multistakeholder*, apontando suas falhas em ocasionar a desigualdade entre as nações e como isso pode resultar em instabilidades, visto que o interesse comum da comunidade internacional acaba não sendo valorizado. Ou seja, a crítica chinesa expressa que interesses particulares são postos acima do interesse comum e, com isso, a insegurança se torna um produto para aqueles que não detém o poder de decisão na dinâmica do ciberespaço global.

A Rússia, por sua vez, apesar de não expressar explicitamente que é contra o modelo *multistakeholder*, faz críticas ao cenário atual por ser marcado pela ausência de normas internacionais apropriadas para o espaço cibernético, indicando que o direito internacional tradicional não é capaz de suprir as novas dinâmicas de interações que o domínio cibernético propicia. Sendo assim, o governo russo tem a posição de que a comunidade internacional precisa elaborar uma regulamentação internacional específica para tratar sobre o ciberespaço, para que questões como a soberania nacional seja resolvida e compreendida por todos.

O aspecto da soberania é algo mencionado tanto pela Rússia, quanto pela China, pois acreditam que os países devem respeitar também as suas soberanias no ciberespaço, tanto em relação às medidas internas dos governos nacionais sobre o setor cibernético, quanto em relação às ações externas de outros atores por meio do espaço cibernético. Na realidade, foi possível notar que o governo chinês considera que, a ausência de uma governança global para o ciberespaço e o sistema de múltiplos atores atual de gerenciamento desse domínio, possibilita que atores mais fortes consigam se prevalecer e até praticar abusos contra outros por conta de suas maiores capacidades.

Dessa forma, a China apoia explicitamente a implementação de um modelo multilateral de governança para o ciberespaço, defendendo uma maior participação dos Estados nos assuntos cibernéticos e resoluções comuns entre a comunidade internacional. No entanto, vimos que existe um receio de que a determinação do multilateralismo irá abrir brechas para a proeminência do autoritarismo no ciberespaço, com ações de reivindicação da soberania que podem ir contra os princípios de liberdade no mundo digital. Mas, a implementação de uma governança global pode fazer com que a soberania de Estados mais fracos passe a ser respeitada, já que por conta da situação atual, esses atores acabam acatando as decisões dos atores mais fortes, que possuem maiores capacidades tecnológicas e poder de influência sobre o arranjo cibernético global. Assim, com a determinação de uma governança global que prevê um sistema

de regras reconhecido por todos, os Estados mais fracos podem ter os seus interesses respeitados, incluindo a sua integridade em assuntos cibernéticos.

Diante de todo o exposto, entende-se que a governança tem por característica e finalidade alcançar a conformidade entre os seus membros, algo que o modelo *multistakeholder* não consegue prover e, por isso e outros aspectos, não pode ser considerado como um exemplo de governança global para o espaço cibernético. Dessa forma, a aplicação do modelo multilateral aparece, pelo menos por hora, como uma alternativa capaz de estabelecer essa governança, ao prever uma regulamentação internacional para o ciberespaço e uma participação conjunta dos Estados por meio de um organismo internacional legitimado por todos.

Sendo assim, foi constatado que essa regulamentação poderia ter a capacidade de criar certa ordem e maior estabilidade nas interações entre os Estados ao determinar regras, diretrizes e condições para as suas condutas no domínio cibernético. Isso porque interpreta-se que o estabelecimento da governança pode servir para a harmonia e condescendência das relações interestatais do mesmo modo que as convenções internacionais para o espaço aéreo, o mar e o espaço sideral serviram. Com isso, olhando pela lente construtivista da segurança ontológica, a elaboração de um padrão de condutas no ciberespaço possibilitada pela governança global pode diminuir as incertezas, ansiedades e receios, aumentando a previsibilidade e a confiança, caso os interesses e identidades dos atores no espaço cibernético sejam construídos visando interações não conflitantes.

Como consequência, esse cenário traria uma maior segurança para as relações no espaço cibernético entre os Estados, indo ao encontro da hipótese proposta neste trabalho, visto que ao ter uma estrutura normativa e diretrizes de comportamento, bem como possíveis repressões e constrangimentos para as ações que fujam das regras estabelecidas pela comunidade internacional, os Estados se sentiriam compelidos a agir de forma adequada para a manutenção da estabilidade internacional. Sendo assim, a governança global do ciberespaço desempenha um papel fundamental na segurança internacional, e seu impacto consiste na promoção de um cenário no qual os Estados devem seguir um padrão de conduta para evitar desavenças, fazendo com que a previsibilidade seja aumentada para as ações conduzidas no espaço cibernético e um conjunto de regras aceito pela maioria seja respeitado.

