CIBERDIPLOMACIA E MULTISTAKEHOLDER DIPLOMACY: UMA ANÁLISE INTRODUTÓRIA

Lauren Giordani Gröhs[1]

RESUMO

O crescente avanço e a pluralidade do mundo cibernético têm ampliado a complexidade das interações no sistema internacional, evidenciando a necessidade de regulamentação e mediação no campo da cibersegurança. Este estudo explora como a diplomacia multistakeholder pode ser aplicada à ciberdiplomacia para facilitar debates e a resolução de conflitos no ciberespaço. A pesquisa analisa diferentes perspectivas sobre cibersegurança, com ênfase em fóruns como o *Paris Call for Trust and Security in Cyberspace*, que utilizam a ciberdiplomacia como instrumento central para discussões globais. Os resultados mostram a multistakeholder diplomacy como uma ferramenta inovadora e eficaz para promover governança inclusiva no ciberespaço, embora sejam identificados desafios significativos para sua implementação. A ausência de regulamentação adequada no uso de tecnologias emergentes entre os diversos atores envolvidos é destacada como um risco relevante para a estabilidade e a cooperação no sistema internacional.

Palavras-chave: ciberdiplomacia; cibersegurança; multistakeholder; sistema internacional.

1 INTRODUÇÃO

Há diversas perspectivas sobre a inclusão de novas tecnologias e ameaças cibernéticas nas políticas do sistema internacional. Um ponto central desse debate é a necessidade de discutir as medidas de promoção e proteção que podem ser adotadas por organismos e atores internacionais para compreender as vantagens e desvantagens desse cenário. Nesse contexto, o estudo de novas abordagens diplomáticas é essencial para a adaptação desses novos cenários no sistema internacional, destacando-se a ciberdiplomacia. Através da análise dessa diplomacia específica é que se torna possível traçar hipóteses sobre seu processo de construção e atuação nas relações internacionais.

A ciberdiplomacia pode ser amplificada por meio da aplicação da diplomacia multistakeholder, um instrumento que estabelece a responsabilização de todos os atores do sistema internacional para a construção de uma governança transnacional.O uso da diplomacia multistakeholder como ferramenta de análise e debate na ciberdiplomacia possibilitará a construção conjunta de tomadas de decisão e soluções, envolvendo diversos atores, com o objetivo de reduzir as ameaças cibernéticas no

[1]Discente do Curso de Relações Internacionais da Universidade La Salle, e-mail: lauren.202111099@unilasalle.edu.br. Artigo desenvolvido em caráter de Trabalho de Conclusão de Curso sob orientação do Prof. Dr. Fabricio Pontin, e-mail: fabricio.pontin@unilasalle.edu.br. Data de Entrega: 13 de dezembro de 2024.

cenário internacional. No entanto, para integrar essa metodologia nos debates internacionais sobre o ciberespaço, é fundamental compreender como a segurança cibernética se desenvolve em um mundo cada vez mais globalizado e quais seriam as implicações de uma gestão diplomática mais eficiente nesse cenário.

Este artigo propõe explorar essas interseções. No primeiro tópico, será examinada a evolução histórica do conceito de segurança internacional, desde as primeiras reflexões filosóficas até as abordagens contemporâneas, que introduzem o campo da segurança cibernética. Essa análise histórica permite observar como a ideia de segurança evoluiu para incorporar as crescentes ameaças do ciberespaço, como guerras cibernéticas, inteligência artificial e vigilância, que impactam diretamente o sistema internacional e levantam questões éticas fundamentais na sociedade atual. A cibersegurança, ao ganhar espaço nas agendas globais, reforça a necessidade de uma abordagem multilateral que transcenda os limites estatais.

O segundo tópico analisará a ciberdiplomacia como um instrumento essencial para compreender e mediar o impacto das tecnologias digitais nas políticas externas e na interação entre os Estados. Através de uma apresentação teórica sobre o conceito, o texto também explora exemplos práticos de quais são os atuais debates sobre o ciberespaço em fóruns internacionais. Entre eles está o desenvolvimento dos limites do uso da internet e a utilização de mecanismos tecnológicos por parte dos Estados e outros atores, destacando o *Internet Corporation for Assigned Names and Numbers* (ICANN) e a Cúpula Mundial sobre a Sociedade da Informação (WSIS), fóruns de debates multilaterais que demonstraram a importância de inclusão de diferentes atores para repensar medidas e regulamentações em conjunto.

A complexidade do ciberespaço, combinada com a multiplicidade de atores envolvidos, exige novas formas de governança. É nesse cenário que, na continuação do segundo tópico, será explorada a diplomacia multistakeholder. Essa abordagem pode ampliar o escopo da tomada de decisão para incluir nos debates os Estados, empresas, organizações internacionais, academia e a sociedade civil. Como base de entendimento, serão abordadas plataformas de diálogo global, como o *Paris Call for Trust and Security in Cyberspace* e as iniciativas das Nações Unidas, como o *Open-Ended Working Group* (OEWG) que tratam sobre o tema. Essas ferramentas exemplificam o esforço coletivo para regulamentar a governança da internet, consolidando o ciberespaço como um campo de ação diplomática crucial na era digital e na inovação dos processos diplomáticos nas relações internacionais.

2 CIBERSEGURANÇA: DEFINIÇÕES E IMPACTOS DENTRO DO DEBATE DE SEGURANÇA INTERNACIONAL

Para entender a construção do conceito de cibersegurança e diplomacia multistakeholder na esfera internacional, é fundamental examinar a evolução da segurança internacional desde a consolidação dos Estados. Dessa forma, a primeira parte do tópico traçará uma linha do tempo do desenvolvimento do conceito de segurança, analisando desde suas primeiras vertentes, com Maquiavel (2009) e Hobbes (2003), até as abordagens contemporâneas, como a segurança discursiva de Buzan (1998) e a segurança cibernética de Clarke e Knake (2010). Na segunda parte, será contextualizado o papel da segurança cibernética nas Relações Internacionais,

identificando as tecnologias atuais em uso nesse campo. Com isso, será possível delimitar conceitos como guerra cibernética, inteligência artificial e vigilância, que têm ganhado destaque no sistema internacional e apresentam relevância crucial para as questões éticas e de sobrevivência da humanidade. A partir da compreensão do que constitui segurança internacional e das diferentes tecnologias que impactam o sistema internacional, torna-se evidente o papel crescente da ciberdiplomaia como um tópico central no diálogo internacional.

2.1 Segurança internacional: conceitos e debates

Ao decorrer dos anos, o conceito de segurança internacional foi se consolidando, aprimorando-se e gerando novas vertentes. O debate sobre segurança é antigo e remonta às primeiras entidades políticas organizadas, que estabeleceram as definições de Estado e Nação. Um dos primeiros estudos sobre a formulação de segurança do Estado e o uso do poder é encontrado no livro “O Príncipe”, de Maquiavel (2009). Nele, o autor formula formas estratégicas do uso da força, da astúcia e da diplomacia para proteger o Estado, enfatizando que a sobrevivência do Estado deve ser o foco para o governante, mesmo que isso exija medidas moralmente questionáveis (Maquiavel, 2009).

