UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS

JÚLIA RODRIGUES FOGGIA

A CIBERDIPLOMACIA BRASILEIRA E O DILEMA DA ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS: O Desafio da Dissuasão

BRASÍLIA
2026

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS

A CIBERDIPLOMACIA BRASILEIRA E O DILEMA DA ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS: O Desafio da Dissuasão

Monografia apresentada como requisito optativo para a obtenção do título de Bacharel em Relações Internacionais pelo Instituto de Relações Internacionais da Universidade de Brasília (UnB).

Orientador: Professor Doutor Marco Cepik

BRASÍLIA
2026

CIP - Catalogação na Publicação

FF655c

Foggia, Julia.
A CIBERDIPLOMACIA BRASILEIRA E O DILEMA DA ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS: O Desafio da Dissuasão / Julia Foggia;

Orientador: Marco Cepik. Brasília, 2026.
61 f.

Trabalho de Conclusão de Curso (Graduação - Relações Internacionais) Universidade de Brasília, 2026.

1. ciberdiplomacia. 2. atribuição cibernética. 3. dissuasão. 4. Itamaraty. 5. segurança internacional. I. Cepik, Marco, orient. II. Título.

JÚLIA RODRIGUES FOGGIA

A CIBERDIPLOMACIA BRASILEIRA E O DILEMA DA ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS: O Desafio da Dissuasão

Monografia apresentada como requisito optativo para a obtenção do título de Bacharel em Relações Internacionais pelo Instituto de Relações Internacionais da Universidade de Brasília (UnB).

Data da aprovação: 29 / 06 / 2026

gov.br
Documento assinado digitalmente
MARCO AURELIO CHAVES CEPIK
Data: 06/07/2026 11:52:10-0300
Verifique em https://validar.iti.gov.br

_____

Marco Cepik - Orientador
Doutor em Ciência Política
Professor do Instituto de Relações Internacionais (IREL/UnB)

RESUMO

O presente trabalho analisa a intersecção entre a ciberdiplomacia brasileira e o dilema da atribuição em operações cibernéticas, com foco no fortalecimento da capacidade de dissuasão do Estado. O ciberespaço impõe um cenário de incerteza técnica, no qual o anonimato de atores maliciosos gera impunidade e dificulta a responsabilização internacional. Nesse contexto, o objetivo geral da pesquisa é investigar de que maneira a institucionalização da atribuição política pelo Ministério das Relações Exteriores (Itamaraty) pode aprimorar a estratégia de dissuasão nacional, elevando o custo reputacional dos agressores transnacionais. Para atingir esse propósito, o estudo adota uma abordagem qualitativa e exploratória, baseada em revisão bibliográfica sistemática e na análise de documentos oficiais, como a Estratégia Nacional de Cibersegurança (E-Ciber) de 2025 e o posicionamento oficial do Brasil na Organização das Nações Unidas sobre Direito Internacional. Os resultados indicam que a ciberdiplomacia brasileira evoluiu de uma postura estritamente voltada à governança multissetorial para uma visão de segurança estratégica, tratando a soberania no ciberespaço como norma vinculante. O dilema da atribuição demonstra não ser apenas uma barreira técnica forense, mas também um desafio de gestão burocrática e de decisão diplomática. Conclui-se que a institucionalização da atribuição oficial pelo Itamaraty altera diretamente o cálculo de custo-benefício de agentes maliciosos. Ao traduzir inteligência e evidências técnicas em posicionamentos diplomáticos soberanos, o Brasil rompe o ciclo de impunidade, impõe sanções reputacionais e consolida o Itamaraty como a linha de frente da defesa cibernética nacional, o que exige uma nova simbiose entre perícia técnica e sensibilidade geopolítica.

Palavras-chave: ciberdiplomacia; dissuasão; Brasil; segurança internacional.

ABSTRACT

This study analyzes the intersection of Brazilian cyberdiplomacy and the attribution dilemma in cyber operations, with a focus on strengthening the State's deterrence capacity. Cyberspace creates a landscape of technical uncertainty, in which the anonymity of malicious actors confers impunity and hinders international accountability. In this context, the general objective of the research is to investigate how the institutionalization of political attribution by the Ministry of Foreign Affairs (Itamaraty) can improve the national deterrence strategy, raising the reputational cost of transnational aggressors. To achieve this purpose, the study adopts a qualitative, exploratory approach based on a systematic literature review and analysis of official documents, such as the 2025 National Cybersecurity Strategy (E-Ciber) and Brazil's official position at the United Nations on International Law. The results indicate that Brazilian cyberdiplomacy has evolved from a posture strictly focused on multistakeholder governance to a strategic security vision that treats sovereignty in cyberspace as a binding norm. The attribution dilemma proves to be not only a technical forensic barrier but also a challenge of bureaucratic management and diplomatic decision-making. It is concluded that the institutionalization of official attribution by Itamaraty directly alters the cost-benefit calculation of malicious agents. By translating intelligence and technical evidence into sovereign diplomatic positions, Brazil breaks the cycle of impunity, imposes reputational sanctions, and consolidates Itamaraty as the frontline of national cyber defense, demanding a new symbiosis between technical expertise and geopolitical sensitivity.

Keywords: cyberdiplomacy; deterrence; Brazil; international security.

LISTA DE ABREVIATURAS

- **APTs**: Ameaças Persistentes Avançadas (do inglês, *Advanced Persistent Threats*)
- **ComDCiber**: Comando de Defesa Cibernética
- **DCiber**: Divisão de Defesa e Segurança Cibernética do Itamaraty
- **DMDC**: Doutrina Militar de Defesa Cibernética (do Brasil)
- **E-Ciber**: Estratégia Nacional de Cibersegurança
- **GGE**: Grupo de Peritos Governamentais da ONU (do inglês, *Group of Governmental Experts*)
- **GSI**: Gabinete de Segurança Institucional
- **IPs**: Protocolos de Internet (do inglês, *Internet Protocols*)
- **MRE**: Ministério das Relações Exteriores
- **NSA**: Agência de Segurança Nacional dos EUA (do inglês, *National Security Agency*)
- **OEWG**: Grupo de Trabalho de Composição Aberta (do inglês, *Open-Ended Working Group*)
- **ONU**: Organização das Nações Unidas
- **OTAN**: Organização do Tratado do Atlântico Norte
- **TTPs**: Táticas, Técnicas e Procedimentos
- **UE**: União Europeia

SUMÁRIO

INTRODUÇÃO ---------- 8

CAPÍTULO 1 - CIBERDIPLOMACIA ---------- 14

1.1 Evolução Conceitual: Da Diplomacia Digital à Ciberdiplomacia ---------- 16

1.2 A Ciberdiplomacia Brasileira: Trajetória, Governança e Segurança ---------- 18

CAPÍTULO 2 - ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS ---------- 30

2.1 Dimensões da Atribuição: Da Perícia Técnica à Decisão Política ---------- 30

2.2 O Dilema da Prova e a Responsabilidade Internacional no Ciberespaço -------- 33

CAPÍTULO 3 - ATRIBUIÇÃO E CIBERDIPLOMACIA ---------- 37

3.1 A Atribuição como Instrumento de Dissuasão ---------- 37

3.2 O Modelo Brasileiro: Entre a E-Ciber 2025 e a Prática Diplomática ---------- 43

CONCLUSÃO ---------- 49

REFERÊNCIAS ---------- 53

INTRODUÇÃO

O ciberespaço consolidou-se como um domínio transversal às interações humanas, redefinindo as dinâmicas de poder e os métodos de condução da política externa no século XXI. É fundamental, portanto, distinguir o ciberespaço da internet ou do espaço digital, pois o primeiro engloba não apenas a rede lógica mundial, mas também toda a infraestrutura física subjacente e o uso do espectro eletromagnético para a transmissão de dados e para operações táticas. Nesse cenário, a atuação internacional dos Estados precisou se adaptar, dando origem a conceitos distintos, porém frequentemente confundidos: a diplomacia digital e a ciberdiplomacia.

