UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS

BÁRBARA CORDEIRO MARTINS

O BRASIL E A CONSTRUÇÃO NORMATIVA DO CIBERESPAÇO NO ÂMBITO DAS NAÇÕES UNIDAS (GGE E OEWG)

BRASÍLIA
2025

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS

Bárbara Cordeiro Martins

O BRASIL E A CONSTRUÇÃO NORMATIVA DO CIBERESPAÇO NO ÂMBITO DAS NAÇÕES UNIDAS (GGE E OEWG)

Trabalho de Conclusão de Curso apresentado à Universidade de Brasília (UnB) como requisito optativo para a obtenção do título de Bacharel em Relações Internacionais.

Orientador(a): Prof. Dr. Tânia Maria Pechir Gomes Manzur

BRASÍLIA
2025

AGRADECIMENTOS

Gostaria de primeiramente agradecer ao meu Senhor Jesus Cristo, autor e consumador da minha fé, por me sustentar em cada passo desta caminhada, guiando-me com graça e misericórdia.

À minha família, pelo amor incondicional e apoio inabalável. Ao meu pai, Dennis, e a minha mãe, Regiane, vocês sempre fizeram o possível para que nada me faltasse—são minha base, meu exemplo e minha maior segurança. À minha segunda mãe, Vanúbia, e ao meu segundo pai, Euclides, vocês são parte essencial de quem eu sou. Serei eternamente grata pelo amor e pelo carinho que me cercaram desde sempre.

Aos meus irmãos — Bianca, Gabriel, Davi e Isabela —, por cada abraço que renovou minhas forças e por todas as risadas que trouxeram leveza até nos dias mais difíceis. À minha avó Raquel, pelos cuidados diários, pelos cafezinhos e papos na cozinha, que foram verdadeiros refúgios. A senhora ilumina minha vida. Sem vocês, eu não seria quem sou.

Aos amigos que tornaram essa jornada mais leve e significativa. Em especial, Gabryelly, Glória e Suíla, que acreditaram em mim quando eu mesma duvidava, leram esse trabalho incontáveis vezes e ficaram comigo até altas horas, dividindo não só conhecimento, mas também muito afeto e cumplicidade. Eu amo vocês. Agradeço também à Lara e à Malu, e demais amigos que fiz ao longo dessa jornada na Universidade de Brasília, pela amizade sincera e pela parceria ao longo da graduação.

Aos professores do IREL, cuja dedicação e ensinamentos moldaram minha formação. Especialmente à minha orientadora, Prof. Dr. Tânia Manzur, por sua paciência, incentivo e orientações valiosas.

Ao meu estágio no Ministério das Relações Exteriores, que foi uma experiência enriquecedora e essencial para o meu crescimento acadêmico e profissional. Meu agradecimento especial aos meus supervisores, Larissa e Marcel, pelo aprendizado, apoio e pela confiança em mim depositada.

Aos amigos que fiz durante o estágio — Mariana, Antônio e Munir —, por compartilharem comigo não apenas desafios e aprendizados, mas também memórias especiais que levarei para sempre.

E, por fim, à universidade pública, por me proporcionar uma educação de qualidade e por ser um espaço de transformação, possibilidades e sonhos realizados.

RESUMO

A crescente interconexão digital e a expansão das ameaças cibernéticas tornaram a segurança no ciberespaço uma prioridade na agenda internacional. Nesse contexto, as Nações Unidas têm promovido espaços de diálogos para a construção de normativa regular o comportamento dos Estados no domínio digital, por meio de fóruns como os Grupos de Especialistas Governamentais (GGEs) e o Grupo de Trabalho Aberto (OEWG). Este estudo analisa a atuação do Brasil nesses espaços, destacando sua postura como mediador e alinhada aos princípios e tradições de sua Política Externa na formulação de normas cibernéticas. À luz do conceito de *norm bridge building*, examina-se como o Brasil conciliou interesses divergentes e promoveu a inclusão de novos atores no debate. Contribuindo para a literatura sobre cibersegurança e política externa brasileira, este trabalho busca preencher a lacuna acadêmica sobre a participação do Brasil na governança do ciberespaço.

Palavras-chave:
Segurança cibernética; Política Externa Brasileira; Nações Unidas; Normas cibernéticas.

ABSTRACT

The growing digital interconnection and the expansion of cyber threats have made cybersecurity a priority on the international agenda. In this context, the United Nations has promoted spaces for dialogue to develop norms to regulate the behavior of States in the digital domain, through forums such as the Groups of Governmental Experts (GGEs) and the Open-Ended Working Group (OEWG). This study analyzes Brazil's role in these spaces, highlighting its role as a mediator and its alignment with the principles and traditions of its Foreign Policy in the formulation of cyber norms. In light of the concept of norm bridge building, it examines how Brazil reconciled divergent interests and promoted the inclusion of new actors in the debate. Contributing to the literature on cybersecurity and Brazilian foreign policy, this work seeks to fill the academic gap on Brazil's participation in cyberspace governance.

Keywords:
Cybersecurity; Brazilian Foreign Policy; United Nations; Cyber norms.

LISTA DE ABREVIATURAS

AGNU - Assembleia Geral das Nações Unidas

CB - Construção de confiança *(Confidence building)*

CBM - Medidas de Construção de Capacidades *(Capacity building Measures)*

DIH - Direito Internacional Humanitário

GGE - Grupo de Especialistas Governamentais *(Group of Governmental Expert)*

OEWG - Grupo de Trabalho Aberto *(Open-Ended Working Group)*

ONU - Nações Unidas

PEB - Política externa brasileira

POA - Programa de Ação

TICs - Tecnologias da informação e comunicação

SUMÁRIO

INTRODUÇÃO

Problemática

O tema da segurança cibernética tem ganhado destaque nas agendas e debates internacionais nos últimos anos. Impulsionada pela crescente interconexão global, sustentada por tecnologias da informação e comunicação (TICs), a transformação tecnológica amplia tanto o potencial de inovação e desenvolvimento quanto as ameaças à segurança dos Estados. Lucas Kello (2017), em seu livro "The Virtual Weapon and International Order", argumenta que as ameaças cibernéticas desafiam profundamente os paradigmas tradicionais de segurança, reconfigurando a dinâmica entre guerra e paz.

As ameaças virtuais expandem o espectro de danos possíveis, subvertendo a definição clássica de conflitos e gerando consequências significativas para a segurança nacional e a ordem internacional. No relatório do Fórum Econômico Mundial de 2024, ataques cibernéticos, desinformação e espionagem digital aparecem em 4º lugar entre os principais riscos globais de curto prazo, com o potencial de causar mais prejuízos à segurança econômica e nacional do que alguns atos de guerra. No entanto, por não se encaixarem nas concepções convencionais de uso da força, essas ameaças permanecem em uma zona cinzenta no Direito Internacional (Eichensehr, 2022)

Diante desse cenário, é evidenciado a relevância dos instrumentos e instituições de cooperação internacional para debater e construir consensos sobre normas e regras aplicáveis ao ciberespaço. As Nações Unidas (ONU) desempenham um papel fundamental na tentativa de coordenar e fomentar a resolução de conflitos no ambiente digital. Ao definir instituições de governança para o mundo digital, buscamos normas capazes de estabelecer regras, padrões ou padrões de ações de acordo com um comportamento desejado dos atores na arena digital.

A criação de fóruns multilaterais, como o Grupo de Especialistas Governamentais sobre Desenvolvimentos das TICs (GGE) e o Grupo de Trabalho Aberto (OEWG) sobre sobre a segurança e o uso das TICs, foram responsáveis por propor uma série de normas e princípios para o comportamento responsável dos estados no ciberespaço que foram posteriormente aprovados pela Assembleia Geral. Estes são exemplos de tentativas instrumentais para contornar as incertezas e ameaças emergentes, bem como para consolidar normas consensuais que orientem a conduta dos Estados e atores não estatais nesse novo contexto.

O estudo das normas cibernéticas (*cybernorms*) é particularmente relevante, uma vez que o ciberespaço não é apenas um fenômeno tecnológico, mas também um fenômeno social em rápida evolução. A crescente tensão entre legisladores que defendem regulamentações

mais rígidas e o setor privado, que privilegia um modelo de autorregulação, evidencia a necessidade de compreender como as normas emergem, se consolidam e são aplicadas nesse ambiente dinâmico. A consideração de normas cibernéticas é crucial tanto para a formulação de restrições formais, como leis e políticas regulatórias, quanto para a adoção de mecanismos informais baseados em boas práticas e consensos internacionais.

Justificativa

A análise da política externa dos Estados, aliada ao estudo das iniciativas internacionais voltadas para a cooperação e governança do ciberespaço, é essencial para compreender os desafios e oportunidades desse novo domínio. O Brasil tem se destacado como um ator relevante nos fóruns multilaterais da ONU sobre segurança cibernética, orientando sua atuação com base em princípios constitucionais, como o respeito à democracia e aos direitos humanos, a valorização do multilateralismo, a defesa do direito internacional e a busca pelo diálogo e pela solução pacífica de controvérsias (Brasil, 2020).

Apesar da relevância do tema, há uma lacuna na literatura acadêmica brasileira sobre a participação do Brasil nesses fóruns, assim como na análise da política externa brasileira (PEB) voltada para a governança cibernética. Além disso, a produção acadêmica em língua portuguesa sobre o assunto é limitada, não sendo encontrados muitos estudos que expliquem de forma acessível e detalhada o funcionamento desses fóruns e os posicionamentos do Brasil. Assim, este trabalho busca contribuir para preencher essa lacuna, fornecendo uma análise estruturada sobre o envolvimento do Brasil, em especial, a sua diplomacia na construção de normas cibernéticas no âmbito da ONU.

A hipótese central deste estudo é que o Brasil atuou de forma coerente e contínua, alinhando-se aos princípios e objetivos históricos de sua Política Externa na construção normativa do ciberespaço. À luz do conceito de *norm bridge building* (Paulus, 2024), analisará-se o papel do Brasil como mediador entre diferentes polos de interesse, contribuindo para a conciliação de posições divergentes (Lauber; Eberli, 2021, Tiirmaa-Klaar, 2021) e a formulação de normas consensuais. Nesse contexto, o Brasil também teria se engajado ativamente na inclusão de atores tradicionalmente passivos no debate, promovendo a democratização do diálogo (Paulus, 2024). Além disso, manteve sua defesa da proteção e aplicabilidade do Direito Internacional, incluindo o Direito Internacional Humanitário e a Carta das Nações Unidas (Brasil, 2024b; Paulus, 2024). Esta autora sugere que esta continuidade da diplomacia brasileira nesse campo estaria relacionada à institucionalização de

diplomatas especializados na agenda cibernética ao longo do tempo, bem como à relativa autonomia do Itamaraty (Paulus, 2024) frente às conjunturas políticas domésticas.

Estrutura e objetivos

O presente trabalho analisará a agenda multilateral, com foco na diplomacia normativa, para examinar a construção do regime cibernético promovido pelas Nações Unidas e o papel do Brasil nesse processo. Para isso, a pesquisa será estruturada em quatro partes: A Parte I apresentará os principais conceitos e teorias que fundamentam este estudo. A Parte II abordará o histórico da atuação das Nações Unidas na formulação de normas para o ciberespaço, com ênfase nas contribuições dos Grupos de Especialistas Governamentais (GGEs). A Parte III analisará o papel do Grupo de Trabalho Aberto (OEWG) na definição de princípios para o comportamento dos Estados e os desafios enfrentados nesse processo. Por fim, a Parte IV examinará o protagonismo do Brasil nesses fóruns, destacando sua atuação estratégica na promoção de uma governança digital mais inclusiva e eficaz.

PARTE I - REFERENCIAL TEÓRICO E CONCEITUAL

1.1 Principais conceitos: ciberespaço e cibersegurança

Inovações tecnológicas, em especial aquelas desenvolvidas nas mais recentes décadas têm sido capazes de induzir países e nações em direção a intensificar sua participação em dinâmicas políticas globais, mesmo considerando um cenário em que já se estabelecia um certo grau de governança global, construído por instituições e regimes que surgiram desde Bretton Woods e se fortaleceram no período pós-Guerra Fria (Ramalho, 2023). A Internet se tornou um substrato essencial para interações econômicas, sociais e políticas nas sociedades contemporâneas de tal maneira que nem mesmo as nações mais remotas ou geridas por governos autoritários conseguiram evitá-la.

A Internet, contudo, não configura a totalidade do espaço cibernético em si; é uma parte dele. Singer e Friedman (2014) destacam a complexidade intrínseca do espaço cibernético e a dificuldade de consenso sobre nomenclaturas e definições. Para os autores, numa tentativa de simplificar o entendimento, o ciberespaço pode ser entendido como "o reino das redes de computadores (e os usuários por trás deles) em que as informações são armazenadas, compartilhadas e comunicadas online" (tradução nossa). Em definição mais completa, Lévy (1999) define o ciberespaço, ou espaço cibernético, como "um espaço de comunicação formado por sistemas eletrônicos que transmitem informações digitais", indo além de um

mero “ambiente virtual", ele engloba também uma vasta infraestrutura física e relacional, como cabos; fibras óticas e satélites, bem como empresas e sistemas de informação interconectados (Mandarino, 2011).

No contexto militar, o ciberespaço pode ser considerado como um quinto domínio geopolítico e estratégico dos Estados, para além dos domínios tradicionais como terra, mar, ar e espaço (Cloramidine; Wibisono, 2024). Entre as características distintivas desse novo domínio, destacam-se a redução das barreiras geográficas, a rapidez nas interações, os baixos custos que facilitam a entrada de novos atores e as dificuldades de atribuição, que dificultam a responsabilização e atrasam respostas a ataques (NIST, 2011). Essas particularidades apresentam novos desafios de segurança para os Estados.