Outros estudos clássicos contribuíram para moldar as percepções de Estado e a importância da segurança nesse contexto. De acordo com Hobbes (2003), a segurança é o objetivo principal da vida política e a consolidação da segurança para uma vida civilizada é inerente ao estado de natureza dos indivíduos. Ainda o mesmo autor descreve que, na ausência de um poder comum, os homens encontrariam-se “numa condição que se chama guerra; e é uma guerra de todos contra todos” (Hobbes, 2003, p.112). A construção do Contrato Social que Hobbes (2003) propunha seria uma forma de garantir a segurança coletiva e buscar a paz como um princípio fundamental. Assim, a criação de normas e instituições serviria para proteger os indivíduos da guerra e da violência.

Através da paz é possível discutir a segurança, não apenas em âmbito local, mas extrapolando para uma segurança global. Kant (2008), em “A Paz Perpétua”, provoca esse debate ao oferecer uma federação de repúblicas democráticas como forma de garantir a paz e, por extensão, a segurança internacional. Para o mesmo autor, a paz perpétua não é apenas um ideal, mas uma obrigação moral e prática que os Estados devem perseguir (Kant, 2008). Dessa forma, a segurança seria assegurada por meio de um direito internacional comum fundado em um federalismo de Estados livres e iguais (Kant, 2008) e na cooperação internacional. Nesse sentido, Kant (2008) propõe um sistema baseado em princípios comuns de direito e moralidade para garantir a segurança de forma perpétua. Contudo, essa perspectiva liberal e cosmopolita parece ser insuficiente em um mundo de constantes manutenções no equilíbrio de poder.

A insuficiência do modelo elaborado por Kant (2008) fica mais latente ao se abordar o problema da segurança desde um viés realista. Nesta perspectiva, a segurança pode ser considerada como inerente a um sistema internacional anárquico, em que cada Estado é responsável por sua própria segurança, estabelecendo diferentes níveis de poder para manter o equilíbrio no cenário global. Como caracterizado por Waltz (1979), essa lógica reflete uma visão realista da anarquia internacional, onde os Estados competem constantemente pela sobrevivência e

segurança, devido à ausência de uma autoridade superior que os regule. Partindo dessa abordagem, o dilema de segurança proposto por Herz (1950) elucida essa dinâmica. Segundo o mesmo autor, o ciclo de insegurança mútua leva os Estados a aumentar suas capacidades de proteção para garantir sua segurança (Herz, 1950), o que resulta ao aumento de proteção de ambos os lados gerando maior insegurança para todos os envolvidos. De acordo com o autor:

> *The unanswered question as to whom these divisions were to do battle with was soon to be answered by history itself: not perceiving a common enemy, they would turn against each other. This turning against each other had as one of its major reasons the security dilemma of politically unintegrated units, and their ensuing competition for power*[2] (Herz, 1950, p. 163).

A busca pela segurança também pode estar intrinsecamente atrelada à busca pela hegemonia, uma vez que o equilíbrio na balança de poder depende do reconhecimento de poder por parte de outros Estados. A perspectiva ofensiva de Mearsheimer (2001, p. 30) coloca o conflito como inevitável, argumentando que "*the structure of the international system forces states which seek only to be secure nonetheless to act aggressively toward each other*"[3] sendo essa a trágica realidade da política internacional. Tanto as perspectivas de Waltz (1979) quanto de Mearsheimer (2001) tendem a desconsiderar as instituições internacionais e as normas por elas estabelecidas para promover a cooperação internacional.

No entanto, conforme proposto por Buzan et al (1998), o processo de securitização pode ser considerado um mecanismo de promoção da segurança internacional por meio do diálogo entre diferentes atores no sistema internacional. A Escola de Copenhague, que emergiu na década de 1980 com esses pesquisadores, focou não apenas na segurança militar, mas também em outros tipos de ameaças que afetam a segurança internacional. Ao fim da Guerra Fria, o *Centre for Peace and Conflict Research*, tornou-se a Escola de Copenhague, adotando uma abordagem construtivista para entender os novos conceitos de segurança (Duque, 2009). Essa perspectiva propõe a compreensão da segurança considerando novos fatores: militar, político, econômico, social e ambiental, não se limitando a entender a segurança como algo objetivo, mas também incorporando novas percepções e representações discursivas.

De acordo com Buzan et al (1998), a securitização é um "ato de fala", no qual um ator do sistema internacional deve declarar publicamente a sua ameaça, gerando um processo discursivo entre os envolvidos para buscar resoluções. Essa nova abordagem possibilitou maiores debates políticos e acadêmicos, além de reformular o conceito de segurança em um mundo mais globalizado e interconectado. A segurança é um conceito dinâmico e, a partir desse novo contexto, novas formas de ameaça foram identificadas, como a guerra cibernética e as implicações para a segurança nacional. Clarke e Knake (2010) foram pioneiros em trazer a pauta de defesa contra ataques

---

[2] Tradução própria: "A questão sem resposta sobre com quem essas divisões deveriam travar batalha logo seria respondida pela própria história: ao não perceberem um inimigo comum, elas se voltariam umas contra as outras. Esse confronto entre elas teve como uma de suas principais razões o dilema de segurança das unidades politicamente desintegradas e a consequente competição por poder."

[3] Tradução própria: "a estrutura do sistema internacional força os estados, que buscam apenas segurança, a agirem de forma agressiva uns em relação aos outros".

cibernéticos, enfatizando a vulnerabilidade das infraestruturas e a busca por normas e leis internacionais para regular os Estados no ciberespaço.

Segundo Clarke e Knake (2010), guerras cibernéticas são reais, globais e já iniciaram, devendo ser tratadas com urgência e seriedade por parte dos Estados como um novo risco à segurança internacional. O debate sobre o tema surgiu após o ataque cibernético à Estônia em 2007, no qual hackers bloquearam o sistema de todo país. Esse evento evidenciou uma nova ameaça e também o despreparo dos Estados para lidar com esse novo cenário. Neste contexto, os mesmos autores propõem um conjunto de medidas para mitigar as ameaças cibernéticas, como o desenvolvimento de normas internacionais que regulem o ciberespaço, investimentos em tecnologias cibernéticas e em especialistas em guerra cibernética (Clarke; Knake, 2010). A partir desse estudo e propostas, o tema de novas ameaças em um campo ainda pouco explorado como o do ciberespaço possibilitou uma reflexão sobre os impactos das novas tecnologias no sistema internacional.

2.2 Impacto de novas tecnologias nas Relações Internacionais

Inovações tecnológicas como Inteligência Artificial, guerras cibernéticas, tecnologias de informação, comunicação e vigilância estão transformando a dinâmica de poder, as ameaças de segurança internacional e a forma como os Estados interagem. O desenvolvimento de tecnologias digitais expôs as vulnerabilidades de infraestruturas críticas de Estados e empresas, como redes elétricas, sistemas financeiros e comunicações. É nesse contexto que a cibersegurança se torna um importante tópico a ser debatido no sistema internacional, pois abrange a proteção e a governança do ciberespaço no contexto global. O ataque cibernético à Estônia, ocorrido em 2007, é amplamente considerado o marco inicial que tornou a cibersegurança uma questão global, sendo referido por muitos pesquisadores como o "*Web War One* (WW1)" (Clarke; Knake, 2010).