Importante ressaltar que este trabalho tem como propósito somente averiguar se a governança global para o ciberespaço é capaz de ser um mecanismo de fomento da segurança internacional. Nesse sentido, urge-se para que pesquisas e trabalhos acadêmicos sejam realizados para identificar e construir um modelo sobre como deve ser o sistema de regras e a arquitetura dessa governança, elucidando sobre a participação dos atores envolvidos e os

procedimentos que devem ser tomados. Isso representaria um passo adiante na confecção de uma regulamentação internacional que leve em consideração as características e especificidades do espaço cibernético, sendo que superar os desafios dependerá da vontade dos Estados de colaborarem e construírem um cenário de confiabilidade.

7 REFERÊNCIAS

ARGENTINA. **Glosario de Términos de Ciberseguridad**. Governo da República Argentina. 2019.

BADER, Julia. **To sign or not to sign. Hegemony, Global Internet Governance, and International Telecommunication Rights**. Foreign Policy Analysis, vol. 0, p. 1-19, 2018.

BALDWIN, David A. **Power and International Relations: A Conceptual Approach**. New Jersey, Princeton University Press. 2016.

BARKIN, Samuel; CRONIN, Bruce. **The state and the nation: chaging norms and the rules of sovereignty in international relations**. International Organization, vol. 48, nº 1, p. 107-130, 1994.

BARRINHA, André; TURNER, Rebecca. **Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India**. Contemporary Security Policy, 2023.

BEAULAC, Stéphane. **The Westphalian model in defining international law: challenging the myth**. Australian Journal of Legal History, v. 8, n. 2, p. 181-213, 2004.

BRAGANÇA, Danillo A. **Soberania e Relações Internacionais: Origens, Evolução e Novos Limites**. Revista de pós-graduação lato sensu da Estácio, Rio de Janeiro, vol. 1, nº 1, 2019.

BEBBER, Robert. **Cyber power and cyber effectiveness: An analytic framework**. Comparative Strategy, 36:5, p. 426-436, 2017.

BECKER, Manuel. **When public principals give up control over private agentes: The new independence of ICANN in internet governance.** Regulation & Governance, vol. 13, p. 561-576, 2019.

BENVENISTI, Eyal. **The future of sovereignty: the nation state in the global governance space**. In: CASSESE, Sabino. **Research Handbook on Global Administrative Law**. Chaltenham: Edward Elgar, 2016.

BEYER. Richard; BRUMMER, Bradley. **Implementing Effective Cyber Security Training for End Users of Computer Networks**. Society for Human Resource Management Series, 2015.

BIERSTEKER, Thomas J.; WEBER, Cynthia. **The social construction of state sovereignty.** In: BIERSTEKER, Thomas J.; WEBER, Cynthia. **State sovereignty as social construct.** Nova York: Cambridge Univerisity Press, 1996.

BORGHARD, Erica D.; LONERGAN, Shawn W. **The Logic of Coercion in Cyberspace**. Security Studies, vol. 26, nº 3, p. 452-481, 2017.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Ministério da Defesa. Brasília, 2016. Disponível em: < https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_2016.pdf>. Acesso em: setembro de 2023.

BRASIL. **Glossário das Forças Armadas**. Ministério da Defesa, 2015.

BUZAN, Barry. **Rethinking Security after the Cold War**. Cooperation and Conflict. SAGE Publications. Vol. 32 (1). p. 5-28, 1997.

CALDERARO, Andrea. **Diplomacy and Responsabilities in the Transnational Governance of the Cyber Domain**. In: HANSEN-MAGNUSSON, Hannes; VETTERLEIN, Antje (ed.). **The Routledge Handbook of Responsability in World Politics**. New York: Routledge, 2021.

CANABARRO, Diego; GONZALES, Alexandre. **Governança Global da Internet: Um mapa da Economia Política Internacional em torno dos identificadores alfanuméricos da rede**. Revista Carta Internacional. Belo Horizonte, v. 13, nº 1, p. 248-273, 2018.

INKSTER, Niger. **Measuring Military Cyber Power**. Survival, vol. 59, nº 4, p. 27-34, 2017.

CANAZZA, Mario R. **The Internet as a global public good and the role of governments and multilateral organizations in global internet governance**. Meridiano, vol. 47, nº 19, p, 1-19, 2018.

CARR, Madeline. **Power Plays in Global Internet Governance**. Millenium Journal of International Studies, v. 43, nº 2, p. 640-659, 2015.

CHENOU, Jean-Marie. **From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multistakeholderism, and the Institutionalisation of Internet Governance in the 1990s**. Globalizations, vol. 2, p. 205-223, 2014.

CHEREPANOV, Anton; LIPOVSKY, Robert. **BlackEnergy – What we really know about the notorious cyber attacks**. Virus Bulletin Conference, outubro, 2016.

CHINA. **Estratégia Nacional para a Segurança no Ciberespaço**. Cyberspace Administration of China, 2016a. Disponível em: <www.cac.gov.cn/2016-12/27/c_1120195926.htm>. Acesso em: novembro de 2023.