Nesse contexto, torna-se relevante apresentar também o conceito de segurança cibernética, ou cibersegurança, este que, semelhantemente ao anterior, é difuso e ainda carece de consenso global consolidado, constitui-se como um dos fundamentos para o avanço da tecnologia e das relações no mundo contemporâneo (Brotherhood, 2024). De acordo com padrões internacionais, como o ISO/IEC 27032:2023[1], o termo centra-se na proteção da confidencialidade, integridade e disponibilidade das informações no ciberespaço. A ausência de uma definição unificada reflete as distintas prioridades nacionais e regionais, que influenciam a forma como cada país desenvolve e implementa suas estratégias de segurança cibernética (Hurel, 2021).

Nos Estados Unidos, a cibersegurança é interpretada como a proteção de sistemas de informação e infraestruturas críticas contra ataques cibernéticos, com ênfase em mitigar riscos para segurança nacional e econômica (NIST, 2018). A União Europeia, por outro lado, possui uma abordagem mais ampla e cooperativa, tratando a cibersegurança como a proteção de redes, sistemas de informação e usuários contra ameaças, buscando equilibrar a proteção de direitos individuais e a resiliência das infraestruturas digitais no bloco (UE, 2019/881). Já a China adota uma visão centralizada e securitária, onde a cibersegurança é integrada a sua estratégia de soberania cibernética, enfatizando o controle estatal sobre dados, infraestruturas e conteúdos digitais, com o objetivo de proteger a estabilidade social e a segurança do regime (Creemers, 2017).

No Brasil, a cibersegurança se refere ao “conjunto de normas, práticas e processos que permitem proteger sistemas críticos, informações particularmente importantes, e sobretudo pessoas de potenciais riscos e ameaças cibernéticas” (Belli, et al, 2023). Essa perspectiva enfatiza a importância de uma estratégia de cibersegurança holística que considere tanto as

[1] https://www.iso.org/standard/76070.html.

ameaças emergentes quanto a proteção eficaz das informações e sistemas críticos, essenciais para garantir a segurança nacional, os cidadãos e a estabilidade no ciberespaço (Choucri, 2012; Singer e Friedman, 2014).

1.2 Dimensões teóricas

A adoção generalizada das Tecnologias de Informação e Comunicação (TICs), agora onipresentes em todas as dimensões da vida e das sociedades, intensifica exponencialmente a vulnerabilidade de Estados e indivíduos a operações cibernéticas maliciosas, configurando um dos desafios mais complexos à paz, segurança e estabilidade internacional na atualidade (Nye JR, 2022). Nesse cenário, o uso malicioso das TICs, perpetrado por atores estatais e não estatais, aumenta continuamente em frequência, escopo e sofisticação, transformando-se em uma ameaça cada vez mais complexa e imprevisível que tem gerado prejuízos financeiros bilionários a cada ano e levantando sérias preocupações quanto à segurança nacional e às suas implicações no âmbito militar (WEF, 2024).

Exemplos notórios, como o Stuxnet – malware avançado atribuído a ações estatais que sabotaram o programa nuclear iraniano – e os ataques de ransomware que, em 2022, paralisaram instituições públicas na Costa Rica, evidenciam o impacto devastador dessas operações (Andrade, 2023). Além dos danos econômicos e sociais, como o comprometimento de infraestruturas críticas e a exposição de dados sensíveis, os ciberataques emergem como uma nova dimensão de guerra, servindo como instrumentos de desestabilização política, espionagem e potenciais conflitos interestatais no domínio digital.

Henry Kissinger (2015) destacou o ciberespaço como um verdadeiro desafio à experiência histórica humana, em razão de suas características distintivas como novo domínio. Segundo o autor, que adota uma perspectiva realista das relações internacionais, essas peculiaridades aproximariam o ciberespaço de um estado de natureza hobbesiano, caracterizado pela imprevisibilidade e pela ausência de uma ordem estabelecida (2015). No entanto, as ferramentas analíticas tradicionalmente mais recorrentes na vertente teórica do realismo, como o cálculo de poder e a dissuasão, mostram-se insuficientes para abordar as complexas implicações do domínio cibernético, que introduz novas variáveis e dinâmicas que escapam às estruturas clássicas de análise, como por exemplo a ação de atores não estatais e a interdependência não somente econômica mas propriamente conectiva.

É fundamental reconhecer que as novas complexidades do cenário internacional, especialmente no contexto das ameaças cibernéticas, não podem ser plenamente compreendidas por meio exclusivo da teoria realista. Embora o realismo continue relevante

para o cálculo de ameaças, riscos e para a análise do papel central dos Estados, ele apresenta limitações ao abordar dinâmicas mais amplas e multifacetadas (Kello, 2017). Nesse sentido, as teorias construtivista e institucional liberal ganham destaque ao oferecer perspectivas complementares, enfatizando a interdependência complexa entre os atores e o papel estratégico das instituições internacionais na promoção da cooperação, na construção de normas e na formulação de consensos.

Teóricos liberais defendem que as instituições internacionais — abrangendo regras, normas, princípios e processos de tomada de decisão globais — desempenham um papel crucial na promoção da cooperação, mesmo em cenários marcados por dilemas de segurança (Keohane, 1984). Essas instituições têm a capacidade de criar e fortalecer normas, embora estas também possam surgir em contextos domésticos e, posteriormente, se disseminar pelo sistema internacional. Ao atuarem como ferramentas que possibilitam a cooperação entre os estados, as instituições impõem restrições ao comportamento estatal. No entanto, essas limitações são geralmente aceitas como um preço necessário para alcançar a cooperação (Keohane, 1984).

No contexto das teorias de relações internacionais, normas podem ser definidas como "*a collective expectation for the proper behaviour of actors with a given identity*" (Katzenstein, 1996, apud Broeders; Van Den Berg, 2020; Finnemore, 2017), dessa forma, por não serem definidas apenas por interesses materiais ou pelo exercício do poder, podem também serem moldadas por processos sociais e culturais. Assim, o desenvolvimento de um regime normativo para o espaço cibernético é igualmente construído a partir das identidades dos atores, que influenciam e são influenciados pelo processo, tornando-se um mecanismo dinâmico e sujeito a transformações ao longo do tempo (Finnemore, 2017).

Por essa razão, o arcabouço teórico do institucionalismo, ao considerar o papel das instituições internacionais na promoção da cooperação e na formação de normas, pode ensejar uma melhor compreensão do tema da cibersegurança, na medida em que as instituições internacionais, como as Nações Unidas, têm atuado na construção de normas globais e mecanismos de governança para o ciberespaço. Ao integrar o institucionalismo e o construtivismo, podemos perceber como as normas de cibersegurança emergem não apenas da necessidade de proteger infraestruturas críticas, mas também das interações sociais que moldam as identidades e expectativas dos Estados em relação ao comportamento no ciberespaço.

1.3 Governança Internacional e a busca pela estabilidade no espaço cibernético

Os benefícios advindos do desenvolvimento tecnológico, bem como as necessidades de garantir a estabilidade do espaço cibernético têm sido amplamente discutidos, assim como os desafios associados a ele. O ciberespaço possui intrinsecamente a característica dual de poder ser utilizado tanto para fins nobres quanto para objetivos questionáveis. Por exemplo, a conectividade global, o anonimato e a falta de rastreabilidade permitem que indivíduos e máquinas acessem dados e sistemas sem a necessidade de identificação explícita, mas essas mesmas características podem ser exploradas por criminosos para cometer delitos com impunidade (GCSC, 2019).

Esses ataques, conduzidos por atores estatais e não estatais, evidenciam a necessidade de construção de uma governança internacional que seja capaz de garantir "estabilidade cibernética" (*cyber stability*), isso é, um estado ideal em que "todos os atores podem usufruir dos benefícios do ciberespaço sem medo" (Klimburg; Almeida, 2019). O alcance desse estado normativo ideal é intrinsecamente complexo e fundamenta-se em diversos princípios, como a conformidade com o Direito Internacional e o fortalecimento de capacidades. Um aspecto unificador em todas as definições de estabilidade cibernética é a tarefa primordial de estabelecer um consenso amplo sobre as "*regras do jogo*", conhecidas como normas de comportamento no ciberespaço, ou "*cyber norms*" (Klimburg; Almeida, 2019). Em um ciberespaço anárquico sem tais regras e expectativas compartilhadas de comportamento, Estados mais fortes serão livres para impor sua vontade sobre Estados mais fracos e incidentes menores podem escalar e sair do controle (Henriksen, 2018).

Diversos processos têm sido promovidos por atores estatais e não estatais para desenvolver essas normas, abrangendo contextos multilaterais, privados, industriais e multissetoriais (Ruhl et al, 2020). No âmbito multilateral, destaca-se a diplomacia normativa liderada pela Assembleia Geral da ONU, com iniciativas como o Grupo de Especialistas Governamentais (GGE) e o Grupo de Trabalho Aberto (OEWG), além de esforços de organizações como o G7, G20 e a Organização de Cooperação de Xangai.

Processos privados e industriais também desempenham papeis importantes. Especialistas independentes, como os participantes da Comissão Global para a Estabilidade do Ciberespaço, têm proposto recomendações sobre normas cibernéticas[2]. No setor industrial, iniciativas como o Cybersecurity Tech Accord da Microsoft[3] e a Charter of Trust[4] da Siemens

[2] https://hcss.nl/global-commission-on-the-stability-of-cyberspace-homepage/
[3] https://cybertechaccord.org/about/
[4] https://www.charteroftrust.com/

buscam promover práticas seguras. Já os processos multissetoriais reúnem Estados, organizações internacionais, sociedade civil e academia para discutir e avançar normas, como o Paris Call para confiança e segurança no ciberespaço[5] e o Christchurch Call contra conteúdos extremistas online[6]. Esses esforços coletivos destacam a diversidade de abordagens e a necessidade de cooperação global na governança do ciberespaço.

O presente trabalho se concentrará na análise da agenda multilateral, com ênfase na diplomacia normativa, para examinar a construção do regime cibernético promovido pelas Nações Unidas e o papel desempenhado pelo Brasil nesse processo. Nesse contexto, será apresentado o histórico do papel das Nações Unidas na construção normativa para o espaço cibernético, destacando as contribuições dos Grupos de Especialistas Governamentais (GGEs) e do Grupo de Trabalho Aberto (OEWG) na formulação de normas e princípios para o comportamento dos Estados. Além disso, serão identificados os principais desafios enfrentados ao longo desse processo, bem como irá explorar o protagonismo do Brasil em tais fóruns das Nações Unidas evidenciando sua atuação estratégica na promoção de uma governança inclusiva e eficaz para o ciberespaço.

PARTE II - A CONSTRUÇÃO NORMATIVA PARA O ESPAÇO CIBERNÉTICO: OS GGEs

Como mencionado na seção anterior, frente às incertezas advindas da utilização da tecnologia, é compreensível que os Estados possuam diferentes perspectivas quanto ao uso das Tecnologias de Informação e Comunicação (TICs), e apesar do reconhecimento dos seus inúmeros benefícios, a ambiguidade acerca de suas implicações negativas, inclusive dos possíveis usos militares, no espaço cibernético catalisou-se como temática fundamental a ser discutida nas Nações Unidas (ONU), principal instituição multilateral global.

As próximas seções serão dedicadas a apresentar uma evolução histórica dos dois principais fóruns multilaterais da ONU – os Grupos de Especialistas Governamentais (GGE) e o Grupo de Trabalho Aberto (OEWG)[7] –, seus principais marcos e avanços na temática.

[5] https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/
[6] https://www.christchurchcall.org/the-christchurch-call-commitments/
[7] “Group of Governmental Experts" (UN GGE) e “Open-Ended Working Group” (OEWG), foi utilizada a tradução dos títulos para facilitar o entendimento, mas mantive a sigla original para manter a coerência com as referências e documentos utilizados.

2.1 Grupo de Especialistas Governamentais (GGE) - Criação e formato

O discurso sobre o estabelecimento de normas para a segurança cibernética, ou "cyber-norms", foi introduzido na agenda das Nações Unidas em meados de 1998, quando a Federação da Rússia apresentou uma proposta de resolução ao Comitê de Desarmamento e Segurança, que resultou na adoção, pela Assembleia Geral, em 1999, da primeira de uma série de resoluções na temática em "*Developments in the field of information and telecommunications in the context of international security*". Afirmando que o mundo havia entrado em um novo estágio de revolução científica e tecnológica por meio do desenvolvimento e da aplicação de novas tecnologias de informação e meios de telecomunicações, a proposta russa propunha que os Estados considerassem conjuntamente as ameaças que esse rápido crescimento da dependência das TICs poderia suscitar (Nações Unidas, 1999).

A proposta russa de 1998 foi inicialmente vista com ceticismo pela comunidade internacional, que não mostrou interesse imediato em discutir a regulamentação das TICs. A iniciativa, que revelava o interesse russo para negociar um possível tratado multilateral, encontrou resistência, especialmente dos Estados Unidos, que se mostrou desinteressado em discutir a adoção de um novo tratado para regular o comportamento dos estados, ou limitar o desenvolvimento no ciberespaço; naquele primeiro momento, esse posicionamento americano foi apoiado por diversos países ocidentais (Adamson, 2020).

Nos anos subsequentes, a Rússia apresentou anualmente outras propostas de resoluções, mais ou menos semelhantes, porém, somente em 2003, a Assembleia Geral adotou resolução que estabeleceu o Grupo de Especialistas Governamentais (GGE)[8] para fomentar consensos internacionais a fim de "fortalecer a segurança dos sistemas globais de informação e telecomunicações" [A/Res.58/32 (2003)][9]. Assim, em 2004, iniciou-se a primeira sessão do GEE sob o seguinte mandato:

> "to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on [the examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems]" (Nações Unidas, 2003, p.4).