A diplomacia digital refere-se, essencialmente, à instrumentalização da tecnologia. Autores como Góes (2017) e Frey (2024) a conceituam como o uso da internet, das redes sociais e de ferramentas digitais como mecanismos de condução da política externa e da diplomacia pública, com o objetivo de influenciar audiências e facilitar a comunicação estatal. Trata-se do meio digital aplicado à diplomacia tradicional.

A ciberdiplomacia, por sua vez, transcende a ferramenta e foca no ciberespaço como o objeto de negociação e disputa. Na literatura, há diferentes abordagens a este conceito. O *Cyber Diplomacy Toolbox* (2026), por exemplo, define a ciberdiplomacia de forma bastante alinhada aos esforços da União Europeia para proteger seus interesses estratégicos e promover valores democráticos no ciberespaço. Outra vertente, apresentada por Gröhs (2024), destaca o aspecto da governança, enfatizando a diplomacia *multistakeholder*, na qual as negociações exigem a participação da sociedade civil e de empresas de tecnologia. Por outro lado, Attatfa, Renaud e De Paoli (2020) definem a ciberdiplomacia de forma mais ampla, como o uso de recursos diplomáticos e de negociação para abordar questões de segurança, estabilidade e normas de comportamento relacionadas ao ciberespaço na agenda internacional. Salvi, Tiirmaa-Klaar e Lewis (2024) complementam essa visão, inserindo-a na interseção entre a política externa, a segurança cibernética e a defesa de infraestruturas críticas.

Para os propósitos desta pesquisa, adota-se a definição estratégica de ciberdiplomacia, pautada por Attatfa, Renaud e De Paoli (2020) e por Salvi, Tiirmaa-Klaar e Lewis (2024). Essa escolha justifica-se, pois um conceito puramente focado em governança multissetorial ou restrito a condenações públicas seria inócuo para analisar o aumento da capacidade de defesa e

de dissuasão do Brasil. A ciberdiplomacia aqui tratada é a aplicação da política externa para salvaguardar a soberania, mediar conflitos e construir capacidades dissuasórias credíveis no espectro cibernético.

Nesse contexto brasileiro, o Ministério das Relações Exteriores (Itamaraty) desempenha um papel central na articulação dessas normas. No entanto, a eficácia das estratégias no ciberespaço enfrenta o desafio persistente do anonimato. Segundo Sheldon (2024), do ponto de vista estritamente técnico, trata-se de determinar a identidade ou localização do autor. Porém, Rid e Buchanan (2015) ampliam o conceito, demonstrando que a atribuição é uma arte que mescla a perícia forense (tática e operacional) com o julgamento político e estratégico, exigindo uma decisão soberana para apontar um culpado.

Essa incerteza técnica gera uma lacuna de impunidade, em que atores transnacionais — compreendidos aqui como agentes não estatais, corporações mercenárias cibernéticas ou grupos criminosos (*proxies*) que operam atravessando fronteiras nacionais e, muitas vezes, a serviço oculto de Estados — operam sob o manto da ambiguidade para evitar responsabilização (TSAGOURIAS; FARRELL, 2020).

A ausência de uma atribuição clara impacta diretamente a segurança do Estado, embora seja imperativo separar a diplomacia (instrumento político de interação estatal) da capacidade de dissuasão (postura estratégica de defesa). A essência da dissuasão consiste na capacidade de impedir que a outra parte realize uma ação indesejada por meio da ameaça de retaliação ou de punição (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022). No domínio cibernético, Nye Jr. (2017) argumenta que a dissuasão opera por negação, por emaranhamento (*entanglement*), por tabus normativos e por punição. Como a punição física imediata — isto é, a retaliação cinética ou ataque militar convencional — é rara e de altíssimo risco de escalada, a atribuição diplomática torna-se fundamental.

Surge, contudo, um questionamento crítico: em que medida publicizar fatos verificáveis em fóruns diplomáticos favorece a defesa cibernética, e como o reconhecimento público de um ataque perpetrado por uma grande potência ajudaria o Brasil a retaliar? A resposta reside na compreensão de que a retaliação cibernética e a dissuasão não dependem exclusivamente do revide bélico. Ao institucionalizar o "*name and shame*" (nomear e envergonhar), sustentado por processos técnicos estruturados, o Estado impõe severos custos reputacionais e econômicos,

isolando o agressor e restringindo seu *soft power* em fóruns multilaterais (EGLOFF; SMEETS, 2023). Além disso, a atribuição pública inequívoca fornece a base legal exigida pelo Direito Internacional para que o Estado vítima possa aplicar contramedidas diplomáticas e sanções econômicas legítimas, elevando o custo de futuras agressões, mesmo quando oriundas de atores com maiores capacidades bélicas (GARCIA, 2025; SCHMITT, 2017).

No entanto, a eficácia das estratégias diplomáticas no ciberespaço enfrenta o desafio persistente do anonimato, que dificulta a responsabilização de atores maliciosos. O chamado "dilema da atribuição" refere-se à complexidade técnica e política de identificar com precisão a autoria e a origem de operações cibernéticas. Conforme apontam os debates no Grupo de Peritos Governamentais da ONU (em inglês, *Group of Governmental Experts* - GGE), as acusações de atos ilícitos devem ser devidamente fundamentadas, pois a infraestrutura de um Estado pode ser utilizada para ataques sem o seu conhecimento direto. Essa incerteza técnica gera uma lacuna de impunidade, na qual agentes transnacionais operam sob o manto da ambiguidade para evitar sanções ou condenações públicas, desafiando a lógica tradicional de custódia territorial (SOUZA; MARTINS, 2023).

Entende-se que a ausência de uma atribuição clara impacta diretamente a capacidade de dissuasão de um Estado. Contudo, é fundamental estabelecer a distinção analítica entre dissuasão e diplomacia, institutos complementares, mas de naturezas distintas. A dissuasão consiste em uma postura estratégica de defesa que visa impedir um adversário de realizar uma ação indesejada por meio da manipulação do seu cálculo racional, tradicionalmente por meio da ameaça crível de retaliação ou punição (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022; MORGAN, 2003). A diplomacia, por sua vez, é o instrumento político e institucional de condução da política externa, pautado pelo diálogo, pela persuasão e pela negociação de interesses do Estado de forma não coercitiva (ARON, 2002; MAGALHÃES, 1996).

Apesar dessa distinção basilar, a capacidade de dissuasão e a ação diplomática devem operar de forma sinérgica no domínio cibernético. A dissuasão digital não se limita à punição militar letal, operando também por meio de mecanismos políticos (NYE JR., 2017). Devido às barreiras operacionais à imposição de uma punição física imediata diante da incerteza técnica do anonimato, Nye Jr. (2017) argumenta que a dissuasão cibernética moderna ampara-se no "emaranhamento" (a interdependência econômica e institucional) e nos "tabus normativos". É precisamente neste ponto que a distinção se materializa: a diplomacia não é a dissuasão em si,

mas atua como o veículo político e jurídico para mobilizar e acionar esses mecanismos de contenção.

Dessa forma, ao realizar a atribuição pública e fundamentada de um ataque, o instrumento diplomático operacionaliza a estratégia dissuasória, expondo o agressor a fim de elevar severamente os seus custos reputacionais, institucionais e econômicos no cenário global (EGLOFF; SMEETS, 2023). É a partir desse nexo — entre a diplomacia como ferramenta de acusação e constrangimento, e a dissuasão como finalidade estratégica de proteção — que se insere o problema de pesquisa deste trabalho: de que maneira a institucionalização da atribuição pelo Itamaraty fortaleceria a capacidade de dissuasão do Estado brasileiro frente a ameaças cibernéticas transnacionais?

A hipótese levantada é que a institucionalização da atribuição política pelo Itamaraty fortaleceria a dissuasão cibernética ao elevar o custo reputacional de atores maliciosos no cenário internacional e ao romper a impunidade decorrente do anonimato. Ao converter subsídios técnicos e fatos verificáveis em posicionamentos diplomáticos oficiais, o Brasil projeta uma postura de assertividade e responsabilidade. Conforme a lógica da "dissuasão pela punição" (NYE JR., 2017), essa prática desestrutura o cálculo de custo-benefício de agentes transnacionais que se valem da ambiguidade do ciberespaço para realizar operações maliciosas sem sofrer sanções ou condenações públicas.