CHINA. **Lei de Segurança Cibernética da República Popular da China**. Office of the Central Cyberspace Affairs Commision. Beijing, 2016b. Disponível em: <www.cac.gov.cn/2016-11/07/c_1119867116.htm>. Aceso em: novembro de 2023.

CHINA. **Estratégia Internacional de Cooperação no Ciberespaço**. Ministry of Foreign Affairs, 2017. Disponível em: < https://www.scio.gov.cn/32618/Document/1543874/1543874.htm>. Acesso em: novembro de 2023.

CHINA. **Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference**. Wuzhen, China. 2015. Disponível em: <

https://www.mfa.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html>. Acesso em: novembro de 2023.

CHINA. **Jointly Implementing the Global Security Initiative for Lasting Peace and Security of the World.** 10th Beijing Xiangshan Forum, 2023. Disponível em: < https://www.mfa.gov.cn/eng/wjbxw/202311/t20231102_11172214.html>. Acesso em: novembro de 2023.

CHOUCRI, Nazli; CLARK, David D. **Integrating Cyberspace and International Relations: The Co-Evolution Dilemma**. Massachussets Institute of Technology Political Science Department. Working Paper nº 29, p. 1-13, 2012.

CHOUCRI, Nazli. **Cyberpolitics in Internation Relations**. Cambridge: The MIT Press, 2012.

COHEN, Julie. **Cyberspace As/And Space.** Columbia Law Review, vol. 107, nº 210, p. 210-256, 2007.

CONSELHO DA EUROPA. **Convenção sobre Crime cibernético.** European Treaty Series, nº 185, Budapeste, 2001. Disponível em: < https://rm.coe.int/1680081561>. Acesso em: fevereiro de 2024.

COX, Robert. **Gramsci, hegemony and international relations: an essay in method**. In: GILL, Stephen (ed.). **Gramsci, historical materialism and international relations**. New York: Cambridge Univeristy Press, 1993.

COX, Robert. **Social Forces, States and World Orders: Beyond International Relations Theory**. Millenium Journal of International Studies, v. 10, nº 2, 1981.

CRAIGEN, Dan *et al*. **Defining Cybersecurity**. Technology Innovation Management Review, vol. 4, nº 10, 2014.

CUBA. **Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the contexto of international security**. Representaciones Diplomáticas de Cuba en El Exterior, '71 UNGA', 2017. Disponível em: <https://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>. Acesso em: outubro de 2023.

CUIHONG, Cai. **Global Cyber Governance: China's Contribution and Approach**. World Century Publishing Corporation and Shanghai Institutes for International Studies. China Quarterly of International Strategic Studies, vol. 4, nº 1, p. 55-76, 2018.

CURRAN, James. **Rethinking internet history**. In: CURRAN, James; FENTON, Natalie; FREEDMAN, Des. **Misunderstanding the Internet**. Nova York: Routledge, 2012, p. 34-67.

DAHL, Robert. **The Concept of Power**. Behavioral Science, vol. 2, nº 3, p. 201-215, 1957.

DEIBERT, Ronald J.; PAULY, Louis W. **Mutual Entanglement and Complex Sovereignty in Cyberspace**. In: BIGO, Didier et al. (ed.). **Data Politics: Worlds, Subjects, Rights**. New York: Routledge, 2019.

DEIBERT, Ronald J.; CRETE-NISHIHATA, Masashi. **Global Governance and the Spread of Cyberspace Controls**. Global Governance, Leiden, nº 18, p. 339-361, 2012.

DE RÊ, Eduardo. **Ciberespaço e Segurança Cibernética: as estratégias cibernética de EUA, China e Israel e as suas relações com a estratégia cibernética do Brasil**. 2021. 108 f. Trabalho de Conclusão de Curso – Curso de Relações Internacionais – Universidade de Santa Catarina, Florianópolis, 2021.

DELERUE, François. **Reinterpretation of Contestation of International Law in Cyberspace?.** Israel Law Review, vol. 52, nº 3, p. 295-326, 2019.

DENARDIS, Laura; RAYMOND, Mark. **Thinking Clearly about Multistakeholder Internet Governance.** Paper presented at Eighth Annual GigaNet Symposium, Bali, p. 1-18, 2013.

DENARDIS, Laura. **Introduction: Internet Governance as an Object of Research Inquiry**. In: DENARDIS, Laura *et al.* **Researching Internet Governance: Methods, Frameworks, Futures.** Londres: The MIT Press, 2020, p. 1-21.

DFI. **A Declaration for the Future of the Internet**. Department of State. 2022 Disponível em: <https://www.state.gov/declaration-for-the-future-of-the-internet>. Acesso em: novembro de 2023.

DOMANSKI, Robert. **Who Governs the Internet? The emerging policies, institutions, and governance of cyberspace**. 2013. 302f. Dissertation (Doctorate) – Philosophy, Faculty in Political Sciences, The City University of New York, 2013.