A Estônia foi considerada por muitos anos uma das sociedades mais avançadas tecnologicamente do mundo, conhecida por ter uma "*e-society*" (*European Commission*, 2024). Após conquistar a sua independência da União Soviética (URSS), em 1991, a Estônia passou por um rápido processo de modernização e digitalização, embora as suas tensões históricas com a Rússia tenham permanecido latentes. Em 2007, o governo estoniano decidiu realocar o "Soldado de Bronze", um monumento sovietico da Segunda Guerra Mundial, do centro da capital, Tallinn, para um cemitério militar nos arredores (Clarke; Knake, 2010). Essa decisão se deve principalmente pelo fato do monumento representar a ocupação soviética no pós-guerra, sendo este um período traumático de repressão e perda de independência.

No entanto, o Soldado de Bronze era visto pelos russos como um monumento altamente simbólico, tanto para a população de origem russa na Estônia quanto para o governo da Rússia, por representar uma homenagem aos soldados soviéticos que lutaram contra o nazismo na Segunda Guerra Mundial. Dessa forma, a remoção do monumento gerou protestos violentos entre os radicais de ambas facções étnicas do conflito no dia 27 de abril de 2007, que ficou conhecido como "*Bronze Night*" (Clarke; Knake, 2010). A partir desse dia, o campo de batalha se deslocou do mundo físico para o ciberespaço. A Estônia foi alvo de um ataque cibernético de negação de serviço

distribuída (DDoS)[4] que sobrecarregou os servidores estonianos com uma quantidade massiva de solicitações, tornando os sites inacessíveis (Clarke; Knake, 2010). Inesperadamente, órgãos governamentais, bancos, meios de comunicação e empresas privadas ficaram sem acessos, interrompendo também o sistema financeiro do país e sua comunicação pública.

A Rússia sempre negou participação no ataque cibernético, contudo também recusou o pedido diplomático formal feito pela Estônia solicitando assistência para traçar os hackers (Clarke; Knake, 2010). Várias especulações foram feitas sobre o envolvimento de crime organizado, do governo russo e dos grupos patrióticos russos na Estônia, contudo muitas perguntas ainda permanecem sem respostas. O ataque cibernético na Estônia revelou uma nova dimensão de insegurança no sistema internacional, evidenciando a vulnerabilidade de diversos sistemas digitais estatais. Esse incidente expôs a falta de preparo global para responder a ameaças cibernéticas e atuou como catalisador para a criação do Centro de Excelência de Defesa Cooperativa da OTAN (CCDCOE).

O CCDCOE, fundado em 2008, é um órgão da OTAN responsável por pesquisa e treinamento especializado em defesa cibernética, fornecendo suporte técnico e capacitação para os outros países membros da Aliança (CCDCOE, 2024). O CCDCOE integra a estrutura militar da OTAN, desempenhando um papel crucial no fortalecimento da segurança cibernética dos Estados aliados. Simultaneamente a criação desse órgão, outro ataque cibernético ocorreu na Europa, dessa vez na Geórgia. Após o colapso da URSS em 1991, a Geórgia declarou sua independência, mas enfrentou diversos conflitos étnicos e políticos, especialmente relacionados às regiões separatistas da Abecásia e da Ossétia, adeptos à autonomia ou à anexação à Rússia (Clarke; Knake, 2010). O conflito escalou, variando entre o domínio físico e o ciberespaço, sinalizando uma nova forma de conduzir a guerra no século XXI.

É interessante ressaltar a natureza dos ataques sofridos pela Geórgia nesse país, e como eles indicam o uso do domínio virtual/digital como um front de conflito. A Geórgia enfrentou uma série de ataques cibernéticos coordenados, sendo alvo de ataques DDoS que bloquearam serviços de mídia, sites governamentais e sistemas bancários. Esses resultaram no bloqueio da comunicação do governo georgiano, dificultando a transmissão de informação ao público e a comunidade internacional (Clarke; Knake, 2010). Um fato que difere o ataque cibernético na Geórgia foi a existência de diversos sites “anti-Georgia”, que forneciam o software para hackers através de um download. Ao clicar em um botão denominado *“Start Flood”* , voluntários eram convidados para participar da guerra cibernética (Clarke; Knake, 2010). Mais uma vez, a Rússia declarou que os ataques eram de grupos nacionalistas e estavam fora do controle do Kremlin. No entanto, a estrutura das atividades cibernéticas sugere que esses grupos contaram com apoio tácito ou explícito do governo russo.

Clarke e Knake (2010, p. 23) definem guerra cibernética como *“actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption”*[5]. Assim, podemos considerar o computador uma arma

[4] Distributed Denial of Service (Negação de Serviço Distribuída), é um tipo de ataque cibernético que tem como objetivo sobrecarregar os recursos de um sistema, geralmente um servidor, serviço online ou rede, tornando-o indisponível para usuários legítimos.

[5] Tradução própria: “ações de um Estado-nação para penetrar nos computadores ou redes de outro Estado com o objetivo de causar danos ou interrupções”.

poderosa que, quando aplicada a informações tecnológicas, torna a guerra cibernética uma forma destrutiva de perpetuar no Estado. Esse novo campo de batalha remete às regras mais firmes estabelecidas no estado de natureza[6] no contexto estatal, exigindo, portanto, a criação de normas nacionais e internacionais para regular esse novo cenário (Giesen, 2014). Nesse contexto, observa-se que a balança de poder cibernética favorece quem ataca primeiro, dessa forma é possível concluir que os governos tendem a investir cada vez mais em ciberdefesa para proteção de seus sistemas estatais (Giesen, 2014). A reconfiguração do atual sistema de internet e de softwares abrange diferentes tipos de ataques potenciais, desde espionagem, propaganda e intervenção. Contudo, além de conflitos cibernéticos serem estabelecidos entres Estados, também é possível ver *"non-state actors"* que, embora subordinados ao controle do Estados, operam de forma não governamental, como os grupos de hackers patrióticos na Rússia ou na China (Giesen, 2014).

Outro exemplo que evidencia o avanço no uso de softwares para promover a guerra cibernética e espionagem é o caso do Stuxnet, um *malware*[7] usado para atacar sistemas de controle industrial do programa nuclear do Irã. Em 2006, o Conselho de Segurança da ONU ordenou ao Irã a suspensão do seu programa de enriquecimento de urânio, contudo o país se recusou a seguir a diretriz, mantendo as suas atividades dentro do permitido no Tratado de Não Proliferação Nuclear (Lindsay, 2013). Estados Unidos e Israel, especialmente, estavam preocupados com o avanço desse programa. Supostamente, o Stuxnet foi desenvolvido por esses dois países como parte de uma operação secreta chamada "*Olympic Games*", que danificou mais de mil centrífugas na instalação Natanz, o mais importante centro nuclear do Irã (Lindsay, 2013).