O primeiro GGE realizou suas sessões entre 2004 e 2005. Em resoluções posteriores, a Assembleia Geral das Nações Unidas (AGNU) solicitou ao Secretário-Geral a criação de outros cinco grupos com mandatos semelhantes. Esses GGEs eram formados por 15 a 25

[8] Nome original: "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security".
[9] https://documents.un.org/doc/undoc/gen/n03/454/83/pdf/n0345483.pdf.

representantes governamentais, selecionados com base em uma distribuição geográfica equitativa (Paulus, 2024; Henriksen, 2018). Essa lista de representantes incluía os cinco membros permanentes do Conselho de Segurança da ONU em todas as sessões[10], o que redundou em uma consequente super-representação da Europa em comparação com as demais regiões, como por exemplo, a América do Sul ou a África (Paulus, 2024). Ademais, os GGEs operam em uma base consensual; dessa forma, eles só publicam relatório substancial caso todos os membros concordem com o conteúdo. Se o grupo não chegar a um consenso, são publicados apenas relatórios processuais que documentam quem participou do grupo e quando as reuniões ocorreram. A Tabela 1, logo abaixo, apresenta uma visão geral dos seis GGEs, incluindo seus relatórios (processuais e substanciais), presidentes e estados-membros.

Nos GGEs, os especialistas foram selecionados, em teoria, para atuar formalmente com base em sua capacidade técnica individual. Na prática, entretanto, a maioria dos membros era composta por diplomatas ou outros funcionários governamentais. Assim, o GGE poderia ser descrito como "um processo diplomático e multilateral por natureza, mesmo que [...] não no nome" (Broeders, 2021, p. 16, apud Paulus, 2024).

[10] Ver na tabela 1.

Tabela 1 - GEEs

Ano	Relatório	Presidência	Membros
2004-2005	A/60/202[11] (Processual)	Rússia	África do Sul, Alemanha, Belarus, Brasil, Coreia do Sul, China, Estados Unidos da América, França, Índia, Jordânia, Malásia, Mali, México, Reino Unido e Rússia (15).
2009-2010	A/65/201[12] (Substantivo)	Rússia	África do Sul, Alemanha, Belarus, Brasil, Catar, China, Coreia do Sul, Estados Unidos da América, Estônia, França, Índia, Israel, Itália, Reino Unido, Rússia. (15)
2012-2013	A/68/98[13] (Substantivo)	Austrália	Alemanha, Argentina, Austrália, Belarus, Canadá, China, Egito, Estados Unidos da América, Estônia, França, Índia, Indonésia, Japão, Reino Unido, Rússia. (15)
2014-2015	A/70/174[14] (Substantivo)	Brasil	Alemanha, Belarus, Brasil, China, Coreia do Sul, Colômbia, Egito, Espanha, Estados Unidos da América, Estônia, França, Gana, Israel, Japão, Quênia, Malásia, México, Paquistão, Rússia. (20)
2016-2017	A/72/327[15] (Processual)	Alemanha	Alemanha, Austrália, Botsuana, Brasil, Canadá, Cazaquistão, China, Coreia do Sul, Cuba, Egito, Estados Unidos da América, Estônia, Finlândia, França, Índia, Indonésia, Japão, Quênia, México, Países Baixos, Reino Unido, Rússia, Senegal, Suíça. (25)
2019-2021	A/76/135[16] (Substantivo)	Brasil	África do sul, Alemanha, Austrália, Brasil, Cazaquistão, China, Estados Unidos da América, Estônia, França, Índia, Indonésia, Japão, Jordânia, Quênia, Maurício, México, Marrocos, Noruega, Países Baixos, Reino Unido, Romênia, Rússia, Singapura, Suíça, Uruguai. (25)

Fonte: Relatórios das Nações Unidas (2005b, 2010, 2013, 2015a, 2017 e 2021a). Elaborada pela autora.

2.1.2 Principais discussões e resultados alcançados

Esta seção abordará, de forma sucinta, as principais temáticas, discussões e os resultados alcançados pelos GGEs. Nesse sentido, ganham destaque as sessões dos anos

[11] https://documents.un.org/doc/undoc/gen/n05/453/63/pdf/n0545363.pdf
[12] https://documents.un.org/doc/undoc/gen/n10/469/57/pdf/n1046957.pdf
[13] https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf
[14] https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf
[15] https://documents.un.org/doc/undoc/gen/n17/257/46/pdf/n1725746.pdf
[16] https://documents.un.org/doc/undoc/gen/n21/075/86/pdf/n2107586.pdf

2009-2010, 2012-2013 e 2019-2021, por terem logrado relatórios substantivos que engendraram significativos avanços nos entendimentos normativos para o espaço cibernético que constituem o atual panorama da ONU. Tal panorama fundamenta-se, principalmente, em quatro pilares: (1) reconhecimento da aplicabilidade do Direito Internacional no ciberespaço, (2) normas não-vinculantes para o comportamento dos estados em tempos pacíficos, (3) medidas de construção de confiança (CBM)[17] no contexto cibernético e (4) construção de capacidades cibernéticas (CB)[18] (Ruhl et al, 2020; Hogeveen, 2022; Kumar et al, 2021; Hoogeveen, 2022).

Os debates nos mandatos dos GGEs concentraram-se em dois pontos principais, resumidos nas seguintes questões: "O Direito Internacional existente seria aplicável à conduta estatal relacionada às TICs? Caso sim, como ele se aplicaria? Quais novas normas ou disposições legais poderiam ser necessárias para regular adequadamente essa questão?" (Paulus, 2024). O Direito Internacional, por sua vez, pode ser entendido como um conjunto de regras para os Estados, aplicável tanto em tempos de paz quanto em tempos de guerra. Ele é geralmente associado às suas principais fontes: convenções internacionais, o costume internacional como evidência de uma prática geral aceita como lei, e os princípios gerais de direito amplamente reconhecidos (Kumar et al., 2021).

O ataque cibernético de 2007 contra o governo da Estônia[19] representou um marco no debate sobre a aplicabilidade do Direito Internacional ao evidenciar a vulnerabilidade das Tecnologias da Informação e Comunicação (TICs) e a crescente dependência dos Estados dessas infraestruturas. Atribuído ao envolvimento de outros Estados, esse episódio acentuou a sensação de insegurança e desconfiança no ciberespaço. Foi a primeira vez que tensões interestatais se manifestaram no domínio cibernético, revelando novos desafios para a segurança internacional (Adamson, 2020).

Outro evento significativo ocorreu em 2010, com o ataque cibernético conhecido como Stuxnet. Esse malware, considerado a primeira arma cibernética, foi desenvolvido pelos Estados Unidos com o apoio de Israel e teve como alvo as centrífugas de enriquecimento de urânio do Irã, explorando vulnerabilidades específicas desses equipamentos (Lopes; Oliveira,

[17] Termo original: “Confidence-Building Measures” (Nações Unidas, 2015a).
[18] Termo original: “Cyber Capacity Building” (Nações Unidas, 2015a).
[19] Em abril de 2007, a Estônia sofreu uma série de ataques cibernéticos durante 22 dias, atingindo sites governamentais, bancos, mídia e outros serviços essenciais. Os ataques ocorreram após a remoção do monumento Soldado de Bronze de Tallinn, símbolo da vitória russa na Segunda Guerra Mundial, que gerou tensão entre grupos pró-Kremlin e nacionalistas estonianos. O episódio desencadeou protestos violentos e conflitos diplomáticos, incluindo agressões físicas e ameaças de guerra. Posteriormente, a OTAN considerou plausível a hipótese de que os ataques faziam parte de uma estratégia russa para influenciar politicamente a Estônia (Santos, 2021).

2013). O software foi programado para causar a destruição física das centrífugas ao acelerar sua rotação a um ponto crítico, danificando os delicados componentes, além de interferir no fluxo de gás de urânio, reduzindo a eficiência do processo de enriquecimento. Enquanto o ataque à Estônia resultou apenas na interrupção de serviços, o Stuxnet gerou danos físicos ao hardware (Zetter, 2014, apud Paulus, 2024).

Diante das novas perspectivas destacadas por tais episódios, formuladores de políticas em todo o mundo entenderam que a segurança cibernética carecia da devida atenção, consequentemente, o debate global sobre normas cibernéticas ganhou engajamento dos atores e pode amadurecer (Tiirmaa-Klaar, 2021; Paulus, 2024). O segundo GGE (2009-2010) teve como mandato continuar a estudar ameaças existentes e potenciais na esfera da segurança da informação e possíveis medidas cooperativas para lidar com elas (Nações Unidas, 2005c). O relatório GGE de 2010 reconheceu que as ameaças cibernéticas carregam riscos significativos para a segurança pública, a segurança das nações e a estabilidade da comunidade internacional globalmente conectada" (Nações Unidas, 2010). As negociações deste GGE levaram a recomendação de que mais diálogo entre os estados seria necessário para reduzir os riscos e incertezas, bem como para proteger a infraestrutura crítica dos Estados, de modo a garantir a estabilidade e segurança cibernética. As seções de recomendações também solicitaram que medidas de construção de confiança fossem criadas para lidar com as implicações do uso estatal de TICs" (Tikk-Ringas, 2016).

Além do processo diplomático entre Estados sob a égide da ONU, os incidentes cibernéticos — o ataque à Estônia em 2007 e o caso do Stuxnet no Irã em 2010 — impulsionaram o desenvolvimento do Manual de Tallinn 1.0, posteriormente aprimorado na versão 2.0. Elaborado pelo Cooperative Cyber Defence Centre of Excellence (CCDCOE), esse manual foi uma das primeiras iniciativas acadêmicas a interpretar a prática estatal quanto à aplicabilidade do Direito Internacional às atividades cibernéticas estatais, incluindo sua relação com conflitos armados e as leis da guerra (jus ad bellum e jus in bello) (Schmitt, 2020).

Acredita-se que esses acontecimentos contribuíram significativamente para a evolução dos debates dos próximos GGEs que culminaram resultados notórios nos relatórios substantivos das sessões de 2013 e 2015 acerca de normas substanciais, algo que as reuniões anteriores ainda não haviam conseguido devido à falta de consenso (Brotherhood, 2024). Finalmente no relatório substantivo de 2013, os Estados alcançaram consenso sobre a aplicabilidade do Direito Internacional ao espaço cibernético, incluindo a adoção de medidas de construção de confiança. Nesse marco, o GGE declarou que "o Direito Internacional, em

particular a Carta da ONU, é aplicável ao espaço cibernético", reconhecendo também a soberania estatal e os direitos humanos como princípios fundamentais.

> that international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. [...] State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory; States must meet their international obligations regarding internationally wrongful acts attributable to them. (Nações Unidas, 2013)

Esse relatório destaca que a aplicação de normas derivadas do Direito Internacional existente, relacionadas ao uso das TICs pelos Estados, é essencial para reduzir os riscos à paz, segurança e estabilidade internacionais. Ele recomenda ainda, o contínuo estudo para promover entendimentos comuns sobre como essas normas se aplicam ao comportamento estatal e ao uso das TICs, dado o caráter único dessas tecnologias, o relatório destaca também que normas adicionais poderiam ser desenvolvidas ao longo do tempo (Nações Unidas, 2013, p. 2). E nesse sentido, o relatório recomenda a realização de diálogo institucional regular sobre essas questões sob os auspícios das Nações Unidas.

Já o relatório de 2015, considerado o como o mais significativo nessa temática (Henriksen, 2018; Paulus, 2024), reafirmou e ampliou esse consenso, identificando conceitos-chave do Direito Internacional aplicáveis ao ciberespaço, como o princípio da soberania estatal, resolução pacífica de controvérsias e o princípio da não intervenção (Nações Unidas, 2015a). O documento também incluiu onze normas voluntárias, não vinculantes (Fig 1), para orientar o comportamento responsável dos estados no ciberespaço visando promover um ambiente de TIC aberto, seguro, estável, acessível e pacífico (Nações Unidas, 2015a), dentre as quais destacam-se: evitar atividades que danifiquem infraestruturas críticas; proteger equipes de resposta a emergências cibernéticas e responder a pedidos de assistência de estados afetados por ataques.

As 11 normas refletem as expectativas da comunidade internacional sobre o comportamento responsável dos Estados e organizações regionais, conforme uma opinião coletiva em constante evolução, influenciada pelo aprofundamento da compreensão sobre segurança cibernética e pela contribuição de novos governos ao processo (Hoogeveen, 2022). Conforme destacado no relatório de 2015 (Nações Unidas, 2015a), essas normas visam "reduzir riscos à paz e segurança internacionais e prevenir conflitos, especialmente em ações entre Estados que possam gerar maiores ameaças". Embora sejam normas de *soft law*[20] e

[20] *Soft law* surge quando normas jurídicas apresentam um grau reduzido de obrigação, precisão ou delegação, podendo variar em intensidade e combinação. Muitos atores internacionais optam deliberadamente por essa forma mais flexível de legalização, seja como etapa preliminar para normas mais rígidas, seja por suas próprias

portanto não impõem obrigações legais vinculantes ou limitam a soberania estatal, as normas fornecem uma base comum para que os Estados desenvolvam capacidades, definam direções estratégicas e atuem de maneira responsável.

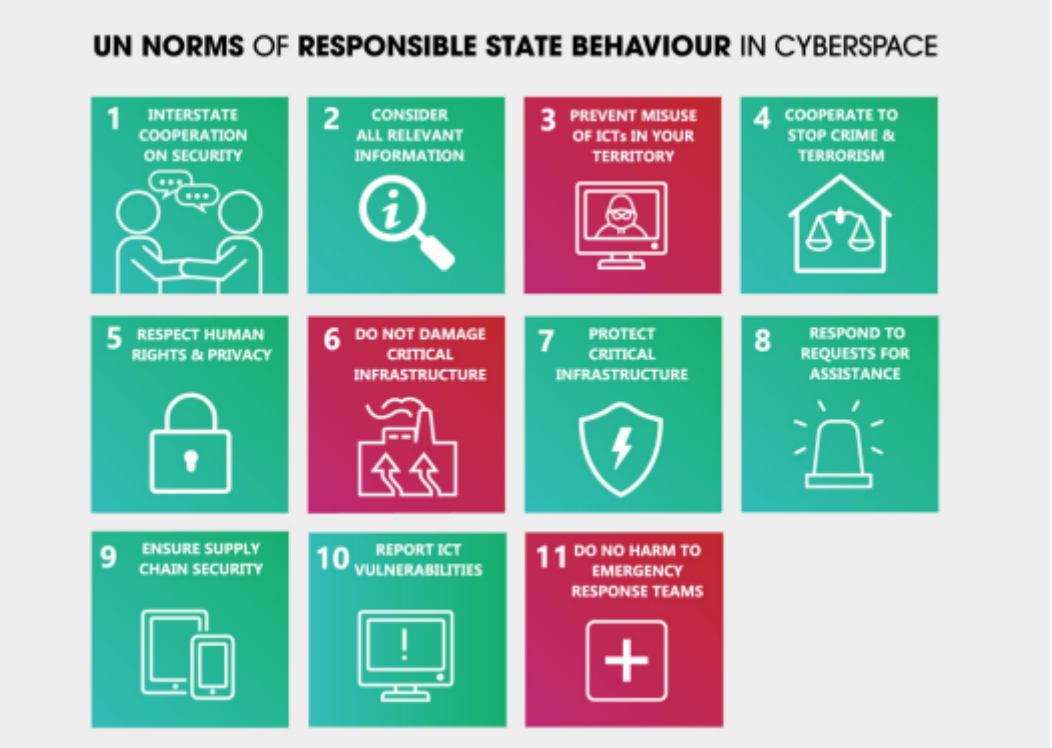

Fig. 1. As onze normas de comportamento responsável dos Estados no ciberespaço do relatório consensual de 2015. Fonte: Hoogeveen, 2022.