A dissuasão no ambiente cibernético exige uma reavaliação do conceito clássico de retaliação militar. Tradicionalmente, a dissuasão baseia-se na capacidade de impor danos físicos inaceitáveis ao adversário. No entanto, na esfera digital, a retaliação não precisa — e, estrategicamente, muitas vezes não deve — ser estritamente cinética ou destrutiva. A dissuasão cibernética opera por meio de múltiplos mecanismos, destacando-se a punição, a negação, o emaranhamento (*entanglement*) e a imposição de tabus normativos (NYE JR., 2017). Para um Estado como o Brasil, ao enfrentar uma grande potência, a capacidade de retaliação não reside em uma assimetria bélica ou no disparo de mísseis, mas na capacidade de impor severos custos políticos, reputacionais e econômicos, materializando o que a literatura denomina retaliação cruzada ou *cross-domain deterrence* (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022).

Ademais, a publicização de "fatos verificáveis" favorece a defesa cibernética, principalmente ao destruir a maior vantagem tática do ofensor: o anonimato e a negação

plausível. Ao documentar e expor publicamente os métodos, táticas, técnicas e procedimentos (TTPs) e as infraestruturas utilizados no ataque, o Estado vítima gera um atrito operacional (*friction*) imediato para o agressor (EGLOFF; SMEETS, 2023). A exposição obriga a grande potência a abandonar ferramentas e servidores comprometidos, o que demanda tempo e recursos financeiros para redesenhar seu arsenal cibernético. Além disso, ao basear a denúncia em fatos estritamente verificáveis, o Brasil alinha-se ao Direito Internacional e evita o chamado "justiceirismo digital", garantindo legitimidade inquestionável à sua narrativa e fortalecendo sua posição diplomática perante a comunidade internacional (GARCIA, 2025).

No que tange à retaliação, a explicitação e o reconhecimento público bem documentado do ataque são os pré-requisitos legais e políticos que viabilizam o revide. De acordo com o Direito Internacional Consuetudinário e as diretrizes do Manual de Tallinn 2.0, a atribuição formal da autoria de um ato internacionalmente ilícito é a condição *sine qua non* para que o Estado agredido tenha o direito de adotar contramedidas proporcionais (SCHMITT, 2017). Se os ataques de uma grande potência persistissem, o reconhecimento público e embasado forneceria ao Brasil a base jurídica para retaliar de forma assimétrica em outros domínios. Isso inclui o congelamento de ativos financeiros, o embargo à importação de tecnologias do país agressor (como restrições às licitações de infraestrutura 5G), a suspensão de acordos bilaterais e a expulsão formal de diplomatas estrangeiros sob a acusação de espionagem (EGLOFF; SMEETS, 2023).

Além disso, a documentação pública do ataque permitiria ao Brasil mobilizar a retaliação coletiva e acionar a lógica do emaranhamento econômico. Nenhuma grande potência atua em vácuo; todas dependem das cadeias globais de suprimentos e de sua reputação no comércio internacional (NYE JR., 2017). Ao levar provas forenses e fatos verificáveis a fóruns multilaterais, como a Assembleia Geral da ONU e o Grupo de Trabalho de Composição Aberta (OEWG, do inglês *Open-ended Working Group*), o Brasil pode invocar o princípio da Devida Diligência (*Due Diligence*), responsabilizando o Estado hostil por permitir o uso malicioso de seu território (MARTINS, 2025). Essa articulação diplomática converte a agressão em um tabu normativo, viabilizando a imposição de sanções conjuntas por blocos aliados, à semelhança do *Cyber Diplomacy Toolbox* da União Europeia (UE) (SERRANO, 2022). Dessa forma, a retaliação brasileira torna-se crível e severa para os interesses do agressor, pois o isolamento

sistêmico e o prejuízo econômico superam, em larga medida, os ganhos táticos pretendidos pela invasão cibernética.

É nessa linha de raciocínio que o objetivo geral desta pesquisa foi definido como: analisar de que maneira a institucionalização da atribuição política de operações cibernéticas pelo Ministério das Relações Exteriores (Itamaraty) pode fortalecer a estratégia de dissuasão brasileira contra ameaças cibernéticas transnacionais, ao elevar o custo reputacional de atores maliciosos e reduzir a impunidade na esfera internacional. Para tanto, os objetivos específicos buscam: contextualizar e definir ciberdiplomacia, identificando o seu papel e evolução dentro da política externa brasileira; investigar os dilemas e desafios da atribuição em operações cibernéticas, diferenciando as dimensões técnicas e políticas; avaliar o nexo entre atribuição e dissuasão cibernética, examinando como a imposição de custos diplomáticos altera o cálculo do agressor; e identificar os desafios da postura brasileira frente às recentes diretrizes da Estratégia Nacional de Cibersegurança do Brasil (E-Ciber), instituída pelo decreto 12.573, de 4 de agosto de 2025.

A condução deste estudo fundamenta-se nas diretrizes propostas por Jaccard e Jacoby (2020), que enfatizam a importância da construção teórica e de modelos conceituais explícitos nas Ciências Sociais. Segundo os autores, o desenvolvimento de uma teoria exige a identificação clara de conceitos e a especificação de como se relacionam, permitindo ao pesquisador organizar o conhecimento de forma lógica e verificável (JACCARD; JACOBY, 2020). Nesse sentido, a pesquisa adota uma abordagem qualitativa e exploratória, tratando a "atribuição política" como a variável central que, quando manipulada de forma diplomática, gera efeitos na "capacidade de dissuasão" do Estado brasileiro.

Seguindo o guia prático para cientistas sociais de Jaccard e Jacoby (2020), a estrutura analítica foi concebida para integrar múltiplas fontes de dados, visando à construção de um modelo que explique o comportamento dos atores no ciberespaço. O processo metodológico envolveu a análise de documentos oficiais, como a Estratégia Nacional de Cibersegurança (E-Ciber) e relatórios internacionais, bem como a realização de uma revisão bibliográfica sistemática. A aplicação desses métodos permite que a pesquisa não apenas descreva o fenômeno, mas também construa uma base teórica capaz de sustentar as recomendações de política externa propostas, garantindo que as inferências sobre o custo reputacional sejam derivadas de um modelo de tomada de decisão racional (JACCARD; JACOBY, 2020).

O primeiro capítulo, intitulado "Ciberdiplomacia", estabelece a base conceitual e o histórico da atuação brasileira. A discussão diferencia rigorosamente a diplomacia digital da ciberdiplomacia, utilizando as contribuições de Attatfa, Renaud e De Paoli (2020) e de Salvi, Tiirmaa-Klaar e Lewis (2024) para alicerçar o conceito de diplomacia como instrumento de segurança e estabilidade, superando visões puramente instrumentalistas ou multissetoriais. O capítulo analisa a evolução da posição brasileira desde a Assembleia Geral da ONU até os fóruns do Grupo de Peritos Governamentais da ONU (GGE) e o Grupo de Trabalho de Composição Aberta (OEWG), buscando entender como a política externa do Itamaraty se adapta às novas ameaças.

O segundo capítulo, "Atribuição em Operações Cibernéticas", dedica-se a investigar os complexos desafios técnicos, jurídicos e políticos de identificar agressores no ambiente virtual. A discussão fundamenta-se no "Manual de Tallinn" (2017) sobre a aplicação do Direito Internacional em conflitos cibernéticos e nos estudos de Thomas Rid e Ben Buchanan (2015) sobre a arte da atribuição. O foco será o "dilema da atribuição", explorando como a ambiguidade técnica é utilizada por atores estatais e não estatais para evitar a responsabilização por atos ilícitos. Trata-se de demonstrar que a atribuição política é um ato soberano que não depende exclusivamente da prova forense perfeita, mas sim de um processo de inteligência e de decisão diplomática.