O Stuxnet representa um marco para a cibersegurança e suscita debates sobre a "Revolução Cibernética", um conceito que sugere que ataques cibernéticos concedem vantagens assimétricas a atores militares mais fracos, tornando a defesa mais difícil e aumentando a eficácia das ofensivas (Lindsay, 2013). No entanto, Lindsay (2013) argumenta que o caso do Stuxnet revela uma realidade diferente: em vez de facilitar ofensivas para atores mais fracos, a complexidade do Stuxnet sugere que operações cibernéticas bem-sucedidas requerem recursos e capacidades técnicas significativas, favorecendo nações mais fortes e tornando a defesa cibernética mais viável que a ofensiva. Embora a mídia tenha retratado o Stuxnet como um prenúncio de uma nova era de guerra cibernética, a recuperação do programa nuclear iraniano dentro de um ano sugere que o impacto foi temporário e não decisivo. Este evento mostrou que a criação, execução e manutenção de tais operações é complexa e que a defesa cibernética é mais viável do que muitos acreditam.

Questões de defesa também estão atreladas a vigilância e privacidade digital, que quando ameaçada provoca movimentos de defesa de privacidade e reforma nas coletas de dados. Um exemplo de tecnologias de vigilância foi o caso Snowden, em 2013, que revelou uma operação de vigilância global conduzida pelos Estados Unidos. A operação foi exposta através do vazamento de diversos documentos classificados por Edward Snowden, um ex-contratado da Agência de Segurança Nacional. Entre as atividades denunciadas estavam acesso a servidores de empresas como Microsoft e

[6] A literatura realista adota a metáfora Hobbesiana na análise, tornando a condição "anárquica" entre estados espelhada no estado de natureza hobbesiano.
[7] Malware é um termo genérico que engloba diversos tipos de ameaças digitais.

Google (Bauman, 2014), registros de chamadas telefônicas e espionagem de líderes políticos aliados, como da presidenta brasileira Dilma Rousseff (Bauman, 2014). A revelação dessas atividades gerou tensões globais entre os países envolvidos e desencadeou o debate sobre os limites da vigilância, evidenciando a necessidade de estabelecer regras de privacidade e segurança global.

Da mesma forma, ao se discutir a Inteligência Artificial (IA), as questões de segurança estão se tornando cada vez mais relevantes para os Estados. Segundo Payne (2018, p.8) “sistemas de IA utilizam métodos de "aprendizagem profunda" que, embora com considerável abstração e simplificação, modelam os processos neurais dos cérebros humanos”. Estudos indicam que a IA será útil tanto a nível tático como a nível estratégico e já se configura como uma realidade, transformando atividades militares, incluindo a logística, as informações e a vigilância (Payne, 2018). No entanto, a IA pode representar um risco para o Estado, tanto em relação à tomada de decisões quanto às informações que ela retém, o que torna a ética da IA um dos principais temas em debate.

A aplicação da IA na política dos Estados representa um exemplo de risco que pode afetar na política interna, como evidenciado pelo impacto que a IA teve nas eleições presidenciais dos Estados Unidos em 2016. Diversos estudos indicam que o uso de bots e algoritmos de IA foram cruciais para a propagação massiva de *fake news*, que influenciaram o comportamento dos eleitores. Tanto o uso de “*social bots*”[8], que espalharam informações falsas nas redes sociais (Brkan, 2019), quanto o uso de algoritmos sofisticados direcionando anúncios políticos baseados em dados comportamentais dos eleitores (Brkan, 2019) exemplificam como a utilização da IA pode ter um impacto danoso. Ademais, tecnologias como *deepfakes*[9] suscitaram preocupações sobre a integridade do processo eleitoral, uma vez que podem ser empregadas para criar conteúdos enganosos com alta capacidade de enganar eleitores, dificultando ainda mais a distinção entre o real e o falso (Brkan, 2019).

Esses diferentes casos de mecanismos tecnológicos evidenciam a importância de se discutir o ciberespaço e estabelecer regras para atuação nesse domínio. Entretanto, para que isso se concretize, é necessário a colaboração entre os diferentes atores do sistema internacional em prol da criação e condução de um sistema de normas voltadas para a resolução de conflitos cibernéticos. Nesse cenário, surge a necessidade de um novo enfoque diplomático, com a incorporação da ciberdiplomacia. Por meio de uma diplomacia específica nesse campo, torna-se possível desenvolver e aplicar as ferramentas necessárias para regulação do ciberespaço. No entanto, é fundamental compreender as principais vertentes desse debate e o seu estado atual no sistema internacional.

3 DA CIBERDIPLOMACIA ATÉ A MULTISTAKEHOLDER DIPLOMACY: A CONSTRUÇÃO DE UM PARADIGMA DE SEGURANÇA

A ciberdiplomacia surge nas Relações Internacionais como um instrumento para compreender a aplicação de diversas tecnologias digitais e seus impactos nas políticas

[8] Programas automatizados que operam em plataformas de redes sociais, simulando o comportamento humano para realizar interações como postar, comentar, curtir ou compartilhar conteúdos.
[9] Vídeos falsos gerados por IA.

externas e interação entre os Estados. No entanto, a partir dessas interações, também surgiu a necessidade de incluir outros atores internacionais nesse debate para aumentar o escopo de tomada de decisão e iniciativas, sendo a diplomacia multistakeholder uma forma de fazer isso acontecer. Dessa forma, o primeiro tópico abordará as diferentes perspectivas teóricas sobre ciberdiplomacia e a forma como foi construída a ideia de uma diplomacia cibernética e como ela é aplicada no contexto internacional. No segundo tópico, será abordado o conceito de multistakeholder e seu viés teórico, aplicando esse conceito através de plataformas de diálogo que facilitam a interação entre os diversos atores do sistema internacional. Entre elas, destacam-se o *Paris Call for Trust and Security in Cyberspace* e as Nações Unidas (ONU), que servem como fóruns de discussão sobre soluções para questões que afetam o ciberespaço. A regulamentação da '*internet governance*' é um tema cada vez mais latente no mundo globalizado, e ambas ferramentas emergem como um meio de viabilizar esse debate entre todos os atores do sistema internacional, não se limitando apenas aos Estados.

3.1 Ciberdiplomacia: definição e aplicação no sistema internacional

Para compreender o surgimento da ciberdiplomacia, é importante entender o papel da diplomacia nas relações internacionais, sendo esta uma ferramenta crucial para comunicação entre Estados e outras entidades envolvidas na política global. De acordo com Bull (2002, p. 196-198) a diplomacia possui algumas funções essenciais, sendo elas:

> Em primeiro lugar, a diplomacia facilita a comunicação entre os líderes políticos dos estados e das outras entidades que participam da política mundial. [...] Uma segunda função da diplomacia é negociar acordos. [...] Uma terceira função da diplomacia é coligir informações, "inteligência" a respeito dos países estrangeiros. [...] Uma quarta função da diplomacia é minimizar os efeitos dos atritos nas relações internacionais [...] Finalmente, a diplomacia preenche a função de simbolizar a existência da sociedade dos estados.

A partir desses aspectos, é possível aplicar a diplomacia em tópicos emergentes com vista à manutenção do sistema internacional. Com a ascensão da tecnologia da informação, particularmente a internet e as redes digitais, novas dimensões de interação e conflito surgiram, gerando a necessidade de uma nova abordagem: a ciberdiplomacia.