Apesar dos significativos avanços dos GGEs anteriores, o GGE de 2017 enfrentou retrocessos pertinentes, não conseguindo produzir um relatório consensual, chegando a ser considerado, na época, "*the end of the road for the UN cyber norms*" (Henriksen, 2018). Um dos fatores apontados para o impasse teria sido o cenário geopolítico instável de 2016-2017, com as supostas intervenções russa nas eleições americanas, intensificaram as divergências entre grandes potências que já polarizavam o debate no GGE desde os primórdios (Brotherhood, 2024; Paulus, 2024; Tiirmaa-Klaar, 2021).

Ademais, o debate agora não era mais sobre se o Direito Internacional é aplicável mas, como ele deveria ser aplicável; desse modo, questões como a inclusão do Direito Internacional Humanitário (DIH), a legitimidade do uso da autodefesa e o direito de os Estados adotarem contramedidas também emergiram como pontos de fricção e polarização,

vantagens. O *soft law* oferece benefícios do *hard law* com menor custo e maior adaptabilidade, tornando-se uma alternativa viável quando a legalização rígida é difícil de alcançar. Ele se posiciona entre o *hard law* e arranjos puramente políticos, nos quais a legalização é mínima ou inexistente (Abbott e Snidal, 2000).

alguns países se opuseram por argumentar que isso poderia "militarizar" o espaço cibernético (Tiirmaa-Klaar, 2021; brotherhood, 2024). Havia ainda, divergências de pontos de vista acerca do princípio de *due diligence* mesmo entre os estados "*like-minded",* dificultando ainda mais os avanços consensuais entre os membros, essas diferenças provavelmente estavam enraizadas na disputa geopolítica mais amplas e consequentemente migraram para o debate sobre normas cibernéticas (Kattemann e Paulus, 2020).

Contudo, após os fracassos de 2017, o novo GGE (2019-2021), criado a partir da resolução A/RES/73/266 (Nações Unidas, 2018b), patrocinado pelos Estados Unidos, logrou relatório consensual, e avanços nos entendimentos da aplicabilidade do Direito Internacional ao ciberespaço. A primeira sessão ocorreu em dezembro de 2019, sob a presidência do Brasil. Nesse mesmo período, contudo, foi estabelecido um Grupo de Trabalho Aberto (OEWG), por proposta russa frente ao descontentamento com os entraves do último GGE, tendo por objetivo dar continuidade nos avanços alcançados pelos GGEs adotando um fórum mais inclusivo, transparente e democrático (Schmitt, 2021). Esse desenvolvimento, contudo, resultou em uma bifurcação nos trabalhos com Rússia e China que concentraram-se no OEWG, enquanto os Estados Unidos, Reino Unido e seus aliados no GGE (Schmitt, 2021).

Esse contexto polarizado e de intensas tensões geopolíticas, destacou ainda mais a relevância da obtenção de consenso pelo grupo (Schmitt, 2021). Tiirmaa-Klaar (2021) atribui esse feito notável à uma combinação de fatores: o comprometimento e a habilidade diplomática neutra dos presidentes brasileiro (GGE) e suíço (OEWG), a dinâmica regional, os esforços eficazes de mediação e retorno dos debates, além da crescente profissionalização dos membros do GGE, que juntos contribuíram significativamente para os resultados positivos alcançados.

Além disso, outra importante consideração do relatório de 2021 foi o Compêndio oficial de contribuições nacionais voluntárias sobre o assunto de como o Direito Internacional se aplica ao uso de TIC[21]. Essas visões contribuem de maneira significativa para o desenvolvimento do *opinio juris*, esclarecendo como as normas consuetudinárias do Direito Internacional podem ser aplicadas no espaço cibernético, retomando conceitos apresentados nos relatórios de 2013 e 2015, e ampliando o panorama construído pelos GGEs (Nações Unidas, 2021c).

Essas posições moldam debates mais amplos, como a obrigação dos Estados de exercer devida diligência em seu território e a legalidade de contramedidas coletivas contra atos ilícitos (Schmitt, 2021). Até o momento, apenas a União Africana e 30 Estados,

[21] https://docs.un.org/en/A/76/136

majoritariamente do Norte Global, emitiram tais posicionamentos (SICW, 2024). O Brasil foi o primeiro país latino-americano a publicar sua posição nacional sobre a aplicabilidade do DI no ciberespaço, contida no compêndio (Nações Unidas, 2021c). No contexto latino-americano, além do Brasil, apenas Costa Rica e Cuba divulgaram suas posições, enquanto outros países consideram seguir o mesmo caminho, muitos enfrentam limitações técnicas e institucionais (SICW, 2024).

PARTE III - OEWG: UM NOVO FÓRUM PARA A CONSTRUÇÃO NORMATIVA DO ESPAÇO CIBERNÉTICO

Como mencionado na seção anterior, diante dos impasses e divergências no Grupo de Especialistas Governamentais (GGE) de 2017, a Assembleia Geral das Nações Unidas (AGNU) aprovou a proposta de resolução apresentada pela Rússia para a criação de um Grupo Aberto de Trabalho (Open-ended Working Group – OEWG). Com a mesma temática dos GGEs, o OEWG surgiu como um novo fórum, mais inclusivo e democrático, com o objetivo de impulsionar o avanço na construção normativa do ciberespaço e na segurança das Tecnologias da Informação e Comunicação (TICs). A seguir, serão abordados a criação, o formato, as principais discussões e resultados deste fórum.

3.1 Grupo de Trabalho Aberto (OEWG) sobre a segurança e uso de Tecnologias de Informação e Comunicação (TICs) - Criação e formato

A Assembleia Geral adotou resolução que estabeleceu, em dezembro de 2018, o Grupo Aberto de Trabalho (Open-ended Working Group – OEWG) sobre a segurança e uso das TICs, a partir da proposta de resolução russa (Nações Unidas, 2018a), a qual foi motivada a partir dos entraves de consensos e interesses do último GGE (2017). Ao contrário dos GGEs, que são compostos por especialistas nomeados, o OEWG é aberto a todos os Estados-membros da ONU que desejam participar, de forma a fomentar a transparência, a inclusividade e a democracia. Esse novo espaço de discussão deveria proporcionar uma oportunidade para os Estados deixados de fora do GGE se envolverem na construção normativa para o espaço cibernético (Ruhl et al, 2020).

O OEWG também possui o diferencial de discutir e formular recomendações sobre a segurança cibernética com consultas intersetoriais que incluem a participação de representantes da sociedade civil, da indústria e do meio acadêmico, ampliando o diálogo para além dos atores governamentais. Estes participam como observadores nas sessões formais, e podem fazer declarações orais em sessões dedicadas e enviar contribuições por escrito. Os

Estados Membros são incentivados a usar o mecanismo de "não objeção" à participação desses observadores de maneira prudente, buscando promover a inclusão da sociedade e stakeholders na construção de tais entendimentos comuns (UNODA, 2025).

Como abordado na seção anterior, os GGEs estabeleceram um panorama normativo, também denominado *acquis* (Nações Unidas, 2018a). O OEWG reconhece esse conjunto de regras, normas e princípios internacionais de comportamento responsável dos Estados, conforme enunciado nos relatórios dos GGEs de 2013, 2015 - e posteriormente de 2021-, que foram adotados por consenso (Nações Unidas, 2016) pelas Nações Unidas:

> Welcomes the following set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2013 and 2015 adopted by consensus and recommended in resolution 71/28 entitled “Developments in the field of information and telecommunications in the context of international security”, adopted by the General Assembly on 5 December 2016 (Nações Unidas, 2018a, Pr. 1).

No entanto, a necessidade de aprofundar o entendimento dos Estados sobre as dinâmicas dessas tecnologias emergentes continuava a crescer. E nesse contexto, o OEWG tem como mandato continuar a desenvolver regras, normas e princípios de comportamento responsável dos Estados e deve apresentar relatórios anuais de progresso e um relatório final sobre os novos entendimentos, a serem adotados por consenso, na AGNU:

> to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States [...], and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts referred [...] (Nações Unidas, 2018a).

Dessa forma, o OEWG busca não apenas consolidar as normas já estabelecidas, mas também explorar mecanismos para sua implementação, adaptar-se às transformações tecnológicas e fomentar um diálogo institucional contínuo e inclusivo no âmbito das Nações Unidas. Hoje, o OEWG está em seu segundo mandato (2021-2025), e segue ainda com semelhantes tópicos de discussão proposto no primeiro mandato (2019-2021) (Nações Unidas 2018a; 2020), podemos dispô-los da seguinte maneira:

a. **Regras, normas e princípios** de comportamento responsável dos Estados e os meios para sua implementação, introduzindo mudanças quando necessário ou

elaborando normas adicionais de conduta. Também deve considerar iniciativas dos Estados para assegurar a segurança no uso das TICs.

b. O estabelecimento de **Diálogo Institucional Regular** sob a ONU com ampla participação dos Estados, que deverá estudar **ameaças existentes e potenciais** na esfera de segurança da informação, incluindo segurança de dados, e possíveis medidas de cooperação para prevenir tais ameaças.
c. A aplicabilidade do **Direito Internacional** ao uso das TICs pelos Estados, bem como **medidas de fortalecimento de confiança** e **desenvolvimento de capacidades**.

3.1.2 Discussões e desafios

O primeiro OEWG iniciou suas atividades em 2019 e, em 2021, aprovou um relatório consensual com recomendações para mitigar ameaças cibernéticas e incentivar normas de conduta responsável dos Estados (Nações Unidas, 2021b). Sob a presidência do embaixador suíço Jürg Lauber, cerca de 100 países participaram das discussões, com um clima inicial de otimismo (Ruhl et al., 2020). O processo também contou com a participação de organizações não governamentais como observadoras e contribuintes para os debates (Nações Unidas, 2021b).

Inicialmente, a criação do OEWG gerou desconfiança entre democracias liberais, que temiam que o grupo se tornasse um campo de batalha entre visões democráticas e autocráticas sobre o futuro do ciberespaço (Ruhl et al, 2020; Tiirmaa-Klaar, 2021). Essa tensão foi aliviada com a escolha de presidentes experientes e historicamente neutros, restaurando a confiança na imparcialidade do processo (Tiirmaa-Klaar, 2021).

Contudo, divergências importantes acompanharam esse novo fórum. Paulus (2024) destaca que um dos principais pontos de discordância foi a divisão entre os defensores do GGE e do OEWG. A disputa não se limitava somente ao conteúdo das discussões, mas também à forma como deveriam ocorrer. Em vez de escolherem um processo em detrimento do outro, a Assembleia Geral da ONU aprovou, por meio de resoluções separadas (Nações Unidas, 2018a; 2018b), tanto a criação do OEWG quanto a renovação do GGE, a tabela 2, logo abaixo, sintetiza as características específicas de cada.

Isso gerou preocupações sobre a condução simultânea desses grupos, que poderia dificultar o avanço das negociações e gerar resistência ao progresso dos trabalhos (Ruhl et al., 2020). A principal preocupação passou a ser como garantir a complementaridade entre os processos e viabilizar o sucesso de ambos (Lauber; Eberli, 2021, Tiirmaa-Klaar, 2021). Esta

bifurcação trouxe preocupações sobre capacidades financeiras e humanas que alguns países, particularmente no Sul Global, deveriam se esforçar para mobilizar, a fim de garantir sua participação em ambos fóruns (Kattemann; Paulus, 2020), como foi o caso do Brasil.

Outro ponto de divergência foi a aplicação do Direito Internacional ao ciberespaço, tema debatido desde antes de 2015. Embora os Estados concordem que o Direito Internacional é essencial para a paz, segurança e estabilidade das TICs, ainda permanecem incertezas sobre como suas regras e princípios devem ser interpretados e aplicados nesse contexto, como a questão da aplicabilidade do Direito Internacional Humanitário (Hurel, 2022). A terceira questão crítica envolveu o desenvolvimento de novas normas para o ciberespaço após o relatório de consenso do GGE de 2015. O desafio era decidir entre a formulação de novas normas ou o aprofundamento da compreensão das já existentes (Paulus, 2024). Houve também tentativas de expandir o mandato do OEWG para tratar de questões como desinformação e campanhas de propaganda (Ruhl et al., 2020). No entanto, os países ocidentais consideraram essa abordagem um risco à liberdade de expressão e resistiram à inclusão desses temas nas discussões do OEWG naquele momento (Lauber; Eberli, 2021).

Tabela 2 - Os processos paralelos (GGE e OEWG)

Categoria	**GGE (Grupo de Especialistas Governamentais) (2019-2021)**	**OEWG (Grupo de Trabalho Aberto) (2019-2021)**
Base Legal	UNGA A/RES/73/266	UNGA A/RES/73/27
Participação	25 Estados-Membros selecionados.	Todos os Estados-Membros interessados.
Principais objetos de discussão	Normas, regras e princípios; CBMs e Construção de Capacidades; Aplicabilidade do Direito Internacional ao ciberespaço.	Normas, regras e princípios; CBMs e Construção de capacidades; Aplicabilidade do Direito Internacional ao ciberespaço; Ameaças cibernéticas; Diálogo Institucional contínuo na ONU.
Relatório Final	Sessão 76 da AGNU (A/76/135, 2021), incluindo anexos com contribuições nacionais, baseada em consenso.	Sessão 76 da AGNU (A/75/816, 2021), baseada em consenso.