O terceiro capítulo, "Atribuição e Ciberdiplomacia", examina o nexo causal entre a quebra do anonimato e o fortalecimento da dissuasão. Com base na teoria de Joseph Nye Jr. (2017) sobre os mecanismos de dissuasão (punição, negação, emaranhamento e tabus), o capítulo analisa como o Itamaraty, ao oficializar atribuições públicas, pode elevar os custos reputacionais dos agressores. Serão incorporadas as perspectivas de Lisboa e Oliveira (2021) sobre a operacionalização da dissuasão no contexto brasileiro, confrontando as metas da Estratégia Nacional de Cibersegurança (E-Ciber) (BRASIL, 2025) com as limitações da postura diplomática atual. A conclusão do capítulo avaliará como a "postura de responsabilidade" adotada pelo Brasil pode atuar como um desincentivo a futuras operações maliciosas contra o país.

CAPÍTULO 1 - CIBERDIPLOMACIA

A emergência do ciberespaço consolidou-o como o quinto domínio de atuação estratégica dos Estados — somando-se aos domínios terrestre, marítimo, aéreo e espacial —,

conforme reconhecido nas doutrinas de segurança de diversos países e na Doutrina Militar de Defesa Cibernética do Brasil (DMDC) (BRASIL, 2023). Se, em décadas anteriores, a tecnologia era percebida meramente como um vetor de eficiência comunicacional, hoje ela constitui o próprio cerne da agenda de segurança e de política externa.

Para compreender este cenário, faz-se necessário definir o conceito clássico de soberania — entendido como a autoridade suprema e exclusiva de um Estado sobre seu território e sua população — e adaptá-lo ao espaço cibernético. A soberania cibernética compreende a extensão dessa autoridade sobre a infraestrutura de tecnologia da informação e comunicação localizada fisicamente dentro das fronteiras do Estado, bem como o direito de regular as atividades cibernéticas que ali ocorrem (BRASIL, 2021).

A fundamentação geopolítica que sustenta a percepção brasileira de soberania no ambiente digital pode ser compreendida por meio do intrincado processo de territorialização do ciberespaço. Conforme discutido na obra organizada por Medeiros Filho, Ferreira Neto e Gonzales (2014), o ciberespaço não deve ser romantizado como um 'vazio' amorfo e desprovido de jurisdição, mas sim como um domínio estratégico, ativamente submetido a uma nova forma de controle espacial e de poder. Ao analisarem as transformações da fronteira física em muros virtuais, os autores demonstram que, diferentemente das fronteiras tradicionais, representadas por linhas e faixas limítrofes, o ambiente cibernético inaugura um tipo de 'fronteira-ponto'. Nesse modelo, a territorialidade do Estado materializa-se em pontos específicos (os 'nós' da rede), abrangendo data centers, infraestruturas críticas de telecomunicações e os próprios pacotes de informação que por eles trafegam. Ao se adotar essa ótica de (re)territorialização, justifica-se plenamente a postura da defesa e da ciberdiplomacia nacionais: uma intrusão não autorizada ou a sabotagem de um desses 'nós' informacionais não se configura como mera falha técnica em um espaço globalizado comum, mas constitui uma violação tangível da 'fronteira-ponto' nacional, equiparando-se a uma quebra direta da integridade territorial do Estado brasileiro (MEDEIROS FILHO; FERREIRA NETO; GONZALES, 2014).

Neste contexto, a ciberdiplomacia surge como um imperativo estratégico para a sobrevivência e projeção de interesses nacionais em um ambiente marcado pela anarquia e pela natureza transnacional das ameaças. Diferentemente das ameaças internacionais (que ocorrem classicamente de Estado para Estado), as ameaças cibernéticas transnacionais envolvem o cruzamento de fronteiras por atores não estatais, como corporações, grupos criminosos e

ativistas, que frequentemente operam à margem da autoridade estatal, diluindo as fronteiras tradicionais (TSAGOURIAS; FARRELL, 2020).

Dessa forma, o capítulo propõe-se a analisar a ciberdiplomacia sob uma perspectiva multidimensional. Inicialmente, estabelece-se a distinção fundamental entre a diplomacia digital e a ciberdiplomacia, evitando equívocos conceituais comuns. Em seguida, examina-se a trajetória da política externa brasileira neste campo, observando como o Itamaraty evoluiu de uma postura focada na governança da internet para um posicionamento mais assertivo no âmbito da segurança internacional e do Direito Internacional aplicável ao ciberespaço.

1.1 Evolução Conceitual: Da Diplomacia Digital à Ciberdiplomacia

Na literatura, há confusão entre diplomacia digital e ciberdiplomacia. No entanto, elas referem-se a objetos e agendas distintos, e não apenas a uma dicotomia entre método e substância.

A diplomacia digital refere-se ao uso das tecnologias de informação e da internet como ferramentas para aprimorar e conduzir a política externa. Conforme define Góes (2017), trata-se da internet como ferramenta da política externa para influenciar audiências e facilitar a diplomacia pública. Frey (2024) reforça essa visão ao apontar que a diplomacia digital aborda o impacto da tecnologia na comunicação moderna e na condução das negociações. Em suma, a diplomacia digital consiste na adoção de plataformas e recursos digitais para a consecução de objetivos diplomáticos clássicos.

A ciberdiplomacia, por sua vez, tem o próprio ciberespaço e sua segurança como objeto da diplomacia. Na literatura, observam-se diferentes ênfases sobre este conceito. Gröhs (2024) aborda a ciberdiplomacia sob o viés da governança e da diplomacia *multistakeholder*, destacando a inclusão da sociedade civil e das empresas nas negociações. Já o *Cyber Diplomacy Toolbox* (2026) apresenta uma definição mais voltada aos interesses e à estratégia de resiliência e estabilidade projetada pela União Europeia.

Neste trabalho, adota-se a visão convergente de Attatfa, Renaud e De Paoli (2020) e Salvi, Tiirmaa-Klaar e Lewis (2024). Para Attatfa, Renaud e De Paoli (2020), a ciberdiplomacia é o uso de recursos diplomáticos para abordar questões relacionadas ao ciberespaço na agenda internacional, visando a resolução de conflitos e a criação de normas. Salvi, Tiirmaa-Klaar e

Lewis (2024) complementam esse entendimento definindo-a como uma prática que opera na interseção entre a política externa, a segurança cibernética nacional e a gestão de crises internacionais. Optou-se por nortear o trabalho sob esta conceituação porque uma visão focada primordialmente na segurança e na regulação internacional do ciberespaço alinha-se à hipótese desta pesquisa, que investiga a capacidade de dissuasão do Estado diante de agressões.

No contexto das Relações Internacionais, a ciberdiplomacia manifesta-se como o esforço dos Estados para normatizar e regular o ciberespaço, inserindo-o nas molduras jurídicas existentes. Como aponta Realpe Díaz (2024), trata-se de uma estratégia essencial para a consecução de interesses nacionais, permitindo ao Estado projetar sua influência. No entanto, as estratégias divergem conforme o tipo de ameaça, sendo um erro tratar os fenômenos cibernéticos como um bloco homogêneo: o cibercrime busca lucro financeiro, a ciberespionagem visa à coleta silenciosa de informações e a guerra cibernética busca a disrupção e a destruição de infraestruturas críticas (LANCELOT, 2020).

Nesse sentido, Cepik, Canabarro e Ferreira (2015) alertam para os riscos do 'alongamento conceitual' (*conceptual stretching*) ao se classificar, de forma imprecisa, generalista ou precipitada, incidentes rotineiros no ciberespaço como 'guerra cibernética'. Segundo Carl von Clausewitz, a guerra envolve necessariamente o uso ou a ameaça de uso da força, de forma instrumental e interativa, o que a imensa maioria dos ciberataques não alcança. Tais operações atuam, em vez disso, por meio de violência indireta, disrupção sistêmica temporária ou espionagem silenciosa (CEPIK; CANABARRO; FERREIRA, 2015). Tratar qualquer intrusão digital como um ato de guerra não apenas trivializa o conceito analítico, mas também induz a respostas estatais precipitadas e a uma militarização do ciberespaço que pode ser altamente prejudicial, inadequada ou ineficaz para o Estado vítima.