Segundo Attafta et al., (2020, p. 61) a ciberdiplomacia "*incorporates the use of diplomatic tools and mindsets to resolve issues arising from the international use of cyberspace*"[10]. Nesse contexto, essa vertente busca promover a construção de normas globais que regulem o comportamento dos Estados e outros atores no ciberespaço, prevenindo incidentes que possam comprometer a estabilidade internacional. Da mesma forma, segundo Radanliev (2023), a ciberdiplomacia também é uma forma de promover a construção de capacidades tecnológicas para cibersegurança, através de partilha de conhecimentos especializados e transferência de tecnologias. Um dos desafios atuais da cibersegurança é a identificação de ataques cibernéticos, dessa

[10] Tradução própria: "incorpora o uso de ferramentas e mentalidades diplomáticas para resolver questões decorrentes do uso internacional do ciberespaço".

maneira, a ciberdiplomacia é uma importante ferramenta para intermediar e garantir a cooperação entre os atores do sistema internacional em relação ao uso do ciberespaço (Radanliev, 2023).

Nesse sentido, pode-se compreender que a ciberdiplomacia não apenas propõe um equilíbrio entre os direitos individuais no ciberespaço, mas também a segurança nacional, ao promover normas cibernéticas que visam a redução de riscos em ciber atividades (Radanliev, 2023). Aqui, o episódio do ataque cibernético à Estônia em 2007 pode ser retomado como um ponto de inflexão para o nascimento da ciberdiplomacia (Attatfa et al, 2020). De acordo com o *Cyber Threat Landscape Report* de 2023 do Centro Internacional de Computação das Nações Unidas (UNICC), esse tipo de ataque cibernético está entre os mais comuns de ocorrer contra agências governamentais, vindo atrás apenas de *phishing*[11], exploração de vulnerabilidade e *malwares* (UNICC, 2023).

A comunidade internacional tem adquirido um conhecimento mais amplo acerca das diversas ameaças no ciberespaço, principalmente no que se refere aos impactos do uso de mecanismos tecnológicos no contexto da segurança nacional. Em 2001, foi aberto para assinatura o primeiro tratado internacional sobre crimes cibernéticos, a Convenção do Conselho da Europa sobre Cibercriminalidade ou Convenção de Budapeste. Embora tenha sido uma iniciativa europeia, a Convenção foi aberta para assinaturas de países de fora do continente europeu. O esforço coletivo dos países e especialistas na área inspirou leis e políticas de cibersegurança em muitos países, sendo os objetivos centrais do tratado:

> I- harmonizar as leis nacionais relacionadas aos crimes cibernéticos; II- apoiar a investigação desses crimes; e III- aumentar a cooperação internacional na luta contra os crimes cibernéticos. Entre outras coisas, o tratado obriga os países participantes a adotar legislação que proíba os crimes cibernéticos especificados. (Araújo, 2022, p. 159).

Os debates que resultaram na Convenção de Budapeste existem desde a década de 1990, impulsionados pela expansão da internet e pelo surgimento de novas tecnologias. Esse novo cenário fomentou discussões acerca da governança global da internet, que une conhecimentos científicos e técnicos com força política e diplomática para enfrentar desafios digitais (Calderaro; Marzouki, 2022). Um marco importante sobre essa discussão foi a criação da *Internet Corporation for Assigned Names and Numbers* (ICANN), em 1998. Trata-se de uma parceria sem fins lucrativos sediada no estado da Califórnia nos EUA, que permite a participação de diferentes atores para promover uma política de utilização dos identificadores únicos da internet (ICANN, 2024).

A principal finalidade da ICANN era supervisionar de forma neutra e global os diferentes aspectos técnicos da internet, como o sistema de nomes de domínio (DNS) e os endereços IP. No entanto, essas informações eram administradas pelo *US Department of Commerce*, gerando debates sobre a legitimidade da instituição de governança da internet (Carr, 2023). Diferentes países começaram a questionar se a

[11] Phishing é uma técnica de ataque cibernético projetada para enganar as pessoas e levá-las a fornecer informações sensíveis, como senhas, dados bancários, números de cartão de crédito ou informações pessoais.

ICANN realmente representava os interesses globais, uma vez que permanecia sob forte influência dos EUA, sendo a instituição acusada de não ter a transparência devida para uma instituição global regulatória (Carr, 2023). Desde 2016, a supervisão da ICANN foi oficialmente transferida para a comunidade global, tornando a organização independente, após a implementação de medidas de transparência e de legitimidade entre os stakeholders envolvidos (Carr, 2023).

Esse debate introduz a ideia de soberania digital, que, segundo Kaloudis (2024, p. 10), é "*the ability of a state or region to control and manage digital infrastructure, data and communication with a relevant degree of autonomy*"[12]. Esse conceito é fundamental para garantir ao Estado o direito de autodeterminação e controle sobre suas redes de dados e políticas cibernéticas (Kaloudis, 2024). Essa autonomia garante decisões independentes e estratégicas por parte dos Estados, contudo, esse cenário mostra a importância da regulação do ciberespaço para manutenção de um mundo interconectado, sendo esse um dos preceitos da ciberdiplomacia. Nesse contexto, a Cúpula Mundial sobre a Sociedade da Informação (WSIS) exemplifica como a ciberdiplomacia foi usada para promover discussões mais inclusivas e equilibradas sobre a internet.

A WSIS foi realizada em duas partes, sendo a primeira em Genebra, em 2003, e a segunda em Túnis, em 2005. Durante esses dois anos, as cúpulas foram precedidas por comitês preparatórios, grupos temáticos e conferências para preparação de cada fase. A primeira fase visava desenvolver e promover de forma clara uma declaração que estabelecesse medidas para uma sociedade de informação igualitária baseada nos interesses de cada envolvido (WSIS, 2015). A segunda fase, por sua vez, tinha como objetivo aplicar os planos da declaração construída em Genebra, chegando a acordos sobre a governança da internet e sobre os mecanismos de financiamento nessa área (WSIS, 2015). Dessa forma, pode-se concluir que a WSIS, no geral, buscava construir um entendimento comum sobre a sociedade de informação e os diferentes impactos que o mundo digital exerce sobre o sistema internacional.

A WSIS representa um exemplo de diplomacia multilateral, na qual diferentes entidades utilizam meios de debate para estabelecer medidas consensuais e resolver conflitos. O principal resultado dos debates no WSIS foi a criação do Fórum de Governança da Internet (IGF), estabelecido como parte da Agenda de Túnis em 2005 (IGF, 2024a). Este fórum tem como principal objetivo reunir diferentes atores de setores públicos e privados para formular políticas sobre o mundo digital, desde segurança cibernética até a governança da internet (IGF, 2024b). Esse modelo inovador de discutir políticas públicas em uma organização internacional caracteriza uma nova forma de aplicação da diplomacia nas relações internacionais. Através do envolvimento de diferentes atores nesse processo, o IGF é apenas um dos exemplos do que seria uma organização multistakeholder. No entanto, para entender esse novo modelo, é necessário entender como ele é visto, estudado e aplicado no sistema internacional.

3.2 Multistakeholder diplomacy: um paradigma de ciberdefesa?

[12] Tradução própria: "a capacidade de um Estado ou região de controlar e gerenciar a infraestrutura digital, os dados e a comunicação com um grau relevante de autonomia".

