OPEN ACCESS

ESCOLA DE HUMANIDADES
PUCRS

CONVERSAS & CONTROVÉRSIAS

Conversas & Controvérsias, Porto Alegre, v. 12, n. 1, p. 1-12, jan.-dez. 2025
e-ISSN: 2178-5694

http://dx.doi.org/10.15448/2178-5694.2025.1.48195

ARTIGOS LIVRES

Ciberdiplomacia e *Multistakeholder Diplomacy*: perspectivas de um novo paradigma

Cyberdiplomacy and Multistakeholder Diplomacy: Perspectives on a New Paradigm
Cyberdiplomacy y Multistakeholder Diplomacy: Perspectivas de un Nuevo Paradigma

Lauren Giordani Gröhs[1]
orcid.org/0009-0006-1123-323
lauren.grohs2610@gmail.com

Fabricio Pontin[1]
orcid.org/0000-0002-3984-1849
fabricio.pontin@unilasalle.edu.br

Recebido em: 9 jun. 2025.
Aprovado em: 28 jul. 2025.
Publicado em: 09 out. 2025.

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 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 a 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 vários atores envolvidos é destacada como risco relevante para a estabilidade e a cooperação no sistema internacional.

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

Abstract: The growing advancement and plurality of the cyber world have increased the complexity of interactions within the international system, highlighting the need for regulation and mediation in the field of cybersecurity. This study explores how multistakeholder diplomacy can be applied to cyberdiplomacy to facilitate debates and conflict resolution in cyberspace. The research analyzes different perspectives on cybersecurity, with emphasis on forums such as the Paris Call for Trust and Security in Cyberspace, which use cyberdiplomacy as a central instrument for global discussions. The findings present multistakeholder diplomacy as an innovative and effective tool for promoting inclusive governance in cyberspace, although significant challenges to its implementation are identified. The lack of adequate regulation regarding the use of emerging technologies among the various actors involved is highlighted as a relevant risk to stability and cooperation within the international system.

Keywords: Cyberdiplomacy; Cybersecurity; Multistakeholder; International System.

Resumen: El creciente avance y la pluralidad del mundo cibernético han ampliado la complejidad de las interacciones en el sistema internacional, evidenciando la necesidad de regulación y mediación en el ámbito de la ciberseguridad. Este estudio explora cómo la diplomacia *multistakeholder* puede aplicarse a la ciberdiplomacia para facilitar los debates y la resolución de conflictos en el ciberespacio. La investigación analiza diferentes perspectivas sobre la ciberseguridad, con énfasis en foros como el *Paris Call for Trust and Security in Cyberspace*, que utilizan la ciberdiplomacia como instrumento central para las discusiones globales. Los resultados muestran que la diplomacia *multistakeholder* es una herramienta innovadora y eficaz para promover una gobernanza inclusiva en el ciberespacio, aunque se identifican desafíos significativos para su implementación. La ausencia de una regulación adecuada sobre el uso de tecnologías emergentes entre los

[1] Universidade LaSalle, Canoas, Rio Grande do Sul, Brasil.

diversos actores involucrados se destaca como un riesgo relevante para la estabilidad y la cooperación en el sistema internacional.

Palabras clave: ciberdiplomacia; ciberseguridad; *multistakeholder*; sistema internacional.

1 Introdução

A discussão sobre tecnologias e ameaças cibernéticas nas políticas internacionais ressalta a necessidade de medidas de proteção. Novas abordagens diplomáticas, como a ciberdiplomacia, são essenciais para essa adaptação. A ciberdiplomacia se beneficia da diplomacia *multistakeholder*, que responsabiliza atores internacionais pela governança transnacional. Essa ferramenta permite decisões e soluções com múltiplos atores, visando reduzir ameaças cibernéticas. Para integrar essa metodologia, é crucial entender o desenvolvimento da segurança cibernética e as implicações de uma gestão diplomática eficiente no ciberespaço.

Este artigo explora essas interseções. Primeiro, analisaremos a evolução do conceito de *segurança internacional* para incluir ameaças cibernéticas, como guerras cibernéticas, IA e vigilância, que exigem uma abordagem multilateral. Em seguida, discutiremos a ciberdiplomacia como instrumento para mediar o impacto das tecnologias digitais na política externa e na interação entre Estados. O texto também explora exemplos de debates sobre o ciberespaço em fóruns internacionais, como o *Internet Corporation for Assigned Names and Numbers* (ICANN) e a Cúpula Mundial sobre a Sociedade da Informação (WSIS), que destacam a importância da inclusão de diferentes atores na regulamentação. O segundo tópico aprofunda a diplomacia *multistakeholder*, que amplia a tomada de decisão para incluir Estados, empresas, organizações, academia e sociedade civil. Abordaremos plataformas como o *Paris Call for Trust and Security in Cyberspace* e iniciativas da ONU, como o *Open-Ended Working Group* (OEWG), que exemplificam o esforço coletivo para regulamentar a governança da internet, consolidando o ciberespaço como campo diplomático.