É precisamente diante dessa constatação teórica que a ciberdiplomacia ganha primazia absoluta sobre a resposta armada ou reativa tradicional. Como a ampla maioria das agressões cibernéticas opera em uma 'zona cinzenta' que permanece abaixo do limiar legal de um ataque armado *stricto sensu*, a dissuasão militar clássica perde a sua aplicabilidade direta, exigindo soluções não cinéticas. Dessa forma, a atuação do Itamaraty na atribuição política dos ataques consolida-se como o instrumento mais adequado e proporcional de defesa: em vez de cogitar o uso da força perante um incidente que não configura guerra convencional, o Estado utiliza a via diplomática institucional para expor a autoria da agressão, invocar o Direito Internacional e

impor severos custos políticos e econômicos, adequando a reação à verdadeira natureza política do conflito (CEPIK; CANABARRO; FERREIRA, 2015).

A transição para a ciberdiplomacia como disciplina autônoma reflete a percepção de que o ciberespaço é um multiplicador de poder. Conforme aponta Realpe Díaz (2024), os mecanismos de ciberdiplomacia são estratégias essenciais para a consecução de interesses nacionais, pois permitem que o Estado projete influência sem recorrer necessariamente ao poder cinético. No entanto, essa projeção de poder enfrenta o "dilema da segurança" no ciberespaço: o aumento das capacidades defensivas de um Estado pode ser interpretado como uma ameaça ofensiva por outro, o que gera uma corrida armamentista digital (DELFINO, 2014).

Assim, a ciberdiplomacia brasileira, ao atuar em fóruns como a ONU, precisa equilibrar a defesa da soberania estatal com a realidade de um ambiente de governança compartilhada e descentralizada.

1.2 A Ciberdiplomacia Brasileira: Trajetória, Governança e Segurança

A inserção do Brasil nos debates internacionais sobre o ciberespaço tem uma trajetória marcada pela defesa da privacidade, do desenvolvimento e, mais recentemente, da segurança e da estabilidade internacionais. O ponto de inflexão na ciberdiplomacia brasileira ocorreu em 2013, após as revelações de espionagem da *National Security Agency* (NSA) dos Estados Unidos da América contra a alta cúpula do governo federal e empresas estratégicas como a Petrobras (VELANDIA, 2025). Aquele evento impulsionou o Brasil a liderar a iniciativa da NETmundial em 2014, posicionando o país como um *norm-shaper* (formador de normas) na governança global da internet.

Embora esse episódio seja frequentemente classificado como o 'despertador cibernético' (*cyber wake-up call*) que impulsionou o engajamento normativo do país nas Nações Unidas (MARTINS, 2025), ele ilustra de forma contundente o 'vácuo de dissuasão' ao qual o Brasil estava submetido. Naquela ocasião, apesar de a autoria ser inquestionável, a comprovação não resultou em retaliações coercitivas diretas, como a imposição de sanções econômicas ou de embargos cruzados. O mal-estar diplomático, embora severo, limitou-se ao campo discursivo e à promoção de normativas multissetoriais (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022). A ausência de custos retaliatórios tangíveis para o agressor evidenciou a vulnerabilidade

do Estado brasileiro frente a uma superpotência e demonstrou que, sem uma ciberdiplomacia estruturada para impor punições não cinéticas, atores com alto poderio tecnológico tendem a operar na impunidade.

No âmbito das Nações Unidas, a atuação brasileira tem sido histórica e tecnicamente fundamentada. O Brasil participa ativamente dos Grupos de Peritos Governamentais (GGE) e do Grupo de Trabalho de Composição Aberta (OEWG). Segundo Martins (2025), o país defende consistentemente que o Direito Internacional, incluindo a Carta da ONU, é aplicável ao ciberespaço. Em 2021, o Ministério das Relações Exteriores oficializou sua posição no documento "Position of Brazil on International Law Applicable to Cyber Operations", reforçando que a soberania estatal se estende à infraestrutura de tecnologia da informação localizada em seu território (BRASIL, 2021).

A operacionalização da segurança nacional exige que o Itamaraty atue como o principal tradutor institucional entre a perícia técnica e a linguagem diplomática. Tal processo de "tradutibilidade" já está em curso por meio da Divisão de Defesa e Segurança Cibernética (DCiber) do Itamaraty, que recebe e filtra informações sensíveis provenientes de órgãos como o Gabinete de Segurança Institucional (GSI) e o Comando de Defesa Cibernética (ComDCiber). Contudo, essa coordenação burocrática enfrenta desafios contínuos de alinhamento interno para que o dado técnico bruto seja convertido tempestivamente em uma narrativa jurídica sólida perante a comunidade internacional (BROTHERHOOD, 2024).

A dissuasão cibernética, foco central desta defesa, é complexa devido ao "dilema da atribuição". O conceito de dissuasão implica impedir que um ator realize uma ação indesejada por meio da ameaça de consequências severas (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022). Nye Jr. (2017) complementa afirmando que a dissuasão no ciberespaço não se baseia apenas na retaliação, operando fortemente por meio da "dissuasão por punição diplomática" e do "emaranhamento". Entretanto, como apontam Rid e Buchanan (2015), sem a capacidade de atribuir (identificar a autoria da operação maliciosa com respaldo técnico e político), a ameaça de punição perde credibilidade. A atribuição cibernética, conforme Sheldon (2024) e Tsagourias e Farrell (2020), abrange não apenas a verificação de registros técnicos (*logs* de IPs e assinaturas de código), mas também uma decisão política consciente e soberana de responsabilizar publicamente um ator.

Ao contrário de grandes potências que utilizam a atribuição unilateral frequentemente como ferramenta de pressão geopolítica, a postura brasileira, liderada pelo Itamaraty, tem sido pautada pela necessidade de evidências verificáveis, evitando expor desnecessariamente vulnerabilidades internas (GARCIA, 2025). A ciberdiplomacia brasileira alcançou sua maturidade normativa, mas a transição de um aparato normativo para a efetiva mitigação de agressões permanece em desenvolvimento.

Portanto, a ciberdiplomacia brasileira enfrenta o desafio de adaptar a sua tradicional política externa "altiva e ativa" (AMORIM, 2014; BROTHERHOOD, 2024) e a sua vocação para a solução pacífica de controvérsias à necessidade de estabelecer mecanismos críveis de dissuasão face a ameaças cibernéticas transnacionais. Nesse sentido, a Estratégia Nacional de Cibersegurança (E-Ciber), atualizada pelo Decreto nº 12.573, de 2025, não constitui uma ruptura de paradigma, mas sim o amadurecimento e a institucionalização dessa agenda na estrutura do Estado, mantendo-se coerente com os valores históricos da inserção internacional do País (MARTINS, 2025). O documento enfatiza a urgência de fortalecer a resiliência nacional e a cooperação internacional no combate a crimes cibernéticos e a ataques estatais (BRASIL, 2025). Dessa forma, a E-Ciber reconhece que a segurança cibernética é um componente indissociável da Defesa Nacional, o que exige a integração perene entre a produção de inteligência e as visões estratégicas do Ministério da Defesa e do Itamaraty.

Na prática, a operacionalização dessa estratégia demonstra que o Itamaraty já atua como o principal tradutor institucional entre a perícia técnica e a linguagem diplomática. Esta 'tradutibilidade' não é meramente semântica, mas uma rotina burocrática consolidada: o Ministério das Relações Exteriores hoje articula e coordena os fluxos de informação sensível provenientes do Gabinete de Segurança Institucional (GSI) e do Comando de Defesa Cibernética (ComDCiber), filtrando as evidências forenses de modo que estas sustentem, com embasamento fático, os posicionamentos oficiais do Brasil em fóruns como o OEWG da ONU (BROTHERHOOD, 2024). A institucionalização definitiva desse processo materializou-se com a criação da Divisão de Defesa e Segurança Cibernética (DCiber) do Itamaraty em 2022. É essa estrutura interministerial que atualmente permite que o dado técnico bruto — como IPs de origem ou assinaturas de *malware* — seja convertido em uma narrativa jurídica de violação de soberania, etapa essencial para garantir a credibilidade e a legitimidade de qualquer resposta internacional do Estado brasileiro (MARTINS, 2025).