O sistema internacional contemporâneo demanda que a diplomacia adote maneiras de cooperação mais amplas e diversificadas. Seu desenvolvimento já não se limita a questões clássicas de guerra, mas envolve uma rede complexa de novos paradigmas para entender os regimes interconectados que ela abrange. Nesse contexto, a Multistakeholder Diplomacy emerge como um conceito essencial e uma ferramenta estratégica para moldar um novo modelo de atuação diplomática. De acordo com a Denardis e Raymond (2015, p. 273), uma governança multistakeholder é definida como *"two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules"*[13]. Essa definição destaca os participantes da tomada de decisão como os atores principais no processo. Entretanto, o conceito de multistakeholder difere do de multilateralismo, descrito por Ruggie (1992, p. 517) como:

> *[...] an institutional form which coordinates relations among three or more states on the basis of "generalized" principles of conduct-that is, principles which specify appropriate conduct for a class of actions, without regard to the particularistic interests of the parties or the strategic exigencies that may exist in any specific occurrence*.[14]

Embora apresentem definições semelhantes, os sistemas cada vez mais complexos exigem a interação de diferentes atores para promover uma diplomacia mais ampla e participativa. A diplomacia multistakeholder propõe essa dinâmica, diferenciando-se da diplomacia tradicional por estruturar mecanismos que promovem a participação, ação e responsabilização de atores não governamentais em nível transnacional (Johnstone et al, 2023). Os diferentes acordos, autoridades internacionais e interesses dos atores exigem uma maior conectividade para regular e mediar ideias e conflitos. Um dos exemplos do uso da multistakeholder é a regulação do ciberespaço, que vai além da atuação dos Estados e abrange os interesses e controle dos setores privados, responsáveis também pela gestão de infraestruturas tecnológicas críticas.

O *Paris Call for Trust and Security in Cyberspace*, lançado em 2018, exemplifica bem o debate sobre a regulação do ciberespaço, sendo a primeira iniciativa internacional a utilizar uma abordagem multistakeholder, envolvendo tanto Estados, empresas privadas e sociedade civil (França, 2024a). A *Call* propõe 9 princípios que orientam as discussões entre esses diversos atores, focando na proteção da internet e suas infraestruturas, na promoção de normas internacionais e na garantia da "*cyber hygiene*" (França, 2024b). Apesar de ser uma iniciativa do governo francês, o projeto contou com a coordenação de empresas privadas, principalmente com a Microsoft. Conforme Gorwa e Peez (2020, p. 273), a empresa *"assumed the role as a key spokesperson for tech firms in the cybernorms debate, thereby creating part of the*

---

[13] Traduação própria: "duas ou mais classes de atores envolvidos em um empreendimento de governança comum sobre questões que consideram de natureza pública, caracterizado por relações de autoridade poliárquicas constituídas por regras procedimentais".

[14] Tradução própria: "uma forma institucional que coordena as relações entre três ou mais estados com base em princípios "generalizados" de conduta — isto é, princípios que especificam a conduta apropriada para uma classe de ações, sem levar em conta os interesses particularistas das partes ou as exigências estratégicas que possam existir em qualquer ocorrência específica."

present-day cyber-norms environment"[15], desempenhando um papel central no debate sobre normas cibernéticas.

A interação entre diferentes atores e seus interesses resulta no que Wolff (2023) identifica como uma dificuldade em determinar exatamente quem liderou o *Paris Call*. Inicialmente desenvolvido entre a Microsoft e o governo francês, o projeto passou a ser liderado mais diretamente pela França após seu lançamento. O *Paris Call* representa um modelo híbrido entre o setor privado e governamental, no entanto, existem outras organizações que utilizam o modelo multistakeholder para deliberação e tomada de decisão. A ONU, por exemplo, possui várias iniciativas neste contexto, como o *Group of Governmental Experts* (GGE), que foi um dos primeiros grupos de debate multistakeholder da ONU, apesar de inicialmente membros não governamentais não participarem das deliberações (Ciglic; Hering, 2021). O tema principal debatido pelo GGE foi '*Developments in the field of information and telecommunications in the context of international security*'[16], destacando a importância do direito internacional como base para a regulamentação da internet e do ciberespaço (Ciglic; Hering, 2021).

O GGE realizou, ao todo, 6 edições, todas focadas em debater o impacto das novas tecnologias no sistema internacional, com destaque para os eventos como os ataques na Estônia e o Stuxnet, já mencionados anteriormente neste texto. Entretanto, por se tratar de um dos primeiros projetos sobre o tema, ao longo das edições houveram divergências significativas de interesses, medidas e propostas debatidas entre os atores envolvidos, com alguns membros considerando-as muito invasivas e outros muito elusivas (Wolff, 2023). A experiência da GGE foi importante para construção e consolidação de um debate multistakeholder. Como evolução desse processo, em 2018 foi estabelecido o *Open-Ended Working Group* (OEWG) das Nações Unidas, que ampliou a participação para além dos Estados membros da organização, incluindo também outros atores do sistema internacional, como ONGs e o setor privado (Wolff, 2023).

A Rússia foi o país que gerou o impulso inicial para o estabelecimento da OEWG devido a sua crítica do GGE ser muito limitado a alguns países membros, se referindo principalmente aos Estados Unidos (Wolff, 2023). De acordo com Wolff (2023) essa dificuldade de alcançar consenso entre as partes é um dos principais desafios de um fórum de discussão multistakeholder. O debate entre Estados em organizações para implementação de acordos já apresenta desafios consideráveis, devido às diferenças nos interesses, parcerias e estruturas de governo de cada participante, sendo esta ideia corroborada por Johnstone et al (2023, p. 12):

> [...] *The challenge for regime-building in this area, therefore, is to accommodate not only the differing authority, legitimacy, power, interests, capacity and expertise (the "stakes") of the many actors but also differing governmental attitudes on whether and how each actor should be involved at all*.[17]

[15] Tradução própria: "assumiu o papel de porta-voz principal para as empresas de tecnologia no debate sobre as cibernormas, criando assim parte do ambiente atual de cibernormas".

[16] Tradução própria: "Desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional".

[17] Tradução própria: "O desafio para a construção de regimes nesta área, portanto, é acomodar não apenas a autoridade, legitimidade, poder, interesses, capacidade e expertise (os "interesses") dos diversos atores, mas também as diferentes atitudes governamentais sobre se e como cada ator deve estar envolvido, ou não."

No entanto, quando a discussão expande para diferentes atores, cada um constituído por suas próprias diretrizes e ideais, a consolidação de um debate rico em resoluções se torna um ponto de observação e análise. Conforme argumentado por Trachtman (2023), a diplomacia multistakeholder não substitui a responsabilização de meios de debates tradicionais, como parlamentos, por exemplo, mas é uma forma de potencializar o poder de decisão através do envolvimento de outros atores. Dessa forma, a participação do setor privado, de organizações não-governamentais (ONGs) e da sociedade civil é essencial para tornar os acordos mais eficazes, enriquecendo o debate por meio de suas contribuições e consultoria. Entretanto, é importante reconhecer que empresas representam seus próprios interesses, enquanto ONGs, por exemplo, focam em objetivos sociais específicos (Trachtman, 2023). Por isso, antes de aplicar uma diplomacia multistakeholder, é necessário avaliar os diferentes níveis de poder, legitimidade e autoridade dos atores envolvidos, garantindo um equilíbrio e resguardos diplomáticos.