Fonte: **Relatórios das Nações Unidas (2018a; 2018b; 2021a; 2021b). Elaborado pela autora.**

A principal missão do presidente do OEWG foi suavizar as divergências acumuladas desde 2015 e apresentar um documento consensual que agregasse valor ao maior número

possível de Estados (Lauber; Eberli, 2021). Diferentemente dos GGEs, que tinham no máximo 25 participantes, o OEWG permitiu a participação de todos os 193 Estados-Membros da ONU, ampliando sua representatividade e permitindo maior inclusão de países em desenvolvimento no debate sobre normas cibernéticas (ibidem, 2021). Essa diversidade tornou o consenso mais desafiador, mas também trouxe novas dinâmicas, como a inclusão de um capítulo detalhado sobre desenvolvimento de capacidades em cibersegurança, um tema pouco abordado nos GGEs anteriores (ibidem, 2021).

As atividades simultâneas do primeiro OEWG e do sexto GGE não provaram ser um fator de impedimento, como algumas delegações temiam no início. A composição muito diferente dos grupos provocou abordagens e métodos de trabalho igualmente diferentes (Kattemann; Paulus, 2020). Apesar das dificuldades, tanto o GGE de 2019 quanto o OEWG de 2019 obtiveram bons resultados, culminando na publicação de relatórios consensuais e na participação ativa de diversos países (Lauber; Eberli, 2021). Dentre alguns fatores, a conjuntura global, com a instauração da pandemia global da COVID-19 e o aumento dos ataques cibernéticos a instituições de saúde e pesquisa reforçou a urgência do tema, mobilizando delegações a avançar no debate (Lauber; Eberli, 2021).

O Relatório Substantivo de 2021 consolidou os temas consensuais entre as delegações, reafirmando o *acquis,* panorama de normas estabelecidas pelo GGEs passados (Nações Unidas, 2021b). Ao contrário dos relatórios do GGE, que eram negociados apenas entre seus membros e posteriormente adotados pela Assembleia Geral da ONU, o OEWG ampliou significativamente a representatividade, permitindo que todos os Estados interessados participassem do processo, garantindo maior transparência e legitimidade ao documento (Lauber; Eberli, 2021).

Este relatório enfatiza, também, a importância da proteção das infraestruturas críticas e da integridade da internet, além de tratar a capacitação em segurança cibernética como um processo colaborativo, oferecendo princípios orientadores (Nações Unidas, 2021b). Apresenta recomendações para o fortalecimento das medidas de construção de confiança (*Confidence-Building Measures* – CBMs), como a criação de Pontos de Contato (*Points of Contact* – PoC[22]) (Nações Unidas, 2021b). Destaca ainda a necessidade de reduzir a exclusão digital, incluindo a de gênero, e reconhece o papel fundamental das partes interessadas não governamentais (Nações Unidas, 2021b). Além disso, aborda a proposta do Programa de

[22] Um Ponto de Contato (PoC) é uma medida de fortalecimento da confiança (CBM) adotada pelos Estados para facilitar a cooperação em segurança cibernética. Ele serve como um canal oficial de comunicação para intercâmbios diplomáticos, políticos, jurídicos e técnicos, além de ser essencial para relatar e responder a incidentes cibernéticos, especialmente em tempos de crise (Nações Unidas, 2021b).

Ação (*Programme of Action* – PoA), apresentada por França e Egito com o apoio de mais de 50 países (Nações Unidas, 2022). Essa iniciativa propõe um mecanismo permanente, inclusivo e orientado para discutir ameaças cibernéticas, apoiar as capacidades dos Estados e promover compromissos baseados no *acquis* já estabelecido (Kattemann; Paulus, 2020). Por fim, o relatório reúne um compêndio de ideias e propostas para futuras deliberações sobre o tema (Schmitt, 2021; Nações Unidas, 2021b).

Em 2020 – antes que houvesse uma oportunidade de propor formalmente o estabelecimento de tal mecanismo – o Primeiro Comitê aprovou um projeto de resolução, patrocinado pela Rússia, para estabelecer um novo grupo de trabalho aberto para o período de 2021-2025 (Nações Unidas, 2020) (Kattemann; Paulus, 2020), com foco nos desafios emergentes, capacitação dos Estados e aplicação do Direito Internacional ao uso das TICs. Este novo OEWG, de mandato parecido com o antecessor, também convidou os Estados-membros a apresentar eventuais comentários e sugestões acerca de quais deveriam ser as características (escopo, estrutura e conteúdo) do PoA e o futuro de seu estabelecimento (Nações Unidas, 2021b).

O primeiro Relatório Anual de Progresso (2021-2025), contudo, refletiu poucos avanços substanciais, funcionando mais como um reconhecimento do interesse dos Estados em manter o diálogo do que como um avanço concreto (Hurel, 2022). Questões jurídicas essenciais, como *due diligence*, Direito Internacional Humanitário e responsabilidade estatal, continuam sem consenso, assim como a regulamentação de ameaças cibernéticas emergentes (Hurel, 2022; DIGITAL WATCH OBSERVATORY, 2025).

Segundo Hurel (2022), para que o OEWG tenha um impacto prático nos próximos anos, os Estados-membros devem priorizar a implementação das normas já existentes, em vez de criar novas, reduzindo a desconfiança por meio de diretrizes concretas. Focar na implementação tornaria o OEWG mais eficaz, facilitando a troca de experiências entre países e permitindo que a ONU apoie esse processo, bem como a inclusão de atores não governamentais, que já trabalham na criação de estruturas para implementação, fortaleceria essa discussão (Hurel, 2022). Apesar das dificuldades na criação do OEWG, as tensões entre os Estados-membros persistem, especialmente diante das crises políticas entre o Ocidente, Rússia e China, que inevitavelmente influenciam as negociações.

PARTE IV - CONTRIBUIÇÕES BRASILEIRAS NA CONSTRUÇÃO NORMATIVA PARA O ESPAÇO CIBERNÉTICO

Esta seção abordará o papel e a relevância da atuação brasileira na construção normativa do ciberespaço sob os auspícios das Nações Unidas, considerando os dois principais fóruns temáticos: Grupo de Especialistas Governamentais (GGE) e o Grupo Aberto de Trabalho (Open-ended Working Group – OEWG). Destaco que por conta da escassez de material sobre o papel e participação brasileira nesses fóruns, as principais referências utilizadas nesta seção foram o livro "*Building bridges in Cyber Diplomacy*" de Alexandra Paulus (2024), que oferece uma análise detalhada e abrangente da contribuição do Brasil na construção normativa para o espaço cibernético; os relatórios substanciais e processuais desses fóruns (Nações Unidas,) e discursos orais proferidos pela delegação brasileira no OEWG (Nações Unidas, .

4.1 Contextualização

Primeiramente, é fundamental destacar que a participação do Brasil no processo de formulação das *cyber norms* no cenário global "does not emerge in a vacuum" (Paulus, 2024, p. 99). Pelo contrário, ela se insere no contexto das tradições da Política Externa Brasileira (PEB) e das percepções nacionais sobre riscos e ameaças cibernéticas, bem como da política de segurança cibernética (ibidem, 2024).

Saraiva (2014), ao analisar o princípio da histórica autonomia da PEB, afirma que "há um padrão histórico que insiste na seta do tempo da inserção internacional do Brasil. A seta não é linear, move-se em oscilações ora tendente a mais autonomia, ora a menos, mas é garantida no tempo, no meio [...]". Assim, a trajetória brasileira reflete uma continuidade da política externa desde o início do século XIX até os dias atuais. De acordo com Paulus, no campo da cibersegurança, essa dinâmica de alinhamento e preservação dos princípios históricos da PEB também se mantém: a diplomacia brasileira tem sido relativamente estável e guiada por quatro eixos de interesses principais: a aspiração à liderança global; o compromisso com a manutenção e reforma da ordem internacional; a ênfase no direito e normas internacionais; e a busca pela *construção de pontes* no cenário internacional (2024, p. 100).

A construção normativa nacional também tem sido influenciada pelas dinâmicas multilaterais internacionais, mas busca manter-se coerente com seus valores e tradições históricos, como o respeito à soberania, o multilateralismo, e o pacifismo. É o que podemos

ver na Estratégia Nacional de Cibersegurança do Brasil, publicada em 2020, que destaca em sua seção sobre a dimensão internacional que o país deve:

> "continuar a se orientar pelos princípios constitucionais brasileiros, pelos valores fundamentais de nossa sociedade – como o respeito à democracia e aos direitos humanos –, pela ênfase ao multilateralismo, pelo respeito ao direito internacional, pela vocação para o diálogo e pela solução pacífica de controvérsias, passando pela identificação de novas oportunidades comerciais" (Brasil, 2020a).

A diplomacia brasileira tem sido marcada por um desejo de transformação estrutural global, com forte defesa da inclusão e de uma ordem internacional mais democrática (Corrêa, 1999). Everton Lucero (2011) ressalta uma característica essencial do engajamento do Brasil na política externa: "Não aderimos facilmente a convenções das quais não participamos do processo de negociação." Esse posicionamento evidencia a importância do envolvimento ativo do Brasil na formulação de normas internacionais, garantindo que suas perspectivas sejam consideradas.

Além disso, considerando que países, principalmente aqueles que não detém relevante *hard power*[23], utilizam a institucionalização de leis e normas internacionais como uma forma de *soft power*, buscando promover seus interesses nacionais (Tikk Ringas, 2016), pode-se observar que esta é a estratégia adotada pelo Brasil na agenda das normas cibernéticas. Episódios e mudanças no cenário doméstico, bem como interferências externas — como as revelações de Edward Snowden[24] —, o contexto de megaeventos em 2014[25] (Hurel, 2019), e a própria tradição da PEB também são fatores relevantes para compreender o posicionamento brasileiro para a governança da segurança cibernética e os interesses que guiam sua participação na construção normativa global.

O Brasil possui um histórico consolidado de atuação como mediador e conciliador nas Nações Unidas, evidenciando seu compromisso com a paz e a solução pacífica de conflitos no cenário internacional (Senado Federal, 2022). Reconhecido por sua capacidade de dialogar com polos divergentes e por sua defesa dos interesses dos países em desenvolvimento

[23] Refere-se à capacidade de um Estado influenciar o comportamento de outros por meio de coerção, uso da força militar ou incentivos econômicos. Esse conceito contrasta com o *soft power*, que se baseia em persuasão e influência cultural (Nye, 2011).

[24] Edward Snowden é um ex-analista de sistemas da Agência de Segurança Nacional dos Estados Unidos (NSA) que, em 2013, revelou a existência de um amplo programa de vigilância global conduzido pelo governo norte-americano. As informações vazadas por Snowden mostraram que a NSA coletava dados de comunicações em larga escala, incluindo espionagem sobre cidadãos, governos estrangeiros e líderes mundiais, gerando debates sobre privacidade, segurança cibernética e governança da internet. A então presidente do Brasil, Dilma Rousseff, e outros funcionários do governo brasileiro, teriam sido alvo dessa espionagem (Greenwald, 2014).

[25] Durante a Copa do Mundo de 2014, o Brasil enfrentou desafios significativos em segurança cibernética, devido ao aumento de ameaças digitais associadas ao evento. Para mitigar esses riscos, o Ministério da Defesa, por meio do Centro de Defesa Cibernética (CDCiber), coordenou ações preventivas e reativas, incluindo o monitoramento de redes e a proteção de infraestruturas críticas. Essas medidas foram essenciais para assegurar a integridade dos sistemas nacionais e a segurança dos participantes e espectadores do torneio (Abdalla et al, 2016).

(Paulus, 2024), essa característica ficou evidente em sua atuação nos principais fóruns multilaterais. Um reflexo desse papel é a escolha do Brasil para presidir dois Grupos de Peritos Governamentais (GGEs), em 2015 e 2019, ambos bem-sucedidos na produção de relatórios substantivos, reafirmando a credibilidade e influência diplomática brasileira nesses espaços.

4.2. Atuação e relevância brasileira nos GEEs

O conceito de *norm-bridge-building* (construção de pontes normativas), proposto por Paulus (2024, p. 178), aplica-se a contextos de conflitos normativos, como disputas entre uma nova proposta de norma e o status quo ou entre alternativas divergentes para mudanças normativas. A construção de pontes normativas envolve dois elementos principais: primeiro, a promoção de compromissos entre lados opostos, utilizando técnicas como facilitação do diálogo e exploração de soluções alternativas; e segundo, o engajamento de atores anteriormente passivos no debate, ampliando as chances de um acordo global ao abordar suas preocupações. Se bem-sucedido, o processo culmina em uma proposta de norma de compromisso. Em suma, trata-se de criar consensos entre partes divergentes e engajar atores passivos na promoção conjunta de normas globais (Paulus, 2024, p. 178).

Considerando esse conceito, o Brasil demonstrou certo protagonismo nas sessões do GGE que resultaram em relatórios consensuais (2013, 2015 e 2019). Embora as reuniões do GGE ocorram a portas fechadas, dificultando uma análise detalhada dos atores e do papel brasileiro na formulação de normas cibernéticas, há indícios claros de uma estratégia de *construção de pontes normativas* (Paulus, 2024, p. 204). O Brasil demonstrou elevado engajamento durante os GGEs, atuando como co-patrocinador de diversas resoluções desde a introdução do tema na ONU (Paulus, 2024). Entre os participantes, apenas os cinco membros permanentes do Conselho de Segurança estavam presentes em todos os seis GGEs. Além deles, apenas três outros países participaram de cinco edições: Estônia, Índia e Brasil.