A doutrina militar brasileira tem acompanhado ativamente a evolução das ameaças no quinto domínio. Documentos estratégicos como o Livro Branco de Defesa Nacional (BRASIL, 2020) e a Doutrina Militar de Defesa Cibernética (BRASIL, 2023) já apontam expressamente para a necessidade de construir capacidades de dissuasão no campo digital. Todavia, a estruturação dessa dissuasão esbarra inicialmente no complexo "problema da atribuição". Como argumentam Rid e Buchanan (2015), sem a capacidade de identificar o agressor de forma inequívoca, qualquer ameaça de retaliação perde a sua credibilidade primária, pois não há um alvo claro contra o qual direcionar a resposta.

Entretanto, a superação do dilema da atribuição e a mera identificação do agressor não garantem, por si sós, o sucesso da estratégia dissuasória. A eficácia da dissuasão no ciberespaço é profundamente condicionada por dois fatores estruturais que, frequentemente, são mais determinantes do que a capacidade de apontar o culpado: a natureza do ato ofensivo e a assimetria de capacidades mútuas entre o agressor e o defensor (NYE JR., 2017). A natureza da agressão dita os limites da resposta: um cibercrime financeiro exige cooperação policial; a ciberespionagem é historicamente tolerada na "zona cinzenta" das relações internacionais; já um ciberataque militar destrutivo exige retaliações severas amparadas pelo Direito Internacional. Paralelamente, o cálculo dissuasório é regido pela balança de poder (capacidades materiais e tecnológicas). Um Estado com capacidades cibernéticas ou bélicas muito inferiores terá severas dificuldades em dissuadir uma superpotência agressora, pois a assimetria de forças reduz drasticamente o temor adversário de sofrer uma retaliação inaceitável (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022).

Neste contexto de disparidade de poder, questiona-se o real impacto do *name and shame* (nomear e constranger) diplomático. Autores como Egloff e Smeets (2023) advertem que a condenação pública possui limitações severas, pois certos atores — como autocracias isoladas, grupos terroristas ou redes criminosas transnacionais — "podem ser nomeados, mas não envergonhados", já que são insensíveis a danos reputacionais. Se o Estado ofensor não teme o desgaste de sua imagem nos fóruns internacionais, e se o Estado vítima não detém poder de fogo (econômico ou militar) para puni-lo, a mera denúncia diplomática torna-se inócua e falha em gerar dissuasão crível (LIBICKI, 2009; EGLOFF; SMEETS, 2023).

É precisamente na tentativa de equilibrar essas balanças assimétricas que a ciberdiplomacia se torna vital, indo muito além do mero repúdio retórico. A atribuição

cibernética, não é apenas um fato técnico de laboratório, mas um ato político-diplomático estratégico (RID; BUCHANAN, 2015). Para potências médias como o Brasil, a explicitação diplomática documentada não substitui os mísseis ou as armas cibernéticas de uma superpotência, mas atua como o gatilho jurídico que viabiliza a retaliação cruzada (*cross-domain deterrence*) e o mecanismo de emaranhamento (*entanglement*) (NYE JR., 2017). Ao transformar a evidência técnica em denúncia oficial amparada pelo Direito Internacional, a ciberdiplomacia legitima a imposição de sanções econômicas, embargos tecnológicos e a mobilização de sanções coletivas por parte de aliados (GARCIA, 2025). Dessa forma, a diplomacia busca artificialmente elevar os custos do agressor, utilizando as engrenagens de interdependência do sistema internacional para compensar as deficiências nas capacidades mútuas de defesa.

Brotherhood (2024) destaca que o papel da diplomacia brasileira nas Nações Unidas tem sido o de promover normas que reduzam a ambiguidade e aumentem a previsibilidade no comportamento dos Estados. Ao transpor os subsídios técnicos da inteligência cibernética para o campo normativo internacional, o Itamaraty busca estruturar a sua capacidade de exercer o que se pode chamar de "poder de atribuição". Ao contrário de grandes potências que utilizam a atribuição unilateral constantemente como ferramenta de pressão geopolítica, a postura brasileira tem sido pautada pela prudência, pelo respeito ao devido processo e à exigência de evidências verificáveis antes de qualquer condenação pública (GARCIA, 2025; MARTINS, 2025).

A ciberdiplomacia brasileira, portanto, encontra-se em um processo de consolidação e amadurecimento institucional (HUREL, 2022). Ela deixou de ser um tópico acessório da política externa para se tornar um pilar central da segurança nacional; contudo, sua governança interna ainda enfrenta os desafios da descentralização operacional entre o Ministério da Defesa, o Gabinete de Segurança Institucional e o Ministério das Relações Exteriores (BROTHERHOOD, 2024). O desafio que se impõe, e que será explorado nos capítulos subsequentes, é como essa estrutura diplomática pode aprimorar sua coordenação para operacionalizar a atribuição política de forma a elevar o custo reputacional de agressores e, consequentemente, fortalecer a dissuasão não cinética. Como aponta a hipótese deste trabalho, a institucionalização desse processo pelo Itamaraty é a chave para mitigar a impunidade (EGLOFF; SMEETS, 2023), uma vez que a arquitetura anônima do ciberespaço dificulta a

erradicação total das ameaças (LIBICKI, 2009), mas a denúncia fundamentada atua como um mecanismo limitador capaz de impor severo ônus aos atores maliciosos.

É importante notar que ainda não há exemplos empíricos documentados de atores que atacaram o Brasil, não ficaram impunes e foram subsequentemente dissuadidos de continuar suas ações ofensivas de forma direta por conta de uma retaliação ou punição diplomática brasileira. A presente pesquisa não ignora que a demonstração factual de que as atribuições em fóruns diplomáticos resultam em um aumento mensurável da capacidade dissuasória ou que a redução direta de ataques contra o Brasil ainda é um tema de difícil comprovação empírica. Os exemplos práticos de dissuasão diplomática e imposição de custos citados na literatura analisada referem-se a outras potências, a título de exemplo, as sanções coletivas aplicadas pela União Europeia (por meio do *Cyber Diplomacy Toolbox*) e o acordo de cessação de espionagem industrial entre Estados Unidos e China em 2015 (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022; EGLOFF; SMEETS, 2023).

A ausência de exemplos de punição diplomática direta deve-se também à forma como o Estado brasileiro enquadra institucionalmente as ameaças digitais. A literatura destaca que o Brasil, historicamente, tende a tratar a maioria dos ciberataques que sofre — a exemplo das graves invasões de *ransomware* ocorridas recentemente contra o Superior Tribunal de Justiça (STJ) e o aplicativo ConectaSUS, além de vazamentos massivos de dados de milhões de cidadãos — primariamente como questões criminais e de segurança pública (HUREL, 2022).

Consequentemente, a resposta nacional frente a esses incidentes tem sido focada na investigação policial e na cooperação penal internacional (como a adesão à Convenção de Budapeste sobre o Cibercrime), e não em atos de retaliação estatal. A ciberdiplomacia brasileira, até o presente, tem se voltado muito mais para a construção de consensos e normas em fóruns multilaterais do que para a imposição unilateral de punições e custos reputacionais a potências agressoras para fins de dissuasão coercitiva (HUREL, 2022; MARTINS, 2025).

A maturidade da ciberdiplomacia brasileira é uma resposta deliberada à complexificação das fronteiras clássicas de segurança. O país, que tradicionalmente priorizava a governança multissetorial da internet (o modelo *multistakeholder*), viu-se obrigado a amadurecer sua visão sobre a aplicação do Direito Internacional em operações cibernéticas para salvaguardar sua soberania.