2 Cibersegurança: definições e impactos na segurança internacional

O conceito de segurança internacional evoluiu, ramificando-se em diversas teorias, e remonta às primeiras entidades políticas. Maquiavel (2009), em *O Príncipe*, defende que a manutenção do poder estatal exige força, astúcia e pragmatismo, priorizando a sobrevivência do Estado. Hobbes (2003) argumenta que a segurança é o objetivo principal da política, uma necessidade primária do estado de natureza. A criação do contrato social, para Hobbes, é a solução, transferindo o monopólio da violência a um soberano que garante ordem e segurança. A ênfase hobbesiana na centralização do poder ressoa com o pensamento realista de Waltz (1979), que vê o sistema internacional como anárquico, marcado pela luta dos Estados por sobrevivência.

Enquanto Maquiavel e Hobbes baseiam a segurança no poder estatal, Kant (2008) propõe uma federação de repúblicas democráticas regida pelo direito internacional para alcançar a segurança internacional. Para Kant, a paz é uma obrigação moral e um imperativo racional, exigindo cooperação e instituições internacionais. Essa visão liberal contrasta com a realidade do sistema internacional, que opera sob dinâmicas de poder. O contraste entre Kant e realistas como Mearsheimer (2001) e Waltz (1979) mostra a tensão entre cooperação e anarquia. Waltz (1979) afirma que, num sistema anárquico, os Estados competem pela segurança, sem autoridade superior para garantir a paz. O dilema da segurança, de Herz (1950), explica como o fortalecimento militar de um Estado gera insegurança nos outros, perpetuando a competição. Mearsheimer (2001) sugere que os Estados agem agressivamente devido à estrutura do sistema internacional.

Nessa perspectiva, a segurança é inerente a um sistema internacional anárquico, em que cada Estado é responsável por sua segurança, buscando o equilíbrio de poder. Para Waltz (1979), essa lógica reflete o realismo da anarquia internacional, no qual Estados competem pela sobrevivência e segurança pela ausência de autoridade superior. O autor destaca:

> *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, 163).

A busca por segurança está ligada à busca por hegemonia, dependendo do reconhecimento de poder por outros Estados. Mearsheimer (2001, 30) considera o conflito 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]. As visões de Waltz (1979) e Mearsheimer (2001) tendem a desconsiderar o papel das instituições e normas internacionais na cooperação.

No entanto, Buzan et al. (1998) propõem a securitização como mecanismo de promoção da segurança internacional via diálogo entre atores. Após a Guerra Fria, o *Centre for Peace and Conflict Research*, agora Escola de Copenhague, adotou uma abordagem construtivista para a segurança (Duque 2009). Essa perspectiva considera novos fatores (militar, político, econômico, social e ambiental), ampliando a discussão da segurança para além do objetivo, incorporando percepções e discursos. A teoria da securitização entende a segurança não como um dado objetivo, mas como um processo discursivo de construção social de ameaças. Ao contrário da ênfase realista na força material, a Escola de Copenhague considera a segurança em múltiplas dimensões, destacando a percepção e retórica na definição de ameaças, o que permite uma leitura mais flexível da segurança internacional, incluindo fatores negligenciados pelos paradigmas clássicos.

A integração da visão de Kant à securitização de Buzan et al. (1998) rompe com a segurança centrada no Estado. O modelo kantiano de federação ressurge em organizações e regimes multilaterais que buscam mitigar riscos da anarquia via cooperação e normatização. A Escola de Copenhague enfatiza que a segurança não depende só de estruturas, mas de como os atores discursam e legitimam ações em nome da segurança. Isso é visível na guerra cibernética, em que a securitização de ameaças digitais é central na política internacional.

Segundo Buzan et al. (1998), a securitização é um "ato de fala", em que um ator internacional declara publicamente sua ameaça, iniciando um processo discursivo para resoluções. A segurança é dinâmica, e novas ameaças como a guerra cibernética e suas implicações para a segurança nacional foram identificadas. Clarke e Knake (2010) foram pioneiros na defesa contra ataques cibernéticos, ressaltando a vulnerabilidade de infraestruturas e a busca por normas internacionais.

Para Clarke e Knake (2010), a guerra cibernética é real e um desafio crescente. O ataque à Estônia em 2007 expôs vulnerabilidades digitais e a necessidade de abordagens para a segurança internacional. Enquanto o realismo sugeriria que Estados desenvolvam capacidades ofensivas/defensivas para soberania cibernética, Buzan et al. (1998) veem a segurança cibernética como um fenômeno discursivo, no qual atores definem e constroem a ameaça digital.

A análise da segurança internacional contemporânea mostra que a relevância da guerra cibernética e novas ameaças globais exigem uma visão abrangente que considere estruturas materiais e aspectos simbólicos/discursivos que moldam a política internacional. Nesse contexto, Clarke e Knake (2010) propõem medidas para mitigar ameaças cibernéticas: desenvolvimento de normas internacionais, investimentos em tecnologias cibernéticas e em especialistas. Seus estudos e propostas impulsionaram a reflexão sobre o impacto das novas tecnologias no sistema internacional, especialmente no campo ainda pouco explorado do ciberespaço.

---

[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".

2.1 Impacto de novas tecnologias nas relações internacionais

Inovações tecnológicas como IA, guerras cibernéticas, tecnologias de informação, comunicação e vigilância transformam a dinâmica de poder, as ameaças de segurança internacional e a interação estatal. O desenvolvimento digital expôs vulnerabilidades de infraestruturas críticas de Estados e empresas (redes elétricas, sistemas financeiros, comunicações). O ataque cibernético à Estônia em 2007 é o marco inicial da cibersegurança global, conhecido como *Web War One (WW1)* (Clarke e Knake 2010).