As motivações que orientam o engajamento brasileiro nessa temática derivam tanto de seus interesses históricos em exercer uma liderança global e influenciar a ordem internacional quanto de suas aspirações, como a reforma do Conselho de Segurança das Nações Unidas, na qual reivindica um assento há décadas (Paulus, 2024). No entanto, o Brasil não dispõe das tradicionais capacidades de poder, ou *hard power*, para alcançar plenamente suas ambições. Diante disso, recorre ao *soft power* como estratégia para projetar seus interesses no sistema internacional, especialmente no âmbito das Nações Unidas. No contexto da construção normativa, em particular, esses fóruns funcionam como plataformas estratégicas para os

países promoverem seus interesses nacionais no desenvolvimento e uso das TICs (Tikk Ringas, 2016).

Em 2013, as revelações de Edward Snowden sobre o programa de vigilância da NSA (National Security Agency) americana marcaram um ponto de inflexão na segurança cibernética global, especialmente para o Brasil (Hurel, 2019). Esse episódio evidenciou a vulnerabilidade das comunicações e o uso indiscriminado da tecnologia para espionagem, violando a soberania dos Estados e o Direito Internacional. A partir desse momento, o Brasil, que até então atuava de forma mais passiva nos GEEs, passou a priorizar essa agenda, delegando sua condução ao Ministério das Relações Exteriores, que passou a contar com representação diplomática especializada na temática (Paulus, 2024).

Paralelamente, com a realização de megaeventos no Brasil, o país adotou uma postura proativa na criação de normas contra a ciberespionagem, destacando-se a conferência NETmundial[26] e a coautoria da resolução A/HRC/27/37, intitulada "*The right to privacy in the digital age*" (Hurel, 2019; Paulus, 2024) promovendo o debate sobre direitos humanos fundamentais, incluindo a privacidade no contexto das TICs (Nações Unidas, 2014). O relatório substantivo do GGE de 2013 refletiu essas preocupações, e o de 2015 mencionou explicitamente a resolução brasileira sobre espionagem (Nações Unidas, 2013; 2015a). Esses episódios impulsionaram mudanças nas políticas domésticas e ficaram conhecidos como o "cyber wake-up call" do Brasil (Paulus, 2024, p. 123).

Posteriormente, o Brasil foi escolhido para presidir o GGE de 2015 devido à sua histórica posição neutra entre os dois principais blocos de poder (Tiirmaa-Klaar, 2021). Esse papel tornou-se ainda mais relevante no contexto geopolítico desafiador da época, com a recente anexação da Crimeia pela Rússia e o consequente agravamento das tensões globais. A obtenção de um relatório substancial representou um sucesso diplomático significativo (Tiirmaa-Klaar, 2021; Paulus, 2024).

Mesmo após o enfraquecimento do GGE em 2017 e a fragmentação dos esforços de construção normativa global com a expansão da agenda para a criação de normas cibernéticas fora da ONU, o Brasil continuou a defender que as Nações Unidas eram o locus adequado, democrático e legítimo para a formulação de normas cibernéticas (Paulus, 2024). Esse

[26] A NETmundial foi um encontro global multissetorial sobre governança da Internet realizado em São Paulo, Brasil, nos dias 23 e 24 de abril de 2014. Organizado pelo Comitê Gestor da Internet no Brasil (CGI.br) e pelo Governo Brasileiro, o evento reuniu representantes de governos, setor privado, sociedade civil, comunidade técnica e acadêmica para debater princípios e diretrizes para a governança da Internet. A conferência resultou na *NETmundial Multistakeholder Statement*, um documento que enfatizou a importância da governança multissetorial, a proteção dos direitos humanos no ambiente digital e a necessidade de colaboração internacional para um ecossistema de Internet aberto, inclusivo e seguro (NETMUNDIAL, 2014).

posicionamento está alinhado às diretrizes históricas do Itamaraty, que prioriza a ONU em detrimento de estruturas menos inclusivas, como organizações regionais ou acordos internacionais (Paulus, 2024). Apesar de apoiar o status quo, o Brasil defende a reforma do sistema internacional para torná-lo mais inclusivo e igualitário (Ramalho, 2015 apud Paulus, 2024).

Nas sessões de consultas informais para a resolução do próximo GGE, o Brasil advogou por um formato mais inclusivo, visando tornar o debate mais equitativo e democrático. Essa discussão levou à ampliação do número de especialistas de 15 para 20, embora o grau de influência brasileira nessa decisão não seja totalmente claro (Paulus, 2024, pg 201). Essa postura reflete o compromisso do país em envolver mais atores passivos no debate e facilitar sua participação.

No que tange à aplicabilidade do Direito Internacional existente, o Brasil adotou uma posição mediadora entre os pólos divergentes: reconheceu que o Direito Internacional Humanitário era, em princípio, aplicável, mas também expressou preocupação com a militarização do espaço cibernético (Paulus, 2024). Esse posicionamento está em consonância com a tradição diplomática brasileira de apoio ao Direito Internacional e suas normas. O Brasil também ressaltou a vulnerabilidade das infraestruturas críticas, especialmente em situações de escalada de conflitos (Delbrasonu, 2014 apud Paulus, 2024), enfatizando a necessidade de fortalecimento de capacidades nos países em desenvolvimento.

Contudo, os esforços brasileiros na construção de pontes normativas enfrentaram desafios. Apesar de avanços no reconhecimento da aplicabilidade do Direito Internacional, o relatório do GGE não alcançou consenso sobre a aplicação do Direito Internacional Humanitário (DIH) às TICs. Além disso, temas cruciais para países em desenvolvimento, como acesso a tecnologias, não foram incorporados na seção de normas (Paulus, 2024, p. 204). Esse tema, no entanto, foi mais explorado no OEWG, conforme abordaremos a seguir.

4.3 Atuação e relevância brasileira no OEWG

A aplicação do conceito de *norm bridge-building* (Paulus, 2024) à atuação do Brasil no OEWG revela padrões semelhantes aos observados no GGE. Como presidente do GGE durante a bifurcação dos trabalhos com a criação do OEWG, o Brasil exerceu um papel estratégico de mediação entre os dois fóruns, buscando garantir a continuidade e a integridade dos processos. O país atuou ativamente para facilitar o diálogo e promover a participação engajada dos envolvidos também no OEWG (Paulus, 2024). O Itamaraty concentrou grande

parte de seus esforços nessa função, utilizando sua posição de liderança para articular os processos e assegurar a efetividade de seus relatórios (ibidem, 2024).

Diante do surgimento de inúmeras propostas sobre as cyber norms fora do âmbito das Nações Unidas, o Brasil reforçou a importância dos fóruns já estabelecidos e defendeu a centralização dos debates nesses espaços institucionais (Paulus, 2024). Esse posicionamento visava evitar a fragmentação das discussões e a duplicação de esforços, fortalecendo a governança global da cibersegurança dentro de um quadro multilateral legítimo. Em discursos proferidos durante as sessões substantivas do OEWG II (2021-2025), a delegação brasileira reiterou essa visão ao afirmar:

> "[...] any efforts aimed at eventually developing new norms must be inclusive and therefore take place within the UN, which currently means this OEWG. While we recognize the value of many international initiatives mentioned throughout this and previous sessions in fostering discussions on key cybersecurity issues and participate in many of them, norms will only have effectiveness and legitimacy when negotiated in an open and inclusive manner in a universal forum, where the needs of all countries – including developing countries – are duly taken into account." (Brasil, 2024b)

Nesse sentido, o Brasil manteve seu compromisso ativo com o engajamento de atores tradicionalmente menos participativos, especialmente os países em desenvolvimento (Paulus, 2024).

No que se refere ao estabelecimento de um diálogo institucional regular e, eventualmente, à criação do PoA, a delegação brasileira apoiou consistentemente o mecanismo, desde que fossem consideradas questões fundamentais, como a promoção da cooperação, o fortalecimento de capacidades e a preservação da integridade do "acquis" já consolidado (Brasil, 2024b). Além disso, em consonância com sua prioridade de fortalecer instituições pacíficas e multilaterais, o Brasil defendeu abordagens que incentivam a cooperação, a unidade e a imparcialidade, expressando preocupação com ações que possam comprometer o multilateralismo e a construção de confiança (Nações Unidas, 2021c; Brasil, 2024e).

O OEWG enfrentou desafios consideráveis em sua criação, e as tensões entre os Estados-membros persistiram ao longo dos últimos anos (Hurel, 2022). No entanto, concentrar-se no desenvolvimento de diretrizes para a implementação de normas poderia tornar o grupo mais eficaz, mesmo diante das divergências sobre outros mecanismos. Esse enfoque permitiria uma troca mais concreta sobre como os países interpretam e monitoram essas normas internamente, além de explorar o papel das Nações Unidas no apoio à sua

implementação (Hurel, 2022). A seguir, apresento um resumo dos principais posicionamentos do Brasil sobre as questões substantivas propostas pelo OEWG, foi utilizado principalmente as postulações brasileira no Compêndio sobre posições nacionais sobre a aplicabilidade do Direito Internacional no espaço cibernético (Nações Unidas, 2021c) e discursos proferidos pela delegação diplomática do Brasil nas mais recentes sessões do OEWG (2021-2025) (Brasil, 2024).

4.3.1 Questões substanciais do OEWG e o posicionamento brasileiro

Regras, Normas e Princípios

O Brasil afirma que, no uso de Tecnologias da Informação e Comunicação (TICs), os Estados devem cumprir o Direito Internacional, incluindo a Carta das Nações Unidas, o Direito Internacional dos Direitos Humanos e o Direito Internacional Humanitário (DIH) (Nações Unidas, 2021c). O Brasil reconhece ainda que "o silêncio não é necessariamente significativo do ponto de vista jurídico e, portanto, não constitui evidência suficiente da prática estatal e/ou opinio juris para o surgimento de novas normas vinculantes sob o direito internacional consuetudinário" (Brasil, 2024c). Nesse sentido, apoia e incentiva os países, especialmente os em desenvolvimento, a apresentarem suas posições nacionais para a construção do Direito Consuetudinário (Brasil, 2024c).

Diante das divergências sobre a aplicação do Direito Internacional ao uso das TICs pelos Estados, o risco de comportamentos imprevisíveis, mal-entendidos e escalada de tensões aumentam. O Brasil afirmou defender que, se necessário, o desenvolvimento de normas adicionais deve ser considerado como um meio de preencher potenciais lacunas legais e resolver incertezas persistentes (Nações Unidas, 2021c). Ademais, refuta a falsa dicotomia entre a aplicabilidade do Direito Internacional existente ao espaço cibernético e a necessidade de um instrumento juridicamente vinculante específico, ressaltando que essas discussões não são, por natureza, excludentes (Brasil, 2024c).

Direito Internacional

No que tange à soberania, o Brasil declarou considerar este como um dos princípios fundadores do Direito Internacional (Nações Unidas, 2021c). Como afirmado pela Corte Internacional de Justiça no Caso do Canal de Corfu[27] “entre Estados independentes, o respeito

[27] No *caso do Canal de Corfu* (Reino Unido v. Albânia, 1949), a Corte Internacional de Justiça (CIJ) reafirmou o princípio fundamental da soberania estatal, destacando que "entre Estados independentes, o respeito pela

pela soberania territorial é uma base essencial para as relações internacionais" (Nações Unidas, 2021c). Assim, a soberania é aplicável como uma regra autônoma, inclusive ao uso de TICs pelos Estados, implicando uma obrigação independente de "cada Estado respeitar a soberania territorial de outros" (Nações Unidas, 2021c).

Atualmente, não há prática estatal ampla nem *opinio juris* suficiente para gerar uma nova norma internacional consuetudinária que permita a violação da soberania do Estado, inclusive por meio de TICs. As interceptações de telecomunicações, por exemplo, sejam ou não consideradas uma intervenção nos assuntos internos de outro Estado, seriam classificadas como atos internacionalmente ilícitos por violarem a soberania estatal (Brasil, 2024c). Da mesma forma, operações cibernéticas contra sistemas de informação localizados em território estrangeiro ou que causem efeitos extraterritoriais podem constituir violações da soberania (Nações Unidas, 2021c; Brasil, 2024c).

No que se refere ao Direito Internacional Humanitário (DIH), o País declarou considerar que sua aplicabilidade se estende a todas as situações equivalentes a conflitos armados, independentemente da classificação dada pelas partes envolvidas (Brasil, 2024c). O objetivo do DIH é minimizar o sofrimento humano e fornecer um nível mínimo de proteção aos civis em qualquer cenário de hostilidades (Brasil, 2024c). Dessa forma, o reconhecimento de sua aplicabilidade ao ciberespaço não deve ser interpretado como necessariamente um endosso à militarização do ambiente digital ou à legitimação da guerra cibernética (Nações Unidas, 2021c; Brasil, 2024c).

Construção de Capacidades (CB) e Medidas de Construção de Confiança (CBM)

Para o Brasil, "nenhum país pode estar a salvo de ameaças no domínio digital isoladamente – somos tão fortes quanto o nosso elo mais fraco" (Brasil, 2024d, tradução nossa)[28]. Assim, para o Brasil, a construção de capacidades no campo da segurança das TICs é essencial para que todos possam colher, de forma sustentável, os benefícios socioeconômicos da transformação digital (Brasil, 2024d). A exclusão digital torna a cooperação internacional uma necessidade urgente para expandir a capacidade dos Estados de mitigar riscos e responder a incidentes cibernéticos (Brasil, 2024d). Nesse contexto, o Brasil afirma que a

soberania territorial é uma base essencial para as relações internacionais". A decisão enfatizou que nenhum Estado tem o direito de intervir nos assuntos internos de outro, reforçando a obrigação de respeitar a integridade territorial dos países. Esse entendimento foi crucial para o desenvolvimento do Direito Internacional, consolidando a proibição de ações coercitivas unilaterais que violem a soberania de um Estado sem seu consentimento (CIJ, 1949).

[28] "No country can be safe from threats in the digital domain in isolation – we are only as strong as our weakest link" (Original).

capacitação foi corretamente reconhecida como um elemento transversal em todo o mandato do OEWG, constituindo, por si só, uma medida de construção de confiança (Brasil, 2024d).