EFRONY, Dan; SHANY, Yuval. **A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice**. American Journal of International Law 112 (4): 583–657, 2018.

EILSTRUP-SANGIOVANNI, Mette. **Why the World Needs an International Cyberwar Convention**. Philosophy Technology, vol 31, p. 379-407, 2018.

ENISA. **ENISA Overview of cybersecurity and related terminology**. Agência para Rede e Segurança da Informação da União Europeia. União Europeia, 2017.

EPSTEIN, Dmitry; KATZENBACH, Christian; MUSIANI, Francesca. **Doing internet governance: practices, controversies, infrastructures, and institutions**. Internet Policy Review, vol 5, n 3, p. 1-14, 2016.

ESTADOS UNIDOS. **DoD Dictionary of Military and Associated Terms**. Department of Defense, United States. Novembro. 2021.

ESTADOS UNIDOS. **National Strategy to Secure Cyberspace**. The White House, 2003. Disponível em:

<https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **International Strategy for Cyberspace**. The White House, 2011. Disponível em: < https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **National Cyber Strategy of the United States of America**. The White House, 2018a. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **Recommendations to the President on Protecting American Cyber Interests through International Engagement**. Office of the Coordinator for Cyber Issues. 2018b. Disponível em: < https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **Estratégia de Segurança Cibernética do Departamento de Segurança Interna dos Estados Unidos**. Department of Homeland Security, 2018c. Disponível em: <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>. Acesso em: fevereiro de 2024.

ESTADOS UNIDOS. **National Cybersecurity Strategy**. The White House, 2023. Disponível em: < https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **U.S Government Submission for NETmundial**. U.S Embassy & Consulates. 2014. Disponível em: <https://br.usembassy.gov/u-s-government-submission-for-netmundial/>. Acesso em: novembro de 2023.

ESTADOS UNIDOS. **Declaração para a Cúpula da Democracia**. Department of State, 2023. Disponível em: <https://www.state.gov/declaration-of-the-summit-for-democracy-2023/>. Acesso em: novembro de 2023.

FANG, Binxing. **Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace**. Singapore: Springer Nature Singapore, 2018.

FARWELL, James; ROHOZINSKI, Rafal. **Stuxnet and the Future of Cyber War**. Survival, vol. 53, nº 1, p. 23-40, 2011.

FINNEMORE, Martha; HOLLIS, Duncan. **Constructing Norms for Global Cybersecurity**. The American Journal of International Law, vol. 110, nº 3, p. 425-479, 2016.

FORUM ECONÔMICO MUNDIAL. **The Global Risks Report**. 14. Ed. Geneva, 2019.

FÓRUM ECONÔMICO MUNDIAL. **Global Cybersecurity Outlook**. Genebra, jan., 2023.

FREIRE, Maria R. **EU and Russia competing projects in the neighbourhood: an ontological security approach**. Rev. Bras. Polílt. Int., 63(1): e013, 2020.

GLEN, Carol M. **Internet Governance: Territorializing Cyberspace?**. Politics & Policy, vol. 42, nº 5, p. 635-657, 2014.

GONÇALVES, Alcindo. **Governança global e o direito internacional público**. In: JUBILUT, Liliana Lyra. **Direito Internacional Atual**. São Paulo: Elsevier, 2014.

GUEDES, Marcos *et al.* **Guia de Defesa Cibernética na América do Sul**. Recife: Editora UFPE, 2017.

GRAMSCI, Antonio. **Selections from the prison notebooks**. Tradução por: Quentin Hoare e Geoffrey Nowell Smith. New York: International Publishers, 1971.

GUTERRES, Antonio. **Secretary-General's address at the Opening Ceremony of the Munich Security Conference.** Organização das Nações Unidas. 2018. Disponível em: < https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general%E2%80%99s-address-the-opening-ceremony-of-the-munich-security-conference-delivered>. Acesso em: janeiro de 2024.

HADDAD, Christian; BINDER, Clemens. **Governing through cybersecurity: national policy strategies, globalized (in-)security and socioethnical visions of the digital Society**. Osterreich Z Soziol, vol. 44, p. 115-134, 2019.

HAGGART, Blayne; SCHOLTE, Jan A.; TUSIKOV, Natasha. **Introduction: Return of the state?.** In: HAGGART, Blayne; TUSIKOV, Natasha; SCHOLTE, Jan A. **Power and Authority in Internet Governance**. Nova York: Routledge, 2021, p. 1-13.

HALVORDSSON, Dennis. **Securitizing the Virtuality of the Real: A Gramscian Analisys of the Securitization of U.S. Cyberspace Governance**. Bachelor Thesis in International Relations, University of Gothenburg, 2012.

HERZOG, Stephen. **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**. Journal of Strategic Security, vol. 4, nº 2, p. 49-60, 2011.