Em 2007, o governo estoniano realocou o "Soldado de Bronze", monumento soviético da Segunda Guerra Mundial, da capital Tallinn para um cemitério militar. A decisão, motivada pelo fato de o monumento representar a ocupação soviética, período traumático de repressão, gerou protestos da população russa na Estônia e do governo russo, para quem o monumento era uma homenagem aos soldados soviéticos. Em 27 de abril de 2007, a *Bronze Night* marcou a mudança do campo de batalha para o ciberespaço. A Estônia sofreu um ataque DDoS[4] que sobrecarregou os servidores estonianos com uma quantidade massiva de solicitações, tornando os *sites* inacessíveis (Clarke e Knake 2010). Órgãos governamentais, bancos, mídia e empresas privadas ficaram sem acesso, interrompendo o sistema financeiro e a comunicação pública.

A Rússia negou envolvimento e recusou o pedido estoniano de ajuda para rastrear os hackers (Clarke e Knake 2010). Especulou-se o envolvimento de crime organizado, governo russo e grupos patrióticos[5], mas muitas perguntas persistem. O ataque estoniano revelou a insegurança internacional, evidenciando a vulnerabilidade de sistemas digitais estatais e a falta de preparo global. Foi catalisador para a criação do Centro de Excelência de Defesa Cooperativa da OTAN (CCDCOE). O CCDCOE, fundado em 2008, é um órgão da OTAN de pesquisa e treinamento em defesa cibernética, fornecendo suporte e capacitação aos membros (CCDCOE 2024). Integrando a estrutura militar da OTAN, o CCDCOE é crucial na segurança cibernética dos aliados.

Simultaneamente, outro ataque cibernético ocorreu na Geórgia. Após o colapso da URSS em 1991, a Geórgia declarou independência, mas enfrentou conflitos étnicos e políticos, especialmente nas regiões separatistas da Abecásia e Ossétia. A natureza dos ataques georgianos indica o uso do domínio virtual como frente de conflito. A Geórgia sofreu ataques DDoS que bloquearam serviços de mídia, *sites* governamentais e sistemas bancários, dificultando a comunicação governamental ao público e à comunidade internacional (Clarke e Knake 2010). Um diferencial foi a existência de *sites* "anti-Geórgia" que ofereciam *software* para *hackers*. Clicar em *Start Flood* convidava voluntários à guerra cibernética (Clarke e Knake 2010). A Rússia alegou que os ataques eram de grupos nacionalistas, fora do controle do Kremlin, mas a estrutura das atividades sugere apoio tácito ou explícito do governo russo.

Clarke e Knake (2010, 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*"[6]. Assim, o computador pode ser uma arma, tornando a guerra cibernética uma forma de perpetuar conflitos entre Estados. Esse campo de batalha remete às regras mais firmes do estado de natureza[7], exigindo normas nacionais e internacionais para regular (Giesen 2014). A balança de poder cibernética favorece o atacante, levando governos a investir mais em ciberdefesa (Giesen 2014). A reconfiguração da internet e de *softwares* abrange ataques potenciais: espionagem, propaganda e intervenção. Além de conflitos estatais, há *non-state actors* (como grupos de

---

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 *on-line* ou rede, tornando-o indisponível para usuários legítimos.

5 Adota-se neste artigo o termo "grupos patrióticos", conforme a terminologia apresentada por Clarke e Knake (2010) em sua obra.

6 Tradução própria: "ações de um estado-nação para penetrar nos computadores ou redes de outra nação com o propósito de causar danos ou interrupções".

7 A literatura realista adota a metáfora hobbesiana na análise, tornando a condição "anárquica" entre estados espelhada no estado de natureza hobbesiano.

hackers patrióticos na Rússia ou na China) que, embora subordinados, operam de forma não governamental (Giesen 2014).

Em 2006, o Conselho de Segurança da ONU ordenou ao Irã a suspensão de seu programa de enriquecimento de urânio; o país recusou, mantendo atividades dentro do Tratado de Não Proliferação Nuclear (Lindsay 2013). O Stuxnet, suposto *malware*[8] desenvolvido por esses países como parte da operação *Olympic Games*, danificou mais de mil centrífugas na instalação nuclear de Natanz (Lindsay 2013).

O Stuxnet marcou a cibersegurança, gerando debates sobre a "Revolução Cibernética", que sugere ataques cibernéticos darem vantagem assimétrica a atores militares mais fracos, dificultando a defesa e aumentando a eficácia ofensiva (Lindsay 2013). Contudo, o caso Stuxnet mostra uma realidade diferente: em vez de facilitar ofensivas para atores mais fracos, operações cibernéticas bem-sucedidas exigem recursos e capacidade técnica significativa, favorecendo nações mais fortes e tornando a defesa mais viável. Embora a mídia o retratasse como prenúncio de uma nova era de guerra cibernética, a recuperação do programa nuclear iraniano em um ano sugere impacto temporário e não decisivo. O evento mostrou a complexidade da criação, execução e manutenção dessas operações e a viabilidade da defesa cibernética.