Um exemplo de plataforma de diálogo multistakeholder que demonstra a inclusão de diferentes perspectivas é o Marco Civil da Internet (MCI), sancionado em 2014 no Brasil por meio da Lei 12.965/14. Essa legislação foi criada para regulamentar os direitos ao uso da internet, estabelecendo o direito à cidadania, diversidade e liberdade de expressão na internet (Brasil, 2024a). O MCI complementa outra legislação brasileira, a Lei Geral de Proteção de Dados (lei 13.709/2018), que também tem como objetivo proteger os direitos de liberdades e privacidades dos indivíduos, inclusive nos meios digitais (Brasil, 2024b). No entanto, o que difere o MCI de outras iniciativas, é o seu caráter multistakeholder, sendo desenvolvido não apenas pelo poder legislativo e executivo brasileiro, mas também com a participação da sociedade civil, acadêmicos e o setor privado. Esse processo colaborativo levou o MCI a ser conhecido como "*The Brazilian Internet Bill of Rights*" (Souza; Perrone, 2024, p. 234).

A participação dos diversos atores no processo ocorreu por meio de uma consulta pública realizada em uma plataforma online, dividida em duas etapas. Na primeira fase houve a colaboração para identificar os temas mais relevantes que seriam posteriormente redigidos pelo Ministério de Justiça (Souza; Lemos, 2016). Na segunda fase, a redação proposta foi publicada na plataforma para que o público pudesse expressar suas opiniões finais e propor ajustes (Souza; Lemos, 2016). Segundo Souza e Lemos (2016, p. 21), essa nova abordagem do processo legislativo do país foi inédita e interessante, pois:

> [...] as opiniões, críticas e sugestões de alterações no texto da futura lei não estavam mais reservadas a notas técnicas distribuídas em gabinetes, mas sim transformadas em contribuições concretas que poderiam ser revistas e comentadas por todos os interessados, como em um típico fórum de discussão na Internet.

Dessa forma, é possível analisar como seria o impacto positivo que uma diplomacia multistakeholder pode ter na construção de medidas e regulamentos burocráticos. Essa abordagem não apenas pode ser aplicada no sistema internacional, como em fóruns, organizações e convenções, mas também pode ser utilizada domesticamente, e, espaços como parlamentos e congressos nacionais. A capacidade

de adaptação da diplomacia multistakeholder é um dos seus fatores diferenciais. Contudo, é essencial regulamentar os processos para facilitar o debate e definir os diferentes tipos de interação entre os atores envolvidos. Através dessa nova ferramenta, é possível encontrar soluções mais eficazes e inclusivas de regulação de cenários diversos, como o ambiente cibernético, garantindo a segurança e a paz no contexto das relações internacionais.

4 CONSIDERAÇÕES FINAIS

O avanço das tecnologias digitais e o aumento das ameaças cibernéticas têm transformado profundamente as dinâmicas do sistema internacional, exigindo novas abordagens para sua compreensão e gestão. Neste contexto, o conceito de cibersegurança e a prática da ciberdiplomacia surgem como fatores centrais para enfrentar desafios que vão desde a guerra cibernética até a regulação da inteligência artificial e a governança da internet. Este artigo destacou a evolução histórica do conceito de segurança, demonstrando como ele foi ampliado para abranger o ciberespaço e analisando as implicações dessa transformação para as relações internacionais.

A ciberdiplomacia, como argumentado, é uma ferramenta essencial para mediar os impactos das tecnologias digitais na interação entre Estados e outros atores no sistema internacional. Contudo, sua eficácia depende de uma abordagem inclusiva e colaborativa, como a proporcionada pela diplomacia multistakeholder. Ao incorporar diversos atores, como empresas, organizações internacionais, academia e sociedade civil, nos debates e nas tomadas de decisão, a diplomacia multistakeholder fortalece a governança transnacional e promove soluções mais abrangentes e sustentáveis para os desafios do ciberespaço.

As iniciativas discutidas, como o *Paris Call for Trust and Security in Cyberspace* e os projetos da ONU, evidenciam a importância de mecanismos globais que facilitem o diálogo e a cooperação entre diferentes atores. Esses esforços não apenas contribuem para mitigar as ameaças cibernéticas, mas também estabelecem um modelo de governança adaptado à complexidade e interconexão do mundo digital. No entanto, é evidente a importância de considerar os diferentes níveis de poder, legitimidade e autoridade dos atores participantes de um fórum multistakeholder para que o processo seja mais inclusivo e transparente, atendendo as necessidades estabelecidas previamente para o debate.

Portanto, a análise apresentada reforça que a integração entre ciberdiplomacia e diplomacia multistakeholder é não apenas desejável, mas indispensável para a construção de um ciberespaço mais seguro e inclusivo. Os espaços digitais serão cada vez mais robustos e complexos, sendo dessa forma importante a compreensão dos possíveis impactos nesse cenário e o estabelecimento de processos de regulamentação e de tomada de decisões a partir desses diferentes mecanismos. Ao explorar essas interseções e propor direções para futuras investigações, o artigo oferece uma base teórica e prática para repensar a segurança internacional e as estratégias diplomáticas neste novo contexto do mundo cibernético.

REFERÊNCIAS

ARAÚJO, Clayton. **Os aspectos gerais dos tratados internacionais e a Convenção de Budapeste sobre Crimes Cibernéticos**. Revista da Faculdade de Direito da Universidade Federal de Uberlândia, v. 50, p. 145-165, 2022. DOI: https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165.

ATTATFA, Amel; DE PAOLI, Stefano; RENAUD, Karen. **Cyber Diplomacy:** A Systematic Literature Review. Procedia Computer Science, v. 176, p. 60-69, 2020.

BAUMAN, Zygmunt et al. **After Snowden:** Rethinking the Impact of Surveillance. International Political Sociology, 2014. DOI: 10.1111/ips.12048

BRASIL. Lei Geral de Proteção de Dados Pessoais: Lei n° 13.709/2018. **Senado Federal**, Brasília. Disponível em: <https://www2.senado.leg.br/bdsf/handle/id/658231#:~:text=pessoais%20%3A%20Lei%20n.-,13.709%2F2018,da%20personalidade%20da%20pessoa%20natural>. Acesso em: 01 dez. 2024b.

BRASIL. Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA. **Senado Noticias**, 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia>. Acesso em: 01 dez. 2024a.

BRKAN, Maja. **Artificial Intelligence and Democracy**: The Impact of Disinformation, Social Bots and Political Targeting. Delphi - Interdisciplinary Review of Emerging Technologies, v. 2, Issue 2, 2019, p. 66-71. DOI https://doi.org/10.21552/delphi/2019/2/4.

BULL, Hedley. **A sociedade anárquica:** um estudo da ordem na política mundial. São Paulo: Editora Universidade de Brasília, 2002.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap. **Security**: A New Framework for Analysis. London: Lynne Rienner Publishers, 1998.