O Pilar Jurídico: A Posição Nacional de 2021

O documento *Position of Brazil on International Law Applicable to Cyber Operations,* submetido oficialmente pelo Brasil à ONU em 2021, rompe com ambiguidades passadas. O Itamaraty sustenta que o princípio da soberania no ciberespaço é uma norma autônoma do Direito Internacional. Contudo, é vital pontuar uma distinção jurídica: uma violação da infraestrutura digital estatal não constitui automaticamente um *casus belli* (motivo para guerra) ou um "ataque armado" nos termos do Artigo 51 da Carta da ONU. Trata-se, na vasta maioria dos casos, de um ato internacionalmente ilícito (violação da integridade ou da não intervenção) que gera responsabilização e permite a adoção de contramedidas proporcionais, mas não o uso da força cinética (SCHMITT, 2017).

Diferente de potências hegemônicas como o Reino Unido e os Estados Unidos — que tendem a interpretar a soberania no ciberespaço com certa margem de ambiguidade, tratando-a muitas vezes apenas como um "valor" ou "princípio orientador" em vez de uma regra autônoma que proíba condutas cibernéticas específicas (GARCIA, 2025; HUREL, 2022; MAČÁK; DIAS; KASPER, 2025) —, a diplomacia brasileira defende que uma invasão à infraestrutura digital em solo nacional constitui uma violação direta da integridade territorial. Essa distinção é crucial para a presente pesquisa: ao firmar a soberania como uma norma primária, sua violação configura um ato internacionalmente ilícito que gera responsabilidade internacional e permite à nação vítima a adoção de contramedidas proporcionais para cessar o dano.

Conforme os parâmetros consolidados pelo Manual de Tallinn 2.0, uma operação cibernética só é equiparada a um ataque armado se as suas consequências causarem danos físicos substanciais, perda de vidas humanas ou a destruição catastrófica de infraestruturas críticas, assemelhando-se aos efeitos cinéticos de um bombardeio militar convencional (SCHMITT, 2017). A imensa maioria das ofensivas no ciberespaço, como o roubo de dados, a espionagem e as interrupções de sistemas, permanece abaixo desse limiar letal. Portanto, a força cibernética e a disrupção tecnológica exigem que o Direito Internacional seja interpretado de forma a evitar lacunas de impunidade diante dessas agressões cotidianas. Ao consolidar a violação de soberania como um ilícito passível de responsabilização, o Brasil garante que o princípio da não intervenção em assuntos internos seja respeitado e punido adequadamente através da ciberdiplomacia e de sanções não cinéticas, sem a necessidade de deflagrar uma guerra (HUREL, 2022).

Ainda, o Brasil destaca a relevância jurídica do conceito de Diligência Devida (do inglês, *Due Diligence*) para a responsabilização no ciberespaço, segundo o documento *Position of Brazil on International Law Applicable to Cyber Operations*, constatando que os Estados têm a obrigação internacional de não permitir conscientemente que a sua infraestrutura ou o seu território sejam utilizados para a prática de atos cibernéticos ilícitos que violem os direitos e a soberania de outros Estados (BRASIL, 2021).

Essa postura nacional de exigir responsabilidade pela omissão alinha-se aos parâmetros jurídicos expostos no *Tallinn Manual 2.0* (SCHMITT, 2017). Contudo, o Estado brasileiro mantém uma estrita cautela diplomática ao não aceitar e não incorporar automaticamente todas as interpretações de manuais produzidos por centros de excelência ligados à Organização do Tratado do Atlântico Norte (OTAN). Em vez de aderir passivamente a doutrinas formuladas por potências militares hegemônicas, a ciberdiplomacia brasileira prefere pautar-se pelo Direito Internacional e privilegiar a negociação de um consenso normativo multilateral, transparente e de caráter universal no âmbito da própria ONU (MARTINS, 2025).

O Pilar Estratégico: A E-Ciber e a Dissuasão

A recém-lançada Estratégia Nacional de Cibersegurança (E-Ciber) consolida a cibersegurança como um esforço coordenado pelo Estado (BRASIL, 2025). Embora categorizar diretrizes como "políticas de Estado" em detrimento de "políticas de governo" seja um recurso retórico que muitas vezes camufla os interesses internos de burocracias específicas, a E-Ciber sinaliza a intenção de criar fluxos perenes de respostas a incidentes e de cooperação internacional, exigindo constante avaliação crítica de sua execução.

Um ponto nevrálgico desse escopo é o reconhecimento da necessidade de elevação do custo reputacional e operacional de atores maliciosos. Isso toca diretamente na hipótese da presente pesquisa. A dissuasão, na era digital, raramente se dá pela ameaça de uso da força física (dissuasão por retaliação cinética), mas sim pela dissuasão por punição diplomática e econômica. No ciberespaço, a credibilidade da punição depende intrinsecamente da capacidade de atribuição.

Conforme argumenta Morgan (2003), apoiado pela lógica clássica da dissuasão, o agressor só recua se acreditar que a identificação e a punição são críveis e prováveis. No sistema internacional contemporâneo, a confiança digital é a "moeda" que viabiliza acordos comerciais,

transferências tecnológicas e tratados diplomáticos. Ser publicamente e tecnicamente identificado pelo Itamaraty como um Estado que abriga ou patrocina ciberataques possibilitaria a imposição de restrições diretas em fóruns de comércio e governança.

Nota-se, ademais, que a dissuasão focada no *name and shame* (nomear e envergonhar) diplomático, visa primariamente Estados adversários, serviços de inteligência estrangeiros e grupos patrocinados por governos (*Advanced Persistent Threats* – APTs). Para cibercriminosos comuns movidos por lucro, a dissuasão opera pelo sistema de justiça penal e extradição (ONU, 2024).

A E-Ciber 2025 inova ao prever mecanismos de cooperação internacional para o compartilhamento de subsídios técnicos que facilitem a identificação de vetores de ataque. Para a ciberdiplomacia brasileira, isso significa que o Itamaraty passa a ter um papel ativo na "tradutibilidade" do dado técnico em discurso diplomático. Brotherhood (2024) enfatiza que a normatização do ciberespaço nas Nações Unidas, defendida pelo Brasil, visa justamente criar um ambiente onde a atribuição não seja um ato unilateral e arbitrário de grandes potências, mas um processo fundamentado em normas de comportamento estatal responsável.

Em suma, a ciberdiplomacia é o veículo para a dissuasão cibernética do Brasil; contudo, para que o País seja efetivo em alterar a conduta de adversários geopolíticos, a diplomacia brasileira depende da superação analítica e política do dilema da atribuição.

O Nexo Atribuição-Dissuasão

No atual cenário de hiperconectividade, a eficácia da defesa cibernética de um Estado depara-se com o persistente desafio do anonimato. A arquitetura descentralizada do ciberespaço gera um ambiente propício para ameaças de natureza intrinsecamente transnacional. Diferentemente dos conflitos internacionais clássicos, que ocorrem primordialmente entre forças armadas regulares de Estados-nações, as ameaças cibernéticas transnacionais envolvem o cruzamento imperceptível de fronteiras jurisdicionais por atores não estatais — tais como corporações mercenárias, grupos criminosos e agentes interpostos (*proxies*), como intermediários do conflito “nas sombras”. Estes atores operam sob o manto da ambiguidade técnica, sendo frequentemente financiados ou tolerados por governos estrangeiros para garantir

a "negação plausível" e evitar a responsabilização direta perante a comunidade global (TSAGOURIAS; FARRELL, 2020).

É diante desta incerteza estrutural que a atribuição institucional de operações cibernéticas por parte do Itamaraty torna-se um mecanismo indispensável para a política de defesa. No entanto, emerge um questionamento estratégico natural: em que medida a publicização de fatos verificáveis em fóruns diplomáticos favorece concretamente a defesa cibernética nacional? E, de forma ainda mais crítica, como o reconhecimento público e documentado de um ataque perpetrado por uma grande potência ajudaria o Brasil a retaliar e dissuadir novas agressões, dada a assimetria de capacidades ofensivas?