Conforme estabelecido em seus princípios, a capacitação deve ser baseada nas necessidades, respeitosa à soberania dos Estados e implementada de forma colaborativa por todas as partes envolvidas. Não deve ser conduzida de forma impositiva, mas sim negociada para garantir benefícios mútuos a todas as partes (Brasil, 2024d). Dessa forma, a capacitação continuará a desempenhar um papel crucial para a construção de um ambiente digital aberto, seguro, estável, pacífico, acessível e interoperável (Brasil, 2024d).

O Brasil defende um diálogo regular, aberto e inclusivo sobre a segurança internacional no contexto das TICs (Brasil, 2021a). Para isso, considera essencial que um mecanismo institucional de diálogo integre aspectos fundamentais para um ambiente digital seguro, incluindo medidas de construção de confiança e capacitação, além de viabilizar debates aprofundados sobre temas em que ainda não há consenso entre os Estados (Brasil, 2024e). Esse diálogo deve se basear na preservação do arcabouço de entendimentos comuns (*acquis*) já estabelecido, abrangendo princípios, normas e regras de comportamento responsável dos Estados no ciberespaço, bem como a aplicação do Direito Internacional nesse domínio (Brasil, 2021a). O Brasil reafirma seu compromisso com o multilateralismo e sua determinação em buscar soluções para as ameaças à paz e à segurança internacionais decorrentes de atividades maliciosas no ciberespaço (Brasil, 2024e).

Novas Tecnologias e Novas Ameaças

No campo do desenvolvimento tecnológico, o Brasil reconhece o potencial disruptivo de tecnologias emergentes, como Inteligência Artificial (IA) e Tecnologia Quântica, bem como os benefícios que podem trazer à humanidade quando utilizadas para fins pacíficos (Brasil, 2024a). Contudo, também reconhece os riscos do uso dual dessas tecnologias, especialmente no contexto militar, com possíveis implicações para a paz e a segurança internacionais. O Brasil apoia a contínua investigação dos riscos e vulnerabilidades decorrentes das TICs, destacando a importância de recomendações concretas para mitigar ameaças e defendendo a inclusão desse tema na agenda do OEWG, a fim de garantir um debate multilateral e unificado (Brasil, 2024a).

4.4 Brasil e a ciber diplomacia: Uma política de Estado?

No que concerne à política externa brasileira, podemos sintetizar, conforme Paulus (2024), os principais pilares de interesse e objetivos do Brasil: a aspiração à liderança global;

o compromisso com a manutenção e reforma da ordem internacional; a ênfase no direito e nas normas internacionais; e a busca pela construção de pontes no cenário global. A Constituição Federal de 1988 (Brasil, 1988), em seu artigo 4º, apresenta os princípios que regem a política externa brasileira, os quais foram formulados considerando o histórico diplomático do país. Entre esses princípios, destacam-se: independência nacional; prevalência dos direitos humanos; igualdade entre os Estados; não intervenção; defesa da paz; solução pacífica de conflitos; e cooperação entre os povos para o progresso da humanidade.

Diante desse arcabouço normativo e principiológico, surgem as seguintes questões: houve mudanças expressivas na atuação do Brasil em fóruns internacionais, especificamente no GGE e OEWG, ao longo dos últimos governos? O Brasil manteve-se coerente com seus interesses e princípios?

Apesar do sigilo que envolve as reuniões dos GGEs, relatos disponíveis, como os de Tiirmaa-Klaar (2021), Lauber e Eberli (2021), evidenciam que o Brasil, representado por diplomatas como Carlos Perez e Guilherme Patriota — que presidiram os GGEs de 2015 e 2021, respectivamente —, teve sua postura mediadora amplamente reconhecida. O Brasil foi escolhido para presidir o GGE de 2015 devido à sua tradicional posição neutra entre os principais blocos de poder, um papel particularmente relevante no contexto geopolítico desafiador da época, marcado pela anexação da Crimeia pela Rússia e o consequente agravamento das tensões globais (Lauber; Eberli, 2021). A obtenção de um relatório substancial representou um sucesso diplomático significativo (Tiirmaa-Klaar, 2021; Paulus, 2024), reforçando o compromisso histórico do Brasil com os princípios de sua política externa e sua coerência na atuação multilateral.

Segundo informações obtidas em entrevistas informais com diplomatas[29] (comunicação pessoal, 2024), a continuidade desse posicionamento pode ser observada na atuação do corpo diplomático brasileiro ao longo do período analisado, com um ponto de convergência na figura do Embaixador Marcelo Câmara. Reconhecido como o primeiro "ciber-diplomata" brasileiro (Brotherhood, 2024), sua atuação como representante no GGE de 2017 foi fundamental para a introdução da ideia de um grupo de composição aberta — proposta que, apesar de não ter sido formalmente adotada naquele momento (Brotherhood, 2024), refletiu o compromisso do Brasil com o multilateralismo e a universalização do debate. O Embaixador seguiu responsável por orientar os posicionamentos brasileiros nesses fóruns, exercendo a

[29] As informações obtidas por meio de entrevistas informais com diplomatas foram registradas a partir de anotações e não foram gravadas ou transcritas integralmente. Para preservar o anonimato das fontes e em conformidade com as normas da ABNT, essas entrevistas são citadas como "comunicação pessoal" e não constam na lista de referências, conforme a NBR 10520:2023.

função de Diretor do Departamento de Assuntos Estratégicos, de Defesa e de Desarmamento (Brasil, 2022), órgão que supervisiona a Divisão de Defesa e Segurança Cibernética (DCiber), criada em abril de 2022 pelo Decreto nº 11.024/2022 (Brasil, 2022; comunicação pessoal, 2024). Explorar essa trajetória poderá contribuir para uma compreensão mais profunda da institucionalização da abordagem diplomática brasileira nesse campo.

Além disso, os discursos oficiais do Brasil no OEWG I e no OEWG II evidenciam certa continuidade ao longo dos anos. A análise preliminar dos discursos brasileiros em sessões finais específicas dos anos 2020, 2021, 2022, 2023 e 2024, demonstram uma argumentação consistente, alinhada aos princípios fundamentais da política externa brasileira. Em tais discursos, o Brasil reiterou a necessidade de reconhecimento do *acquis* sobre a aplicabilidade do Direito Internacional, incluindo os princípios estabelecidos nos GGEs anteriores (Brasil, 2020b, 2020b, 2022, 2023, 2024b), e enfatizou que o OEWG representa um espaço adequado para esclarecer entendimentos sobre essa aplicabilidade. Uma investigação mais aprofundada sobre o contexto de formulação desses discursos e os atores envolvidos em sua construção poderia enriquecer a compreensão sobre a estabilidade da atuação brasileira nesses fóruns. Além disso, acredita-se que a análise discursiva ao longo dos anos de atuação do Brasil nesses fóruns — sobretudo considerando a relevância do discurso na construção de normas — representa uma abordagem promissora para compreender os processos normativos internacionais.

Ademais, levanta-se a hipótese de que essa continuidade diplomática esteja relacionada à institucionalização de diplomatas responsáveis por essa agenda ao longo do tempo e à relativa autonomia do Itamaraty frente às conjunturas políticas domésticas (Paulus, 2024). No entanto, essa relação ainda demanda estudos mais aprofundados para avaliar em que medida esses fatores influenciam a constância do posicionamento brasileiro no cenário multilateral. Pesquisas futuras poderiam explorar, com base em documentos oficiais e entrevistas com diplomatas, até que ponto a tradição institucional do Itamaraty e a rotatividade de seus quadros impactam sua atuação nesses fóruns.

CONSIDERAÇÕES FINAIS

Os apelos por normas para proteger e estabilizar o ciberespaço tornaram-se onipresentes, refletindo a crescente preocupação com a governança digital e a segurança cibernética. No entanto, o sucesso desses esforços depende não apenas do conhecimento técnico sobre segurança cibernética, mas também da compreensão conceitual sobre o

funcionamento, a disseminação e a efetividade das normas no contexto internacional (Finnemore, 2017). Construir novas normas é um processo desafiador, frequentemente enfrentando resistência e obstáculos estruturais, mas fatores como liderança influente e ampla adesão podem contribuir para seu sucesso.

As normas cibernéticas ganham destaque porque mecanismos regulatórios tradicionais, como tratados internacionais, enfrentam desafios de implementação, especialmente em relação à atribuição de operações cibernéticas (Paulus, 2021). Nesse contexto, a prática dos Estados e a *opinio juris* desempenham papel fundamental na evolução do direito internacional consuetudinário, tornando essencial que diplomatas e formuladores de políticas compreendam as dinâmicas do ciberespaço e sua interação com o direito internacional (Lotrionte, 2022).

A adesão dos Estados às normas cibernéticas estabelecidas no âmbito da ONU fortalece a resiliência cibernética, promove a credibilidade internacional e contribui para a construção de um ambiente digital mais seguro e previsível. Além disso, incentiva a transparência, a confiança e a cooperação entre os países, reduzindo riscos e prevenindo conflitos desnecessários (Hoogeveen, 2021).

No contexto brasileiro, a busca por maior protagonismo na governança do ciberespaço reflete sua política externa voltada para a promoção da igualdade e da inclusão digital. Como aponta Cervo, um país que almeja autonomia estratégica deve manter seus referenciais conceituais ao longo do tempo, adaptando-se às mudanças sistêmicas sem perder de vista suas prioridades (Cervo, 2008 em Saraiva, 2014). Dessa forma, a participação ativa do Brasil e de outros países em desenvolvimento é essencial para garantir que a aplicação do direito internacional no ciberespaço não reforce desigualdades existentes, mas, ao contrário, contribua para a construção de um ambiente digital mais equitativo e acessível.

Para aprofundar a compreensão do papel do Brasil na formulação de normas internacionais, é fundamental o contínuo estudo desse tema. Um caminho promissor para pesquisas futuras seria um estudo comparativo entre diferentes períodos da política externa brasileira, especialmente considerando a mudança ideológica e estratégica entre os governos Lula I e II — marcados pela diplomacia "altiva e ativa" — e os governos Dilma, Temer, Bolsonaro e Lula III. Tal análise permitiria avaliar em que medida as conjunturas domésticas influenciam a atuação diplomática do Brasil no cenário internacional e sua coerência em fóruns multilaterais.

Por fim, o monitoramento contínuo das posições nacionais, sobretudo dos países em desenvolvimento, é crucial para ampliar a diversidade de perspectivas nesse debate e evitar a cristalização de assimetrias tecnológicas e regulatórias. A política externa brasileira para

temas digitais deve, portanto, seguir comprometida com a redução dos hiatos tecnológicos, promovendo um ciberespaço mais inclusivo, seguro e alinhado com os princípios do multilateralismo e da cooperação internacional.

REFERÊNCIAS BIBLIOGRÁFICAS

ABBOTT, Kenneth W.; SNIDAL, Duncan. **Hard and Soft Law in International Governance.** International Organization, v. 54, n. 3, p. 421-456, Summer 2000. Cambridge: The MIT Press. Disponível em: https://www.jstor.org/stable/2601340. Acesso em: 15/02/2025.

ABDALLA FILHO, Eduardo Mamed; PEDAES, Kaique Souza; OLIVEIRA, Pedro Henrique Petrocelli de; OLIVEIRA, Yan Castro de; ROCHA, Guilherme Otávio Barbosa de Oliveira; GARCIA, Daiene Kelly. **Defesa cibernética no Brasil: análise da atuação do Ministério da Defesa na Copa do Mundo de 2014 e nas Olimpíadas de 2016.** Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/defesaa_ciberneticaa_noa_brasila_analisea_daa_atuacaoa_doa_ministerioa_daa_defesaa_naa_copaa_doa_mundoa_dea_2014a_ea_nasa_olimpiadasa_dea_2016.pdf. Acesso em: 22/02/2025.

ADAMSON, Liisi. **International Law and International Cyber Norms: A Continuum?** In: BROEDERS, Dennis; VAN DEN BERG, Bibi (Eds.). Governing Cyberspace: Behavior, Power, and Diplomacy. London: Rowman & Littlefield, 2020. p. 19-44.

ANDRADE, Elisa Maria Woehl de. **Segurança cibernética: uma análise das consequências geradas por ataques hackers dentro do sistema internacional.** Universidade Federal do Pampa, Santana do Livramento, 2023.

BARRINHA, A., & RENARD, T. **Cyber-diplomacy: the making of an international society in the digital age.** Global Affairs, 3(4–5), 353–364. 2017. Disponível em: https://doi.org/10.1080/23340460.2017.1414924.Acesso em: 04/11/2024.

BELLI, Luca; FRANQUEIRA, Bruna; et al. **Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil.** FGV. 2023. Disponível em: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil. Acesso em: 16/02/2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia Nacional de Segurança Cibernética** – E-Ciber. Brasília, DF: GSI/PR, 2020a. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber. Acesso em: 16/02/2025.

BRASIL. Missão do Brasil nas Nações Unidas. **Declaração da Delegação do Brasil na Segunda Sessão Substantiva do OEWG sobre Segurança no Uso das TICs.** Nova York, 11 fev. 2020b. Disponível em: https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/11Feb_Brazil.pdf. Acesso em: 22/02/2025.

BRASIL**. Brazil's views on the future regular institutional dialogue on information and communication technology in the context of international security.** 2021a. Disponível em: docs-library.unoda.org. Acesso em: 17/02/2025.

BRASIL. Missão do Brasil nas Nações Unidas. **Declaração da Delegação do Brasil na Terceira Sessão Substantiva do OEWG sobre Segurança no Uso das TICs.** Nova York,

8-12 mar. 2021b. Disponível em: https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/statements/8March_Brazil.pdf. Acesso em: 22/02/2025.

BRASIL. Missão do Brasil nas Nações Unidas. **Declaração da Delegação do Brasil na Terceira Sessão Substantiva do OEWG sobre Segurança no Uso das TICs** – Comentários sobre o Relatório de Progresso. 27 jul. 2022. Disponível em: https://documents.unoda.org/wp-content/uploads/2022/07/Brazil-part-1.pdf. Acesso em: 22/02/2025.