HOFMANN, Jeanette. **The Multistakeholder Concept as Narrative: A Discourse Analytical Approach**. In: DENARDIS, Laura *et al.* **Researching Internet Governance: Methods, Frameworks, Futures.** Londres: The MIT Press, 2020, p. 253-269.

HOFMANN, Jeanette. **Multi-stakeholderism in Internet governance: putting a fiction into practice**. Journal of Cyber Policy, vol. 1, nº 1, 2016.

HOLLIS, Duncan D.; OHLIN, Jens. **What if Cyberspace Were for Fighting?** Ethics & International Affairs, vol. 32, nº 4, p. 441-456, 2018.

HONG, Yu; HARWIT, Eric. **China's globalizing internet: history, power, and governance**. Chinese Journal of Communication, vol. 13, nº 1, p. 1-7, 2020.

HUANG, Zhixiong; MACÁK, Kubo. **Towards the International Rule of Law in Cyberspace: Constrasting Chinese and Western Approaches**. Oxford University Press. The Chinese Journal of International Law, p. 271-310, 2017.

ICANN. **Bylaws for Internet Corporation for Assigned Names and Numbers**. Internet Corporation for Assigned Names and Numbers, 2023. Disponível em: < https://www.icann.org/resources/pages/governance/bylaws-en>. Acesso em: janeiro de 2024.

ICANN. **Getting to know the ICANN board of directors.** Internet Corporation for Assigned Names and Numbers, 2020. Disponível em: <https://www.icann.org/en/system/files/files/get-to-know-the-icann-board-31dec20-en.pdf>. Acesso em: dezembro de 2023.

ICAO. **Convenção sobre Aviação Civil Internacional**. Organização de Aviação Civil Internacional. Chicago, 1944. Disponível em: < https://www.icao.int/publications/Documents/7300_orig.pdf>. Acesso em: fevereiro de 2024.

INNERARITY, Daniel. **La gobernanza global, de la soberania a la responsabilidad.** Revista CIDOB d'Afers Internacionals, nº 100, p. 11-23, 2012.

ISRAEL, Carolina Batista. **Território, jurisdição e ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet.** Geousp-Espaço e Tempo, vol. 24, nº 1, p. 69-82, 2020.

JESUS, Diego. **O baile do monstro: O mito da Paz de Vestfália na história das relações internacionais modernas**. História (São Paulo), vol. 29, nº 2, p. 221-232, 2010.

JONGEN, Hortense; SCHOLTE, Jan Aart. **Legitimacy in Multistakeholder Global Governance at ICANN**. Global Governance, vol. 27, p. 298-324, 2021.

JUNIOR, Luiz. **Rever ou romper** c.om **Vestfália?: por uma releitura da efetiva contribuição dos acordos de paz de 1648 à construção do modelo vestfaliano de Estados**. Revista de Direito Internacional, vol. 14, nº 1, p. 358-376, 2017.

KAUL, Inge *et al*. **Defining global public goods.** In: KAUL, Inge *et al*. **Global Public Goods: International cooperation in the 21st century.** 1. ed. Nova York: Oxford University Press, 1999, p. 2-20.

KAUL, Inge; MENDOZA, Ronald U. **Advancing the Concept of Public Goods**. In: KAUL, Inge *et al*. **Providing Global Public Goods: Managing Globalization**. New York: Oxford University Press, 2003, p. 78-112.

KAUL, Inge. **Global Public Goods: A concept for framing the Post-2015 Agenda?**. Discussion paper. Deutsches Institut fur Entwicklungspolitik, 2013.

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

KINNVALL, Catarina; MITZEN, Jennifer. **An introduction to the special issue: Ontological securities in world politics**. Cooperation and Conflict, p. 1-9, 2016.

KIM, Saeme. **Roles and Limitations of Middle Powers in Shaping Global Cyber Governance**. The International Spectator. Italian Journal of International Affairs, vol. 57, nº 3, p. 31-47, 2022.

KITTICHAISAREE, Kriangsak. **Public International Law of Cyberspace**. Cham: Springer International Publishing Switzerland, 2017.

KLEINWACHTER, Wolfgang. **Cybersecurity, internet governance, and multistakeholder approach: the role of non-state actors in internet policy making**. Cyberstability Paper Series, nº 1, p. 1-19, 2021.

KRASNER, Stephen. **Structural Causes and Regime Consequences: Regime as Intervening Variables**. International Organization, vol. 36, nº 2, p. 185-205, 1982.

KRASNER, Stephen D.; WEINSTEIN, Jeremy M. **Improving Governance from the Outside In**. Annual Review of Political Science, vol. 17, p. 123-145, março, 2014.

KRASNER, Stephen D. **Rethinking the sovereign state model**. Review of International Studies, Cambridge, vol. 27, p. 17-42, 2001.

KRASZNAY, Csaba. **Case Study: The NotPetya Campaign.** In: BERNÁT, Torok. **Információ- és kiberbiztonság**. Budapeste: Ludovika Egyetemi Kiadó, 2020, p. 485-499.