Além desses casos, a diplomacia *multistakeholder* tem sido fundamental para mitigar ameaças cibernéticas e fortalecer a segurança global. Organizações como o Grupo de Especialistas Governamentais da ONU (UNGGE) e o Diálogo Global sobre Segurança Cibernética reúnem atores estatais e privados para discutir normas sobre o uso de tecnologias digitais em conflitos internacionais. Nesse contexto, o UNGGE foi um dos primeiros fóruns a reunir representantes estatais e não governamentais para debater esses eventos (Ciglic e Hering 2021). O objetivo principal era estabelecer um consenso sobre a regulação do ciberespaço. Essa iniciativa representou uma das primeiras tentativas da ONU de adotar uma abordagem *multistakeholder*.

Questões de defesa também incluem vigilância e privacidade digital, cujas violações geram reações em defesa da privacidade e reforma na coleta de dados. O caso Snowden, em 2013, expôs uma operação de vigilância global dos Estados Unidos. O vazamento de documentos de Edward Snowden, ex-contratado da Agência de Segurança Nacional, revelou acesso a servidores de empresas como Microsoft e Google (Bauman et al. 2014), registros de chamadas e espionagem de líderes como Dilma Rousseff (Bauman et al. 2014). As revelações causaram tensões globais e iniciaram o debate sobre os limites da vigilância, mostrando a necessidade de regras de privacidade e segurança global.

O debate sobre Inteligência Artificial (IA) também traz questões de segurança crescentes para os Estados. Segundo Payne (2018, 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 é uma realidade e será útil tática e estrategicamente, transformando atividades militares, como logística, informações e vigilância (Payne 2018). Contudo, a IA também representa riscos estatais na tomada de decisões e no manejo de informações, tornando a ética da IA central.

O uso da IA na política estatal impacta a política interna, como nas eleições presidenciais dos Estados Unidos em 2016. Estudos mostram que *bots* e algoritmos de IA foram cruciais na propagação de *fake news*, influenciando eleitores. O uso de *social bots*[9] para espalhar informações falsas em redes sociais e algoritmos sofisticados para direcionar anúncios políticos baseados em dados eleitorais (Brkan 2019) exemplificam o impacto negativo da IA. Além disso, tecnologias como *deepfakes*[10] levantam preocupações sobre a integridade eleitoral, ao permitir a criação de

---

[8] *Malware* é um termo genérico que engloba diversos tipos de ameaças digitais.

[9] Programas automatizados que operam em plataformas de redes sociais, simulando o comportamento humano para realizar interações como postar, comentar, curtir ou compartilhar conteúdo.

[10] Vídeos falsos gerados por IA.

conteúdos enganosos que dificultam a distinção entre o real e o falso (Brkan 2019).

Esses casos de mecanismos tecnológicos mostram a importância de discutir o ciberespaço e definir suas regras. Isso exige colaboração entre os atores internacionais na criação de normas para resolver conflitos cibernéticos. Surge, assim, a necessidade de um novo enfoque diplomático: a ciberdiplomacia. Uma diplomacia específica nesse campo pode desenvolver e aplicar as ferramentas para regular o ciberespaço. É fundamental compreender as vertentes desse debate e seu estado atual.

3 Da ciberdiplomacia à *multistakeholder diplomacy*: construindo um paradigma de segurança

Para entender a ciberdiplomacia, é essencial compreender a diplomacia nas relações internacionais, ferramenta crucial para comunicação entre Estados e atores globais. Bull (2002, 196-198) aponta as funções diplomáticas:

> 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 diplomacia se aplica a temas emergentes para a manutenção do sistema internacional. Com o avanço da tecnologia da informação, especialmente da internet, surgiram novas interações e conflitos, exigindo uma abordagem específica: a ciberdiplomacia.

A ciberdiplomacia surge como resposta à interdependência digital dos Estados e à necessidade de mitigar riscos no ciberespaço. Segundo Attatfa et al. (2020, 61), a ciberdiplomacia "*incorporates the use of diplomatic tools and mindsets to resolve issues arising from the international use of cyberspace*"[11]. Ela adapta funções tradicionais da diplomacia (negociação, comunicação, resolução de conflitos) à realidade digital, estabelecendo protocolos e normas internacionais para o comportamento de Estados e outros atores no ciberespaço. Além da criação de normas, a ciberdiplomacia medeia crises cibernéticas e constrói confiança entre Estados, prevenindo escaladas de conflitos por ataques ou disputas de infraestrutura digital.

Além de regulamentação e mediação, a ciberdiplomacia fortalece a cooperação internacional em segurança digital. Radanliev (2024) destaca que ela promove capacitação tecnológica em cibersegurança, viabilizando intercâmbio de conhecimento, desenvolvimento de capacidades defensivas e criação de mecanismos de resposta conjunta a ameaças digitais. Um grande desafio da cibersegurança é a dificuldade de atribuir responsabilidade por ataques, o que gera tensões. A ciberdiplomacia constrói redes de cooperação, facilita a troca de informações sobre ameaças, define padrões de resposta e mitiga riscos sistêmicos. Ao integrar esforços multilaterais, é essencial para um ambiente digital mais seguro e estável. Um dos desafios atuais da cibersegurança é a identificação de ataques cibernéticos; dessa maneira, Radanliev (2024) também aponta que a ciberdiplomacia é ferramenta crucial para intermediar e garantir a cooperação entre atores no uso do ciberespaço.