CALDERARO, Andrea; MARZOUKI, Meryem. **Introduction: Global Internet Governance**: an Uncharted Diplomacy Terrain?. Internet Diplomacy: Shaping the Global Politics of Cyberspace, Rowman & Littlefield, 2022.

CARR, Madeline. Global Internet Governance. In: WEISS, Thomas; WILKINSON, Rorden. **International Organization and Global Governance**. Nova Iorque: Routledge, ed. 3, p. 776-786, 2023.

CIGLIC Kaja; HERING, John. **A multi-stakeholder foundation for peace in cyberspace**. Journal of Cyber Policy, 2021, p. 360-374. DOI: 10.1080/23738871.2021.2023603.

CLARKE, Richard; KNAKE, Robert. **Cyber War**: The Next Threat to National Security and What to Do About it. New York: HarperCollins, 2010.

DENARDIS, Laura; RAYMOND, Mark. **Multistakeholderism:** Anatomy of an Inchoate Global Institution. International Theory 7, 2015, n. 3, p. 572–616. https://doi.org/10.1017/S1752971915000081.

DUQUE, Marina Guedes. **O papel de síntese da escola de Copenhague nos estudos de segurança internacional**. Rio de Janeiro: Contexto Internacional, v. 31, n° 3, 2009. Disponível em: <https://www.scielo.br/j/cint/a/ftcHwZvqyMrrb3ZFRxbwVpF/>. Acesso em: 10 set. 2024.

EUROPEAN COMMISSION. Estonia leads the way with advanced e-services for citizens, 2016. Disponível em:<https://ec.europa.eu/regional_policy/en/projects/estonia/estonia-leads-the-way-with-advanced-e-services-for-citizens>. Acesso em: 5 out 2024.

FRANCE. Paris Call for Trust and Security in Cyberspace. **Ministère de l'Europe et des Affaires étrangères**, 2024. Disponível em: <https://www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace>. Acesso em: 23 nov. 2024a.

GIESEN, Klaus-Gerd. **Justice in Cyberwar**. Florianópolis: Ethic@, v.13, n.1, 2014. DOI: https://doi.org/10.5007/1677-2954.2014v13n1p27.

GORWA Robert; PEEZ, Anton. Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord. *In*: BROEDERS, Dennis; VAN DEN BERG, Bibi (ed.). **Governing Cyberspace:** Behavior, Power and Diplomacy. Maryland: Rowman & Littlefield International, 2020, p. 263-284. Disponível em: <https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf>. Acesso em: 23 nov 2024.

HERZ, John. **Idealist Internationalism and the Security Dilemma**. Maryland: World Politics, v. 2 , i. 2, p.157-180, 1950.

HOBBES, Thomas. **Leviatã**. São Paulo: Marlins Fontes, 2003.

ICANN. What Does ICANN Do?. **ICANN**. Disponível em: <https://www.icann.org/resources/pages/what-2012-02-25-en>. Acesso em: 30 out 2024.

INTERNATIONAL TELECOMUNICATION UNION. About WSIS Basic Information. **ITU**. Disponível em: <https://www.itu.int/net/wsis/basic/about.html>. Acesso em: 4 nov 2024.

INTERNET GOVERNANCE FORUM. The IGF and UN Processes. **IGF**. Disponível em: <https://www.intgovforum.org/en/content/the-igf-and-un-processes>. Acesso em: 9 nov 2024a.

INTERNET GOVERNANCE FORUM. About the IGF. **IGF**. Disponível em: <https://www.intgovforum.org/en/about>. Acesso em: 9 nov 2024b.

JOHNSTONE, Ian; SUKUMAR, Arun; TRACHTMAN, Joel. Building cybersecurity through
multistakeholder diplomacy: Politics, processes, and prospects. In: _____. (org.). **Building an International Cybersecurity Regime:** Multistakeholder Diplomacy. Elgar International Law and Technology, 2023, p. 2-18. DOI https://doi.org/10.4337/9781035301546.

KALOUDIS, Martin. Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in Democracies. In: BURT, Sally. **National Security in the Digital and Information Age**. Intech Open, 2024. DOI 10.5772/intechopen.1005415

KANT, Immanuel. **A paz perpétua**. Um projeto filosófico. Covilhã: LusoSofia, 2008.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. **Marco Civil da Internet:** Construção e Aplicação. Editar Editora Associada, 2016.

LINDSAY, Jon R. **Stuxnet and the Limits of Cyber Warfare**. Security Studies, 2013. DOI: 10.1080/09636412.2013.816122.

MAQUIAVEL, Nicolau. **O Príncipe**. São Paulo: Madras Editora, 2009.

MEARSHEIMER, John. **The Tragedy of Great Power Politics**. New York: W. W. Norton & Company, 2001.

NATO Cooperative Cyber Defence Centre of Excellence. About Us. **CCDCOE**. Disponível em: <https://ccdcoe.org/about-us/>. Acesso em: 5 out. 2024.

PARIS Call. The 9 principles. **Paris Call**, 2024. Disponível em: <https://pariscall.international/en/principles>. Acesso em: 23 nov. 2024b.

PAYNE, Kenneth. **Artificial Intelligence:** A Revolution in Strategic Affairs?. Survival, 2018. DOI: 10.1080/00396338.2018.1518374.

PERRONE, Christian; SOUZA, Carlos Affonso. Brazil and multistakeholder diplomacy for the Internet: Past achievements, current challenges and the road ahead. *In:* JOHNSTONE, Ian; SUKUMAR, Arun; TRACHTMAN, Joel (org.). **Building an International Cybersecurity Regime:** Multistakeholder Diplomacy. Elgar International Law and Technology, 2023. p. 220-237. DOI https://doi.org/10.4337/9781035301546.

RADANLIEV, Petar. **Cyber diplomacy:** defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 2024. DOI: 10.1080/23742917.2024.2312671.

RUGGIE, John. **Multilateralism:** the Anatomy of an Institution. International Organization, v. 46, n. 3, 1992, p. 561-598. Disponível em: <https://www.jstor.org/stable/2706989>.

TRACHTMAN, Joel. Developing multistakeholder structures for cybersecurity norms: Learning from experience. *In:* JOHNSTONE, Ian; SUKUMAR, Arun; TRACHTMAN, Joel (org.). **Building an International Cybersecurity Regime:** Multistakeholder Diplomacy. Elgar International Law and Technology, 2023. p. 85-110. DOI https://doi.org/10.4337/9781035301546.

UNITED NATIONS INTERNATIONAL COMPUTING CENTRE. 2023 Cyber Threat Landscape Report. **UNICC**. Disponível em: <https://www.unicc.org/wp-content/uploads/2024/07/2023-Cyber-Threat-Landscape-Report-1.pdf> . Acesso em: 21 set. 2024.

WALTZ, Kenneth. **Theory of International Politics**. California: Addison-Wesley Publishing Company, 1979.

WOLFF, Josephine. Multistakeholder characteristics of past and ongoing cybersecurity norms processes. *In:* JOHNSTONE, Ian; SUKUMAR, Arun; TRACHTMAN, Joel (org.). **Building an International Cybersecurity Regime:** Multistakeholder Diplomacy. Elgar International Law and Technology, 2023. p. 59-84. DOI https://doi.org/10.4337/9781035301546.