KU, Charlotte. **International Law, International Relations and Global Governance**. Nova York: Routledge, 2012.

KUEHL, Daniel T. **From Cyberspace to Cyberpower: Defining the Problem**. In: KRAMER, Franklin et al. (ed.). **Cyberpower and National Security**. Washington: National Defence University Press and Potomac Books, 2009.

LAMBACH, Daniel. **The Territorialization of Cyberspace**. International Studies Review (0), p. 1-25, 2019.

LEE, Gun-woong; SHAO, Benjamin; VINZE, Ajay. **The Role of ICT as a Double-Edge Sword in Fostering Societal Transformations**. Journal of the Association for Information Systems, vol. 19, nº 3, p. 209-246, 2018.

LEE, Robert; ASSANTE, Michael; CONWAY, Tim. **Analysis of the Cyber Attack on the Ukrainian Power Grid**. Electricity Information Sharing and Analysis Center, março, 2016.

LEINER, Barry *et al.* **A Brief History of Internet**. Computer Communication Review, vol. 39, nº 5, outubro, 2009.

LIAROPOULOS, Andrew. **Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics**. Journal of Information Warfare, v. 15, nº 4, p. 14-26, 2016.

LOBASTOVA, Svetlana. **Geopolitics of Cyberspace and Virtual Power**. Journal of Liberal Arts and Humanities, v. 1, nº 3, 2020.

LONERGAN, Shawn. **Cyber Power and the International System**. 2017. 202f. Tese (Doutorado em Filosofia) – Faculdade de Artes e Ciências, Universidade de Columbia, 2017.

LUPOVICI, Amir. **Ontological security, cyber technology, and states responses**. European Journal of International Relations, vol. 29, nº 1, p. 153-178, 2023.

MACASKILL, Ewen. **Putin calls internet a 'CIA project' renewing fears of web breakup**. The Guardian, Londres, 2014. Disponível em: < https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia>. Acesso em: novembro de 2023.

MAINKA, Peter J. **O Congresso da Paz de Vestfália (1643-1648): convocação, negociações, resultados**. História Unisinos, vol. 25, nº 3, p. 460-472, 2021.

MAINWARING, Sarah. **Always in control? Sovereign states in cyberspace**. European Journal of International Security, vol. 5, p. 215-232, 2020.

MALAGUTTI, Marcelo. **Regulating States Cyber-Behaviour: Obstacles for a Consensus**. Nação e Defesa, nº 163, p. 93-114, dezembro, 2022.

MARTINS, Marco. **Ciberespaço: Uma Nova Realidade para a Segurança Internacional**. Revista sobre Cibersegurança do IDN. Lisboa. Nº 133. pp. 32-49. 2012.

MARLIN-BENNET, Renée. **Soft power's dark side**. Journal of Political Power, vol. 15, nº 3, Baltimore, p. 437-455, 2022.

MASOUMIFAR, Ali M. **Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet?**. Journal of Cyberspace Studies, vol. 6, nº 1, p. 1-20, 2022.

MATHEW, Ashwin J. **The myth of the decentralised internet**. Internet Policy Review, vol. 5, nº 3, p. 1-14, 2016.

MIGNOLO, Walter D. **Local Histories/Global Designs: Coloniality, Subaltern Knowledges, and Border Thinking**. Nova Jersey: Princeton Univerisity Press, 2012.

MURPHY, Craig N. **The Emergence of Global Governance**. In: In: WEISS, Thoma G.; WILKINSON, Rorden. **International Organization and Global Governance**. Nova York: Routledge, 2018, p. 25-37.

NAGAN, Winston P.; HAMMER, Craig. **The Changing Character of Sovereignty in International Law and International Relations**. Columbia Journal of Transnational Law, vol. 141, nº 43, p. 142-187, 2004.

NETO, Walfredo B. F.. **Por uma Geopolítica Cibernética: apontamentos da Grande Estratégia brasileira para uma nova dimensão da guerra**. 2013. 212f. Dissertação de Mestrado. Universidade Federal Fluminense. Niterói, RJ. 2013.

NOCETTI, Julien. **Contest and conquest: Russia and global internet governance**. International Affairs, v. 91, nº 1. p. 111-130, 2015.

NYE, Joseph. **Cyber Power**. Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, p. 1-24, 2010.

NYE, Joseph. **Soft Power**. Foreign Policy, nº 80, p. 153-171, 1990.