A ciberdiplomacia busca equilibrar direitos individuais no ciberespaço com segurança nacional, promovendo normas que reduzam riscos em ciberatividades (Radanliev 2024). O ataque à Estônia em 2007 é visto como ponto de inflexão para seu surgimento (Attatfa et al. 2020). Segundo o *Cyber Threat Landscape Report* de 2023 do UNICC[12], esse tipo de ataque é dos mais frequentes contra agências governamentais, atrás apenas de *phishing*[13], exploração de vulnerabilidade e

---

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

[12] Centro Internacional de Computação das Nações Unidas.

[13] *Phishing* é uma técnica de ataque cibernético projetada para enganar as pessoas e levá-las a fornecer informações sensíveis, como

malwares (UNICC 2024).

A comunidade internacional vem ampliando seu conhecimento sobre ameaças cibernéticas, especialmente os impactos de tecnologias na segurança nacional. Em 2001, foi aberto o primeiro tratado internacional sobre crimes cibernéticos: a Convenção de Budapeste. De iniciativa europeia, foi aberta a países não europeus. O esforço coletivo inspirou leis e políticas de cibersegurança, tendo como objetivos centrais:

> 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, 159).

Os debates para a Convenção de Budapeste começaram nos anos 1990, impulsionados pela internet. Esse cenário fomentou discussões sobre a governança global da internet, unindo conhecimento científico e técnico com força política e diplomática (Calderaro e Marzouki 2022). Um marco foi a criação da *Internet Corporation for Assigned Names and Numbers* (ICANN) em 1998, uma parceria sem fins lucrativos na Califórnia, Estados Unidos, que permite a participação de atores para promover a política de uso de identificadores únicos da internet (ICANN 2024).

A ICANN foi criada para supervisionar, de forma neutra e global, aspectos técnicos da internet, como DNS[14] e endereços IP. No entanto, essas informações eram administradas pelo *US Department of Commerce*, gerando debates sobre a legitimidade da governança da internet (Carr 2023). Países questionaram se a ICANN representava interesses globais, por estar sob forte influência dos Estados Unidos e ser acusada de falta de transparência (Carr 2023). Desde 2016, a supervisão da ICANN foi transferida à comunidade global, tornando-se independente após medidas de transparência e legitimidade entre os *stakeholders* (Carr 2023).

Esse debate introduz a soberania digital, definida por Kaloudis (2024, 10) como "*the ability of a state or region to control and manage digital infrastructure, data and communication with a relevant degree of autonomy*"[15]. Esse conceito garante ao Estado o direito à autodeterminação e ao controle de suas redes e políticas cibernéticas (Kaloudis 2024). Essa autonomia permite decisões estratégicas independentes, mas também reforça a importância da regulação do ciberespaço para um mundo interconectado, um dos fundamentos da ciberdiplomacia. A Cúpula Mundial sobre a Sociedade da Informação (WSIS) exemplifica o uso da ciberdiplomacia para debates mais inclusivos sobre a internet.

A WSIS ocorreu em duas partes: Genebra (2003) e Túnis (2005), ambas precedidas por comitês preparatórios, grupos e conferências. A fase inicial visou uma declaração para uma sociedade da informação mais igualitária (WSIS 2015). A segunda aplicou os planos de Genebra, acordando sobre governança e financiamento da internet (WSIS 2015). Assim, a WSIS buscou um entendimento comum sobre a sociedade da informação e impactos digitais no sistema internacional.

A WSIS é um exemplo de diplomacia multilateral, em que entidades debatem medidas consensuais. O principal resultado foi o Fórum de Governança da Internet (IGF), parte da Agenda de Túnis em 2005 (IGF 2024a). O IGF reúne atores públicos e privados para formular políticas sobre o mundo digital, da segurança cibernética à governança da internet (IGF 2024b). Esse modelo inovador de discutir políticas públicas em uma organização internacional caracteriza uma nova aplicação da diplomacia. Com a participação de diferentes atores, o IGF é um exemplo de organização *multistakeholder*. Para entender esse novo modelo, é preciso ver como ele é estudado e aplicado.

senhas, dados bancários, números de cartão de crédito ou informações pessoais.

[14] Sistema de nomes de domínio (DNS).

[15] 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".

3.1 *Multistakeholder diplomacy*: um paradigma de ciberdefesa?

O sistema internacional exige que a diplomacia adote cooperação mais ampla e diversificada, indo além de questões de guerra para lidar com regimes interconectados. Nesse contexto, a *multistakeholder diplomacy* é essencial e estratégica para um novo modelo diplomático. Para Denardis e Raymond (2015, 273), uma governança *multistakeholder* é *"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"*[16]. Essa definição enfatiza a centralidade dos atores na decisão. O conceito difere do multilateralismo, descrito por Ruggie (1992, 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*[17].

Embora semelhantes, sistemas complexos exigem interação de diferentes atores para uma diplomacia mais ampla e participativa. A diplomacia *multistakeholder* propõe essa dinâmica, diferenciando-se da tradicional por estruturar mecanismos que promovem participação, ação e responsabilização de atores não governamentais transnacionalmente (Johnstone et al. 2023). Acordos, autoridades internacionais e interesses diversos exigem maior conectividade para regular e mediar ideias e conflitos. A regulação do ciberespaço é um exemplo, envolvendo não só Estados, mas também interesses e controle de setores privados, que gerem infraestruturas tecnológicas críticas.