BRASIL. **Missão do Brasil nas Nações Unidas. Declaração da Delegação do Brasil nas Sessões Intersecionais do OEWG sobre Segurança no Uso das TICs.** Maio de 2023. Disponível em: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_May_2023_intersessional_-_Brazil.pdf. Acesso em: 22/02/2025.

BRASIL. **Discurso do Brasil na 3ª Reunião Plenária do Open-Ended Working Group (OEWG).** Webtv UN, 05 de março. 2024a. Disponível em: https://webtv.un.org/en/asset/k1f/k1flooc3za. Acesso em: 16/02/2025. Parte citada: 05min43s – 12min33s.

BRASIL. **Discurso do Brasil na 4ª Reunião Plenária do Open-Ended Working Group (OEWG).** Webtv UN, 05 de março. 2024b. Disponível em: https://webtv.un.org/en/asset/k18/k18kielg65. Acesso em: 16/02/2025. Parte citada: 02h15min09s – 2h18min39s.

BRASIL. **Discurso do Brasil na 5ª Reunião Plenária do Open-Ended Working Group (OEWG).** Webtv UN, 06 de março. 2024c. Disponível em: https://webtv.un.org/en/asset/k14/k14wfj6q3t. Acesso em: 16/02/2025. Parte citada: 02h00min58s – 2h05min47s.

BRASIL. **Discurso do Brasil na 8ª Reunião Plenária do Open-Ended Working Group (OEWG).** Webtv UN, 07 de março. 2024d. Disponível em: https://webtv.un.org/en/asset/k1x/k1x5na3qc8. Acesso em: 16/02/2025. Parte citada: 02h34min16s – 2h37min40s.

BRASIL. **Discurso do Brasil na 9ª Reunião Plenária do Open-Ended Working Group (OEWG).** Webtv UN, 08 de março. 2024e. Disponível em: https://webtv.un.org/en/asset/k13/k13wagbh8g. Acesso em: 16/02/2025. Parte citada: 50min23s – 54min25s.

BROTHERHOOD, Rafael Oliveira. **Cibersegurança e Cyberdiplomacy: O papel da diplomacia brasileira nas Nações Unidas para a normatização do ciberespaço**. 2024. Dissertação (Mestrado em Relações Internacionais) – Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa, Lisboa, 2024.

BROEDERS, Dennis; VAN DEN BERG, Bibi. **Governing Cyberspace: Behavior, Power, and Diplomacy**. Lanham: Rowman & Littlefield, 2020.

CORTE INTERNACIONAL DE JUSTIÇA. **Caso do Canal de Corfu (Reino Unido da Grã-Bretanha e Irlanda do Norte v. Albânia)**. Sentença de 9 de abril de 1949. Disponível em: https://www.icj-cij.org/en/case/1. Acesso em: 17/02/2025.

CHOUCRI, Nazli. **Cyberpolitics in International Relations.** MIT Press, 2012.

CLORAMIDINE, F.; WIBISONO, A. A. **Global Cyber Norms Subsidiarity (UN GGE and UN OEWG) within ASEAN's Body.** Hasanuddin Journal of Strategic and International Studies (HJSIS), 2(2), 21-37. 2024.

CREEMERS, R. **Cyber China: Upgrading Propaganda, Public Opinion Work, and Social Management for the Twenty-First Century.** Journal of Contemporary China, v. 26, n. 103, p. 85-100, 2017. DOI: 10.1080/10670564.2016.1206281.

CORRÊA, Luiz Felipe de Seixas. **O Brasil e o mundo no limiar do novo século: diplomacia e desenvolvimento.** Revista Brasileira de Política Internacional, Brasília, v. 42, n. 1, p. 5-12, jun. 1999. Disponível em: https://www.scielo.br/j/rbpi/a/XJKWTjCpkyDQkNXH5bwC77t/?lang=pt. Acesso em: 17 fev. 2025.

DIGITAL WATCH OBSERVATORY. **UN Open-ended Working Group (OEWG).** Disponível em: https://dig.watch/processes/un-gge. Acesso em: 06/02/2025.

EICHENSEHR, Kristen E. **Ukraine, Cyberattacks, and the Lessons for International Law**. AJIL Unbound. 2022. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ukraine-cyberattacks-and-the-lessons-for-international-law/69B36016B06998BCE1EC67C757CDF34D. Acesso em: 22/02/2025

FINNEMORE, Martha; HOLLIS, Duncan B. **Cybersecurity and the Concept of Norms.** Carnegie Endowment for International Peace, 30 nov. 2017. Disponível em: https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870. Acesso em: 17/02/2025.

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE (GCSC). **Advancing Cyberstability: Final Report.** Hague: GCSC, 2019.

GREENWALD, G. **Sem lugar para se esconder: Edward Snowden, a NSA e a espionagem do governo norte-americano.** Rio de Janeiro: Editora Sextante. 2014.

HENRIKSEN, Anders. **The end of the road for the UN GGE process: The future regulation of cyberspace.** Journal of Cybersecurity, v. 5, n. 1, p. 1–9, 2019. Disponível em: https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865. Acesso em: 28/01/ 2025.

HOGEVEEN, B. **The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN**. Australia: ASPI. 2022. Disponível em: https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace. Acesso em: 17/01/2025.

HUREL, Louise Marie. **Securitização e a governança da segurança cibernética no Brasil.** In: HORIZONTE presente: tecnologia e sociedade em debate. Belo Horizonte: Editora Letramento, 2019. p. 321-342. Disponível em: https://www.researchgate.net/publication/329973134_Securitizacao_e_Governanca_da_Seguranca_Cibernetica_no_Brasil. Acesso em: 17/01/2025.

HUREL, Louise M. **Cibersegurança no Brasil: uma análise da estratégia nacional.** Artigo Estratégico 54. Instituto Igarapé, Abril, 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 17/01/2025.

HUREL, Louise M. **The rocky road to cyber norms at the United Nations.** Council on Foreign Relations. 2022. Disponível em: https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0. Acesso em: 06/02/2025.

KELLO, Lucas. **The Virtual Weapon and International Order**. Yale University Press, 2017.

KEOHANE, R. O. After Hegemony: **Cooperation and Discord in the World Political Economy.** Princeton University Press. 1984.

KISSINGER, Henry**. World order**. New York: Penguin Press, 2015.

KLIMBURG, Alexander; ALMEIDA, Virgílio A. F. **Internet Governance: Cyber Peace and Cyber Stability, Taking the Norm Road to Stability.** IEEE Internet Computing, [S.l.], v. 23, n. 4, p. 61-67, 2019. Disponível em: https://doi.org/10.1109/MIC.2019.2926847.

KUMAR, Sheetal; BARBER, Ian; TIKK, Eneken. **Unpacking the GGE's framework on responsible state behaviour: International law.** Global Partners Digital, 2021. Disponível em: https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-capacity-building-2/. Acesso em: 18/01/2025.

LAUBER, Jurg; EBERLI, Lukas. **From confrontation to Consensus: taking Stock of the OEWG Process**. Cyberstability Paper Series. The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace. 2021.

LÉVY, Pierre. **Cibercultura.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999. Cap. 5, p. 92-94.

LOTRIONTE, Catherine. **Bringing the law in: unlearned lessons for diplomats and others.** In: DEMCHAK, Chris C.; SPIDALIERI, Francesca (Eds.). Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020. West Point: Army Cyber Institute, The Cyber Defense Review, 2022. p. 23-32.

LUCERO, E. Governança da Internet: **Aspectos da formação de um regime global e oportunidades para a ação diplomática.** Fundação Alexandre Gusmão. 2011. Disponível em: https://funag.gov.br/biblioteca-nova/produto/1-74-governanca_da_internet_aspectos_da_form

acao_de_um_regime_global_e_oportunidades_para_a_acao_diplomatica. Acesso em: 16/02/2025.

MANDARINO, Rafael Junior. **Segurança e defesa do espaço cibernético brasileiro.** Recife: CUBZAC, 2010. p. 40-41.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Resolução A/RES/53/70, Assembleia Geral, 1998. Disponível em: https://digitallibrary.un.org. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/58/373, Assembleia Geral, 2003. Disponível em: https://documents.un.org/doc/undoc/gen/n03/454/83/pdf/n0345483.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/60/95, Assembleia Geral, 2005a. Disponível em: https://documents.un.org/doc/undoc/gen/n05/453/63/pdf/n0545363.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/60/202, Assembleia Geral, 2005b. Disponível em: https://documents.un.org/doc/undoc/gen/n05/490/30/pdf/n0549030.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/65/201, Assembleia Geral, 2010. Disponível em: https://documents.un.org/doc/undoc/gen/n10/469/57/pdf/n1046957.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.** Relatório A/68/98, Assembleia Geral, 2013. Disponível em: https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS**.** Conselho de Direitos Humanos. **The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights.** A/HRC/27/37. Genebra: ONU, 2014. Disponível em: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/A-HRC-27-37_en.pdf. Acesso em: 17/02/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/70/174, Assembleia Geral, 2015a. Disponível em: https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Resolução A/RES/70/237, Assembleia Geral, 2015b. Disponível em: https://docs.un.org/en/A/RES/70/237. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **The role of science and technology in the context of international security and disarmament.** Resolução A/RES/71/28. Assembleia Geral, 2016. Disponível em: https://undocs.org/A/RES/71/28. Acesso em: 06/02/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/72/327, Assembleia Geral, 2017. Disponível em: https://documents.un.org/doc/undoc/gen/n17/257/46/pdf/n1725746.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Resolução A/73/27. Assembleia Geral, 73ª Sessão, 5 nov. 2018a. Disponível em: https://docs.un.org/en/A/RES/73/27. Acesso em: 6/02/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/73/266, Assembleia Geral, 2018b. Disponível em: https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Nova York: Nações Unidas, 2020. Disponível em: https://docs.un.org/en/A/RES/75/240. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/76/135, Assembleia Geral, 2021a. Disponível em: https://documents.un.org/doc/undoc/gen/n21/075/86/pdf/n2107586.pdf. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Developments in the field of information and telecommunications in the context of international security.** Relatório A/75/816. Assembleia Geral, 2021b. Disponível em: https://docs.un.org/en/A/75/816. Acesso em: 28/01/2025.

NAÇÕES UNIDAS. **Voluntary national contributions on how international law applies to the use of information and communications technologies by States**. Relatório 76/136, Assembleia Geral, 13 jul. 2021c. Disponível em: https://undocs.org/en/A/76/136. Acesso em: 16/02/2025.

NAÇÕES UNIDAS. **Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.** Relatório A/77/37. Assembleia Geral, 2022. Disponível em: https://docs.un.org/en/A/res/77/37. Acesso em: 28/01/2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Department of Defense strategy for operating in cyberspace.** [S.l.: s.n.], 2011. Disponível em: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Acesso em: 16/12/2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.** Gaithersburg: NIST, 2018.

Disponível em: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf. Acesso em: 9/01/2025.

NETMUNDIAL. **NETmundial Multistakeholder Statement.** São Paulo: CGI.br, 2014. Disponível em: https://netmundial.br. Acesso em: 17/02/2025.

NYE, Joseph S. **The Future of Power.** New York: PublicAffairs, 2011.

PAULUS, Alexandra. **Building Bridges In Cyber Diplomacy: How Brazil Shaped Global Cyber Norms.** German Institute for International and Security Affairs (SWP). Berlin, Germany. 2024.

RAMALHO, Antonio Jorge. 2023**."Inovações na Era Digital: usos e riscos para a ação do Estado na política internacional"**. CEBRI-Revista Ano 2, Número 7: 17-40.

RUHL, Christian; HOLLIS, Duncan; HOFFMAN, Wyatt; MAURER, Tim. **Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.** Washington, DC: Carnegie Endowment for International Peace, 2020.

SANTOS, Ilana Danielle Soares. **A ascensão do ciberespaço como tema de Relações Internacionais: Uma análise da produção científica de RI e dos conceitos aplicados à sua interpretação.** 2021. Dissertação (Mestrado em Relações Internacionais) – Universidade de Brasília, Brasília, 2021.

SARAIVA, José Flávio Sombra. **Autonomia na inserção internacional do Brasil: um caminho histórico próprio.** Contexto Internacional, Rio de Janeiro, v. 36, n. 1, p. 9-41, jan./jun. 2014.

SCHMITT, Michael N. **Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace.** Texas National Security Review, v. 3, n. 3, out. 2020.

SCHMITT, Michael N. **The Sixth United Nations GGE and International Law in Cyberspace.** Just Security. 2021. Disponível em: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/. Acesso em: 21/01/2025.

SINGAPORE INTERNATIONAL CYBER WEEK (SICW). **National Positions on International Law in Cyberspace.** 2024. Disponível em: https://www.sicw.gov.sg/events/15-oct/national-positions-on-international-law-in-cyberspace/#:~:text=States%20have%20agreed%20that%20international,North%2C%20have%20issued%20such%20positions. Acesso em: 16/02/2025.

SINGER, P. W., FRIEDMAN, Allan. **Cybersecurity and Cyberwar: what everyone needs to know.** Oxford University Press. New York. 2014.

TIIRMAA-KLAAR, Heli. **The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body. Cyberstability Paper Series.** The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace. 2021.

TIKK-RINGAS, Eneken. **International Cyber Norms Dialogue as an Exercise of Normative Power.** Georgetown Journal of International Affairs, v. 17, n. 3, p. 47-59, Fall/Winter, 2016. Disponível em: https://www.jstor.org/stable/26395975. Acesso em: 15/02/2025.

UNIÃO EUROPEIA (UE). **Regulamento 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação de cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança).** Disponível em: https://eur-lex.europa.eu/eli/reg/2019/881/oj. Acesso em: 09/01/2025.

UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). **"Open-Ended Working Group on Information and Communication Technologies"**. Disponível em: https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021. Acesso em: 06/02/2025.

WORLD ECONOMIC FORUM (WEF). **Global Risks Report 2023**. World Economic Forum. 2024. Disponível em: https://www.weforum.org/publications/global-risks-report-2024/. Acesso em: 24/11/24**.**