OEVER, Niels. **The metagovernance of internet governance**. In: HAGGART, Blayne; TUSIKOV, Natasha; SCHOLTE, Jan A. **Power and Authority in Internet Governance**. Nova York: Routledge, 2021, p. 56-76.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Tratado do Espaço Sideral**. ONU, Londres, 1967. Disponível em: < https://media.nti.org/documents/outer_space_treaty.pdf>. Acesso em: fevereiro de 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção das Nações Unidas sobre o Direito do Mar**. ONU. 1982. Disponível em: < https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf>. Acesso em: fevereiro de 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**. ONU, 1945. Disponível em: <https://www.oas.org/dil/port/1945%20Carta%20das%20Na%C3%A7%C3%B5es%20Unidas.pdf>. Acesso em: agosto de 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **International Code of Conduct for Information Security**. Assembleia Geral das Nações Unidas. A/66/359. 2011.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **International Code of Conduct for Information Security**. Assembleia Geral das Nações Unidas. A/69/723. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Global Governance: Our Global Neighborhood**. The Report of the Commission on Global Governance. ONU, 1995.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security**. Assembleia Geral das Nações Unidas. A/76/135, 2021.

OLIVEIRA, Vítor. **O multistakeholderismo global não nem multi nem global: Uma investigação sobre as estruturas coloniais da Governança da Internet da ICANN**. 2019. 97f. Dissertação (Mestrado em Direito). Faculdade de Direito, Universidade de Brasília, Brasília, 2019.

PEGRAM, Tom. **Global human rights governance and orchestration: National human rights institutions as intermediaries**. European Journal of International Relations, vol. 21, nº 3, p. 595-620, 2015.

PNUD. **Human Development Report**. Programa das Nações Unidas para o Desenvolvimento. Nova York: Oxford University Press, 1994.

POHLE, Julia; AUDENHOVE, Leo. **Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change**. Media and Communication, v. 5, nº 1, p. 1-6, 2017.

POHLE, Julia. **Digital Sovereignty: a new key concept of digital policy in Germany and Europe**. Konrad-Adenauer-Stiftung, Berlim, p. 1-26, 2020.

RAYMOND, Mark; SHERMAN, Justin. **Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice**. Contemporary Security Policy, 2023.

RAYMOND, Mark; DENARDIS, Laura. **Multistakeholderism: anatomy of an inchoate global institution**. International Theory, vol. 7, nº 3, p. 572-616, 2015.

RAZA, Salvador. **The security and defense matrix: Concepts matter in defense analysis?.** Defense and Security Analysis, vol. 21, nº 1, p. 67-78, 2005.

REUS-SMIT, Christian. **Changing Patterns of Governance: From Absolutism to Global Multilateralism**. In: PAOLINI, Albert J.; JARVIS, Anthony P.; REUS-SMIT, Christian. **Between Sovereignty and Global Governance: The United Nations, The State and Civil Society**. Londres: Macmillan Press LTD, 1998.

RID, Thomas. **Cyber War Will not Take Place**. Journal of Strategic Studies, vol. 35, nº 1, p. 5-32, 2012.

RONZONI, Miriam. **Two conceptions of state sovereignty and their implications for global institutional design**. Critical Review of International Social and Political Philosophy, vol. 15, nº 5, p. 573-591, 2012.

ROSENAU, James N. **Governance, order, and change in world politics**. In: ROSENAU, James N.; CZEMPIEL, Ernst-Otto. **Governance without government: order and change in world politics**. Cambridge: Cambridge University Press, 1992, p. 1-30.

ROSENAU, James N. **Strong Demand, Huge Supply: Governance in an Emerging Epoch**. In: BACHE, Ian; FLINDERS, Matthew. **Multi-level Governance**. Nova York: Oxford University Press, 2004, p. 31-49.

RUBIN, Barnett R. **Constructing Sovereignty for Security**. Survival, vol. 47, nº 4, p. 93-106, 2005.

RÚSSIA. **Doctrine of Information Security of the Russian Federation**. The Ministry of Foreign Affairs of the Russian Federation. 2016.

RÚSSIA. **Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030**. Decreto Presidencial, Kremlin, 2017.

RÚSSIA. **Comunicado de imprensa sobre a adoção de uma resolução russa sobre segurança da informação internacional na Assembleia Geral das Nações Unidas**. Ministério das Relações Exteriores da Federação Russa, 2018.

RÚSSIA. **Estratégia de Segurança Nacional da Federação Russa**. Decreto Presidencial, Kremlin, 2021.

RÚSSIA. **O Conceito da Política Externa da Federação Russa**. Decreto Presidencial, Kremlin, 2023.

RYAN, Johnny. **A history of the Internet and the Digital Future**. Reaktion Books, London, 2010.

SAHEL, Jean-Jacques. **Multi-stakeholder governanace: a necessity and a challenge for global governance in the twenty-first century**. Journal of Cyber Policy, vol. 11, nº 2, p, 1-19, 2016.

SALEH, Alam. **Broadening the Concept of Security: Identity and Soceital Security**. Geopolitics Quarterly, vol. 6, nº 4, p. 228-241, 2010.

SALTZMAN, Ilai. **Cyber posturing and the offense-defense balance**. Contemporary Security Policy, 34(1), p. 40–63. 2013.