O *Paris Call for Trust and Security in Cyberspace*, lançado em 2018, exemplifica o debate sobre regulação do ciberespaço, sendo a primeira iniciativa internacional *multistakeholder*, envolvendo Estados, empresas e sociedade civil (France 2024a). A Call propõe nove princípios que orientam discussões entre esses atores, focando na proteção da internet e infraestruturas, promoção de normas e *cyber hygiene* (France 2024b). Iniciativa do governo francês, contou com coordenação de empresas, principalmente Microsoft. Segundo Gorwa e Peez (2020, 273), essa empresa *"assumed the role as a key spokesperson for tech firms in the cybernorms debate, thereby creating part of the present-day cyber-norms environment"*[18], sendo central no debate sobre normas cibernéticas.

A interação entre diferentes atores e seus interesses leva Wolff (2023) a identificar dificuldade em determinar quem liderou o *Paris Call*. Inicialmente articulado por Microsoft e governo francês, a França assumiu a liderança após o lançamento. O *Paris Call* é um modelo híbrido público-privado, mas outras organizações também usam o modelo *multistakeholder* para deliberação e decisão. A ONU, por exemplo, promove iniciativas como o *Group of Governmental Experts* (GGE), um dos primeiros grupos de debate *multistakeholder* da ONU, embora inicialmente sem participação não governamental (Ciglic e Hering 2021). O tema principal do GGE foi '*Developments in the field of information and telecommunications in the context of international security*'[19], destacando o direito internacional como base para regulamentação da internet e ciberespaço (Ciglic e Hering 2021).

O GGE teve seis edições, focadas no impacto de novas tecnologias no sistema internacional, com destaque para ataques na Estônia e o Stuxnet. Por ser uma das primeiras iniciativas, houve divergências de interesses e propostas, algumas vistas como invasivas, outras, como elusivas (Wolff 2023). A experiência do GGE foi importante

---

[16] Tradução 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".
[17] 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".
[18] 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".
[19] Tradução própria: "Desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional".

para a construção e a consolidação do debate *multistakeholder*. Como desdobramento, a ONU criou em 2018 o *Open-Ended Working Group* (OEWG), que ampliou a participação para além dos Estados-membros, incluindo ONGs e setor privado (Wolff 2023).

A Rússia impulsionou a criação do OEWG, criticando o GGE por ser restrito a poucos países, especialmente os Estados Unidos (Wolff 2023). Segundo Wolff (2023), a dificuldade de consenso é um desafio de um fórum *multistakeholder*. Para Johnstone et al. (2023, 12), o debate entre Estados para acordos já é difícil devido a interesses e estruturas governamentais:

> *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*[20].

Contudo, quando a discussão se expande para diferentes atores com suas diretrizes, a consolidação de um debate com resoluções se torna um ponto crucial de observação e análise. Segundo Trachtman (2023), a diplomacia *multistakeholder* não substitui meios de debate tradicionais, como parlamentos, mas amplia a capacidade decisória ao integrar participantes diversos. A participação do setor privado, ONGs e sociedade civil enriquece os acordos com contribuições e perspectivas especializadas. É importante reconhecer que empresas representam seus interesses, enquanto ONGs focam em objetivos sociais (Trachtman 2023). Por isso, antes de aplicar a diplomacia *multistakeholder*, é essencial avaliar os níveis de poder, legitimidade e autoridade dos atores, garantindo equilíbrio e resguardos diplomáticos.

Um exemplo de plataforma de diálogo *multistakeholder* que inclui diferentes perspectivas é o Marco Civil da Internet (MCI), sancionado no Brasil em 2014 (Lei 12.965/14). Essa legislação estabelece princípios e direitos para o uso da internet, cidadania, diversidade e liberdade de expressão (Brasil 2024a). O MCI complementa a Lei Geral de Proteção de Dados (Lei 13.709/2018), que protege direitos de liberdade e privacidade, inclusive digitais (Brasil 2024b). O MCI se diferencia por seu caráter *multistakeholder*, desenvolvido não só pelo Legislativo e pelo Executivo, mas também com a participação da sociedade civil, acadêmicos e setor privado. Esse processo colaborativo levou o MCI a ser conhecido como *The Brazilian Internet Bill of Rights* (Perrone e Souza 2023, 234).

A participação dos atores ocorreu via consulta pública *on-line* em duas etapas: na primeira, colaboraram para identificar temas relevantes que depois foram redigidos pelo Ministério da Justiça; na segunda, a redação foi publicada para opiniões públicas e ajustes (Lemos e Souza 2016). Segundo Souza e Lemos (2016, 21), essa nova abordagem legislativa 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.

Assim, a diplomacia *multistakeholder* impacta positivamente na construção de medidas e regulamentos burocráticos. Ela pode ser aplicada internacionalmente — como fóruns, organizações e convenções — e domesticamente em parlamentos e congressos. A capacidade de adaptação da diplomacia *multistakeholder* é um diferencial. Contudo, é essencial regulamentar os processos para facilitar o debate e definir as interações entre os atores. Essa ferramenta permite soluções mais eficazes e inclusivas para regulação de cenários diversos, como o cibernético, garantindo segurança e paz nas relações internacionais.

4 Considerações finais

O avanço tecnológico e as ameaças ciberné-

[20] 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".

ticas transformam as dinâmicas internacionais, exigindo novas abordagens. A cibersegurança e a ciberdiplomacia são centrais para enfrentar desafios como guerra cibernética, regulação da IA, vigilância digital e governança da internet. Este artigo destacou a evolução do conceito de *segurança*, mostrando sua ampliação para o ciberespaço e suas implicações no cenário internacional.

A ciberdiplomacia se consolida como uma ferramenta essencial para mediar impactos digitais na interação entre Estados e outros atores. Sua eficácia depende de abordagens mais inclusivas que reconheçam a multiplicidade de interesses e competências envolvidos na governança digital, sendo um exemplo disso a diplomacia *multistakeholder*. Ao incluir empresas, organizações, academia e sociedade civil em debates e decisões, esse modelo fortalece a governança transnacional e promove soluções abrangentes para o ciberespaço.

Iniciativas como o *Paris Call* e projetos desenvolvidos na ONU, como o OEWG, evidenciam a importância de mecanismos multilaterais capazes de facilitar o diálogo e a cooperação entre atores. Esses esforços não apenas mitigam as ameaças cibernéticas, mas também contribuem para a construção de um modelo de governança global mais adaptado à complexidade digital. Para que esse modelo seja eficaz, é crucial considerar os níveis de poder, legitimidade e autoridade dos participantes para um processo inclusivo e transparente.

O cenário futuro aponta para um ciberespaço cada vez mais disputado, sofisticado e fragmentado. A ausência de um marco normativo vinculante, a dificuldade em atribuir a responsabilidade por ataques cibernéticos e a crescente influência de tecnologias como a Inteligência Artificial e os *deepfakes* tornam ainda mais urgente o fortalecimento da cooperação internacional. Nesse contexto, uma das principais perspectivas futuras é o fortalecimento de fóruns de debate *multistakeholder*, capazes de reunir os diversos atores envolvidos no desenvolvimento, incentivo e uso dessas tecnologias. Também se vislumbra o avanço de tratados e acordos internacionais que estabeleçam normas de comportamento responsável no ciberespaço, um tema que vem ganhando crescente relevância na agenda internacional.

Ademais, com a ampliação dos conhecimentos e estudos críticos sobre esses processos, é possível que haja mais pesquisas futuras sobre as tensões entre soberania digital e interdependência global, os impactos da assimetria tecnológica na formulação de normas cibernéticas entre diferentes atores e os limites éticos do uso dessas tecnologias. Repensar a segurança internacional à luz dos conflitos cibernéticos requer, portanto, a articulação entre teoria e prática, entre diplomacia tradicional e novas formas de cooperação diplomática.

A integração entre ciberdiplomacia e diplomacia *multistakeholder* é indispensável para um ciberespaço seguro e inclusivo. Compreender os impactos dos novos ambientes digitais e estabelecer processos de regulamentação e decisão por meio desses mecanismos é vital, e, ao mesmo tempo, o atual momento da diplomacia global deixa pouco espaço para esforços de regulamentação multipolar, apontando, pelo contrário, para soluções cada vez mais unilaterais ou à *la carte* para problemas de regulamentação. Essa tensão configura o principal desafio para estudos futuros sobre ciberdiplomacia e *multistakeholder diplomacy*: como criar pontos focais para regulamentação em um cenário de progressiva fragmentação da ordem internacional.

Referências

Araújo, Clayton. 2022. "Os aspectos gerais dos tratados internacionais e a Convenção de Budapeste sobre Crimes Cibernéticos." *Revista da Faculdade de Direito da Universidade Federal de Uberlândia*: 50: 145–65. https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165.

Attatfa, Amel, Stefano De Paoli, e Karen Renaud. 2020. "Cyber Diplomacy: A Systematic Literature Review." *Procedia Computer Science* 176: 60–9.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, e R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology*. https://doi.org/10.1111/ips.12048.

Brasil. 2024a. "Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA." *Senado Notícias*. https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia.

Brasil. 2024b. *Lei Geral de Proteção de Dados Pessoais: Lei nº 13.709/2018*. Senado Federal. https://www2.senado.leg.br/bdsf/handle/id/658231.

Brkan, Maja. 2019. "Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting." *Delphi - Interdisciplinary Review of Emerging Technologies* 2 (2): 66–71. https://doi.org/10.21552/delphi/2019/2/4.

Bull, Hedley. 2002. *A sociedade anárquica: um estudo da ordem na política mundial*. Universidade de Brasília.

Buzan, Barry, Ole Waever, e Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Calderaro, Andrea, e Meryem Marzouki. 2022. "Introduction: Global Internet Governance: An Uncharted Diplomacy Terrain?" In *Internet Diplomacy: Shaping the Global Politics of Cyberspace*. Rowman & Littlefield.

Carr, Madeline. 2023. "Global Internet Governance." In *International Organization and Global Governance*, edited by Thomas Weiss e Rorden Wilkinson. Routledge.

Ciglic, Kaja, e John Hering. 2021. "A Multi-Stakeholder Foundation for Peace in Cyberspace." *Journal of Cyber Policy*: 360–74. https://doi.org/10.1080/23738871.2021.2023603.

Clarke, Richard, e Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Denardis, Laura, e Mark Raymond. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (3): 572–616. https://doi.org/10.1017/S1752971915000081.