SÁNCHEZ, Manuel Herrero. **Paz, razón de estado y diplomacia en la Europa de Westfalia. Los limites del triunfo del sistema de soberanía plena y la persistencia de los modelos policéntricos (1648-1713)**. Estudis. Revista de Historia Moderna, nº 41, p. 43-65, 2015.

SANTANIELLO, Mauro. **From governance denial to state regulation: A controversy-based typology of internet governance models**. In: HAGGART, Blayne; TUSIKOV, Natasha; SCHOLTE, Jan A. **Power and Authority in Internet Governance**. Nova York: Routledge, 2021, p. 15-37.

SCHERMA, Marcio. **As Fronteiras nas Relações Internacionais**. Revista Monções, vol. 1, nº 1, p. 102-132, jan/jun, 2012.

SCHMITT, Michael N.; VIHUL, Liis. **Respect for Sovereignty in Cyberspace**. Texas Law Review, vol. 95, p. 1639-1670, 2017.

SCHMITT, Michael N. **Grey Zones in the International Law of Cyberspace**. The Yale Journal of International Law, vol. 42, nº 2, p. 1-21, 2017.

STARR, Stuart H. **Toward a Preliminary Theory of Cyberpower**. In: KRAMER, Fraklin D.; STARR, Stuart H,; WENTZ, Larry K. **Cyberpower and National Security**. Dulles: National Defense University Press, 2009, p. 43-91.

SINGER, P.W; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know**. 1. ed. Oxford: Oxford University Press, 2013.

STONE, John. **Cyber War Will Take Place!**. Journal of Strategic Studies, vol. 36, nº 1, p. 101-108, 2013.

SUCHMAN, Mark C. **Managing Legitimacy: Strategic and Institutional Approaches**. Academy of Management Review, vol. 20, nº 3, p. 571-610, 1995.

TEIXIERA, Tarcisio; SABO, Isabela C. **Democracia ou autocracia informacional? O papel da Internet na Sociedade Global do Século XXI**. Revista de Direito, Governança e Novas Tecnologias, vol. 2, nº 1, p. 39-54, jan/jun, 2016.

TOWERS, Judy. **Internet Governance – Order out of Chaos.** 2014. 74f. Dissertação (Mestrado em Ciência em Segurança Cibernética). Utica College, 2014.

UIT. **Overview of cybersecurity**. União Internacional de Telecomunicações. ITU-T X.1205. 64f. 2008.

UIT. **Measuring the Information Society**. Genebra: International Telecommunication Union. 2010. Disponível em: < https://www.itu.int/ITU-D/ict/publications/idi/material/2010/MIS_2010_without_annex_4-e.pdf>. Acesso em: setembro de 2023.

VALO, Janne. **Cyber Attacks and the Use of Force in International Law**. 2014. 101f. Dissertação de Mestrado. University of Helsinki, 2014.

VENTRE, D. **Ciberguerra**. In: Academia General Militar. **Seguridad Global y Potencias Emergentes en un Mundo Multipolar.** XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza. 2012.

VERHELST, Anne; WOUTERS, Jan. **Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives**. International Organisations Research Journal, vol. 15, nº 2, p. 105-124, 2020.

WAN, Katherine S. **NotPetya, Not Warfare: Rethinking the insurance war exclusion in the context of international cyberattacks**. Washington Law Review, vol. 95, nº 3, 2020.

WANG, Guiguo. **ARE THERE INTERNATIONAL RULES GOVERNING CYBERSPACE?**. Journal of International and Comparative Law, vol. 8, nº 2, p. 357-384, 2021.

WEISS, Thomas G.; WILKINSON, Rorden. **From international organization to global governance**. In: WEISS, Thoma G.; WILKINSON, Rorden. **International Organization and Global Governance**. Nova York: Routledge, 2018, p. 1-12.

WEISS, Thomas G.; WILKINSON, Rorden. **Global Governance to the Rescue: Saving International Relations?**. Global Governance, vol. 20, p. 19-36, 2014.

WENDT, Alexander. **Anarchy is what States Make of it: The Social Construction of Power Politics**. International Organization, vol. 46, nº 2, p. 391-425, 1992.

WENDT, Alexander. **Social Theory of International Politics**. 1. ed. Cambridge: Cambridge University Press, 1999.

WILLET, Marcus. **Assessing Cyber Power**. Survival, vol. 61, nº 1, p. 85-90, 2019.

WGIG. **Report of the Working Group on Internet Governance**. Organização das Nações Unidas. Working Group on Internet Governance. 2005.

WOOD, Georgia. **Geopolitics and the Digital Domain: How Cyberspace is Impacting International Security**. Independent Study Project (ISP) Collection, 3290 SIT Study Abroad, p. 1-27, 2020.

YELI, Hao. **A Three-Perspective Theory of Cyber Sovereignty**. PRISM, vol. 7, nº 2, p. 108-115, 2017.