Duque, Marina Guedes. 2009. "O papel de síntese da escola de Copenhague nos estudos de segurança internacional." *Contexto Internacional* 31 (3). https://www.scielo.br/j/cint/a/ftcHwZvqyMrrb3ZFRxbwVpF/.

European Commission. 2016. "Estonia Leads the Way with Advanced E-Services for Citizens." https://ec.europa.eu/regional_policy/en/projects/estonia/estonia-leads-the-way-with-advanced-e-services-for-citizens.

France. 2024a. *Paris Call for Trust and Security in Cyberspace*. Ministère de l'Europe et des Affaires étrangères. 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.

France, 2024b. *Paris Call for Trust and Security in Cyberspace*. The 9 principles. https://pariscall.international/en/principles.

Giesen, Klaus-Gerd. 2014. „Justice in Cyberwar." *Ethic@* 13 (1). https://doi.org/10.5007/1677-2954.2014v13n1p27.

Gorwa, Robert, e Anton Peez. 2020. "Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord." In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by Dennis Broeders e Bibi van den Berg. Rowman & Littlefield International. https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf.

Herz, John. 1950. "Idealist Internationalism and the Security Dilemma." *World Politics* 2 (2): 157–80.

Hobbes, Thomas. 2003. *Leviatã*. Martins Fontes.

ICANN. 2024. "What Does ICANN Do?" https://www.icann.org/resources/pages/what-2012-02-25-en.

WSIS – International Telecommunication Union. 2015. "About WSIS Basic Information." https://www.itu.int/net/wsis/basic/about.html.

Internet Governance Forum. 2024a. "The IGF and UN Processes." https://www.intgovforum.org/en/content/the-igf-and-un-processes.

Internet Governance Forum. 2024b. "About the IGF." https://www.intgovforum.org/en/about.

Johnstone, Ian, Arun Sukumar, e Joel Trachtman. 2023. "Building Cybersecurity through Multistakeholder Diplomacy: Politics, Processes, and Prospects." In *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Elgar International Law and Technology. https://doi.org/10.4337/9781035301546.

Kaloudis, Martin. 2024. "Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in Democracies." In *National Security in the Digital and Information Age*, edited by Sally Burt. Intech Open. https://doi.org/10.5772/intechopen.1005415.

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

Lemos, Ronaldo, e Carlos Affonso Souza. 2016. *Marco Civil da Internet: Construção e Aplicação*. Editar Editora Associada.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies*. https://doi.org/10.1080/09636412.2013.816122.

Maquiavel, Nicolau. 2009. *O Príncipe*. Madras Editora.

Mearsheimer, John. 2001. *The Tragedy of Great Power Politics*. W. W. Norton & Company.

CCDCOE – Nato Cooperative Cyber Defence Centre of Excellence. 2024. "About Us." https://ccdcoe.org/about-us/.

Paris Call. 2024. "The 9 Principles." Paris Call. https://pariscall.international/en/principles.

Payne, Kenneth. 2018. "Artificial Intelligence: A Revolution in Strategic Affairs?" *Survival*. https://doi.org/10.1080/00396338.2018.1518374.

Perrone, Christian, e Carlos Affonso Souza. 2023. "Brazil and Multistakeholder Diplomacy for the Internet: Past Achievements, Current Challenges and the Road Ahead." In *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*, edited by Ian Johnstone, Arun Sukumar e Joel Trachtman. Elgar International Law and Technology. https://doi.org/10.4337/9781035301546.

Radanliev, Petar. 2024. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Security Technology*. https://doi.org/10.1080/23742917.2024.2312671.

Ruggie, John. 1992. "Multilateralism: The Anatomy of an Institution." *International Organization* 46 (3): 561–98. https://www.jstor.org/stable/2706989.

Trachtman, Joel. 2023. "Developing Multistakeholder Structures for Cybersecurity Norms: Learning from Experience." In *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*, edited by Ian Johnstone, Arun Sukumar e Joel Trachtman. Elgar International Law and Technology. https://doi.org/10.4337/9781035301546.

UNICC – United Nations International Computing Centre. 2024. *2023 Cyber Threat Landscape Report*. https://www.unicc.org/wp-content/uploads/2024/07/2023-Cyber-Threat-Landscape-Report-1.pdf.

Waltz, Kenneth. 1979. *Theory of International Politics*. Addison-Wesley Publishing Company.

Wolff, Josephine. 2023. "Multistakeholder Characteristics of Past and Ongoing Cybersecurity Norms Processes." In *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*, edited by Ian Johnstone, Arun Sukumar e Joel Trachtman. Elgar International Law and Technology. https://doi.org/10.4337/9781035301546.

Lauren Giordani Gröhs

Graduada em Relações Internacionais pela Universidade La Salle (2024), atuo como pesquisadora independente, analisando a Diplomacia Multistakeholder como ferramenta para a aplicação da ciberdiplomacia.

Fabricío Pontin

PhD, pela Southern Illinois University (2013), é professor na Pós-Graduação em Educação e na Pós-Graduação em Direito na Universidade LaSalle.

Endereço para correspondência

LAUREN GIORDANI GRÖHS

lauren.grohs2610@gmail.com

FABRICÍO PONTIN

fabricio.pontin@unilasalle.edu.br

Os textos deste artigo foram revisados por Araceli Pimentel Godinho e submetidos para validação dos autores antes da publicação.