A resposta para essa indagação reside na necessária readequação do conceito clássico de dissuasão para as dinâmicas do domínio digital. A essência da dissuasão consiste em convencer um adversário a abster-se de uma ação indesejada através da ameaça de uma punição severa (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022). Contudo, no ciberespaço, a retaliação cinética imediata — como um bombardeio militar contra a infraestrutura física do agressor — é uma medida rara, desproporcional e de altíssimo risco de escalada bélica (NYE JR., 2017). Dessa forma, a dissuasão cibernética crível não depende do uso da força militar ou de ataques de força bruta recíprocos; ela opera pela imposição de substanciais custos diplomáticos, reputacionais e econômicos, como já foi comentado ao longo da pesquisa.

Ao institucionalizar o *name and shame* amparado em sólidas evidências forenses e inteligência, a ciberdiplomacia afeta diretamente os interesses globais do agressor. No sistema internacional contemporâneo, a confiança digital é essencial. Ser publicamente identificado e tecnicamente atrelado a um ciberataque corrói a credibilidade do Estado infrator, restringindo o seu *soft power* e dificultando a celebração de acordos comerciais, transferências tecnológicas e parcerias em fóruns multilaterais (EGLOFF; SMEETS, 2023).

A capacidade de converter o dado técnico-militar em uma narrativa política ampara-se no amadurecimento daquilo que a literatura especializada denomina como 'diplomacia de defesa'. Conforme conceituado por Silva, A. (2015), a diplomacia de defesa consiste na institucionalização de práticas sociais e estatais que utilizam os recursos tangíveis e intangíveis das Forças Armadas de forma estritamente não coercitiva nas relações internacionais. Embora o aparato militar (como os centros de inteligência e defesa cibernética) seja classicamente

associado ao uso da força, a sua expertise técnica possui uma utilidade diplomática inestimável em tempos de paz (SILVA, A., 2015). Transpondo esse conceito para o quinto domínio, a atuação coordenada entre o ComDCiber e a DCiber do Itamaraty materializa a diplomacia de defesa cibernética na sua forma mais pura: o Estado utiliza um recurso de inteligência militar (a perícia forense que rastreia a origem de um ciberataque) não para iniciar um conflito armado, mas como o alicerce probatório pacífico que fundamentará a denúncia diplomática, a negociação multilateral ou a imposição de sanções, projetando os interesses de segurança do Brasil sem recorrer à coerção bélica.

Adicionalmente, a explicitação inequívoca e documentada da autoria do ataque cumpre um papel jurídico fundamental na ordem global. A atribuição pública formal fornece a materialidade e a base legal exigidas pelo Direito Internacional para que o Estado vítima possa aplicar, de forma legítima, sanções econômicas e contramedidas diplomáticas contra o Estado patrocinador da agressão (SCHMITT, 2017). Portanto, a publicização institucional não representa uma assunção de vulnerabilidade, mas o exercício prático de uma salvaguarda jurídica que rompe com a impunidade gerada pelo anonimato. Essa postura eleva sistematicamente o ônus de longo prazo para o agressor, desestruturando o seu cálculo de custo-benefício e conferindo credibilidade à dissuasão brasileira, independentemente da superioridade bélica do adversário (GARCIA, 2025).

A trajetória do Brasil, marcada pela transição de uma postura estritamente voltada à governança multissetorial para uma visão de segurança estratégica, reflete a compreensão de que o ciberespaço é um território de competição geopolítica. Conforme evidenciado, o posicionamento brasileiro de 2021 sobre a aplicação do Direito Internacional e a recente E-Ciber (2025) formam um arcabouço sólido que sustenta a interpretação da soberania como norma vinculante. Como destaca Martins (2025), o país atua como um mediador normativo, defendendo que o ciberespaço não é um "vácuo jurídico", mas um espaço sujeito às responsabilidades do sistema internacional.

Todavia, a eficácia das normas internacionais e da própria E-Ciber depende da capacidade do Estado em converter princípios abstratos em ações dissuasórias concretas. A dissuasão cibernética, conforme discutido, não opera sob a lógica bélica de destruição mútua assegurada que marcou a Guerra Fria, mas fundamenta-se estritamente na lógica racional do cálculo de custo-benefício. Para compreender a dinâmica desse cálculo, é imperativo recorrer à

filosofia do direito e à teoria utilitarista no enfrentamento da criminalidade, consolidada a partir das formulações de pensadores como John Stuart Mill. Segundo essa matriz teórica, corroborada pelos estudos contemporâneos de punição legal, o verdadeiro poder dissuasório de uma sanção contra condutas transgressoras não reside na severidade extrema ou no nível de força física da retaliação, mas fundamentalmente na certeza inabalável da descoberta e na inevitabilidade da punição (ALTMAN, 2021; LIPPKE, 2024).

No ambiente cibernético, essa premissa filosófica assume uma dimensão crítica, pois a principal arma tática de um ator malicioso é a expectativa do anonimato. Se a impunidade e a invisibilidade são percebidas pelo agressor como regras incontornáveis, a ameaça da mais violenta das retaliações perde o seu valor coercitivo e falha em coibir a ofensa (LIBICKI, 2009). Portanto, para que o Brasil possa, de fato, alterar o cálculo do adversário, elevar o custo reputacional das agressões e reduzir sistemicamente a impunidade transnacional, a ciberdiplomacia deve dominar a capacidade e o processo de apontar inequivocamente o agressor. Como ressalta Morgan (2003), a tentativa de estabelecer dissuasão sem a capacidade de identificar o perpetrador é inócua; é apenas através da certeza da revelação da autoria — a essência do instrumento de atribuição — que o véu do anonimato é destruído e o custo político de uma agressão torna-se inaceitável.

Em suma, mesmo a ciberdiplomacia fornecendo as ferramentas políticas, enfrenta o dilema da atribuição. Enquanto o Itamaraty possui a autoridade para proferir condenações e aplicar sanções diplomáticas, a produção de provas técnicas e a decisão política de "romper o silêncio" permanecem desafios complexos. Este capítulo estabeleceu que a ciberdiplomacia é o veículo para a dissuasão; contudo, para que esse veículo se mova, é preciso desvendar os mecanismos técnicos e políticos que permitem identificar a verdadeira autoria das operações.

Dessa forma, os fundamentos aqui expostos preparam o terreno para a investigação subsequente. No próximo capítulo, serão explorados os dilemas e desafios da atribuição em operações cibernéticas, diferenciando o que é tecnicamente verificável do que é politicamente comunicável, e como essa distinção impacta a segurança cibernética brasileira.

CAPÍTULO 2 - ATRIBUIÇÃO EM OPERAÇÕES CIBERNÉTICAS

A arquitetura original da rede mundial de computadores foi projetada com foco na resiliência e no compartilhamento descentralizado de informações, negligenciando mecanismos nativos de segurança ou de identificação inequívoca de seus usuários. Nas relações internacionais, essa característica de engenharia traduz-se no "problema da atribuição", um dos maiores obstáculos para a estabilidade internacional.

É imperativo ressaltar que esse problema transcende a infraestrutura lógica da internet. Conforme discutido anteriormente, o domínio cibernético abarca todo o espectro eletromagnético, as camadas físicas de cabos e servidores, além dos protocolos lógicos de rede (BRASIL, 2023). Portanto, quando uma operação maliciosa é executada, o agressor se aproveita das vulnerabilidades estruturais de todo esse ecossistema cibernético, operando sob camadas complexas de ofuscação, servidores *proxy* e operações de bandeira falsa (*false flags*) para apagar seus rastros físicos e lógicos, diferenciando-se radicalmente das trajetórias balísticas ou térmicas facilmente rastreáveis do domínio bélico tradicional.

Este capítulo investiga o processo de atribuição em duas dimensões fundamentais: a técnico-forense e a político-diplomática. Argumenta-se que a atribuição não é um evento binário, mas sim um processo cumulativo de construção de evidências e convicção política. A análise foca em como a incerteza inerente ao domínio cibernético desafia os conceitos tradicionais de responsabilidade estatal e como o Brasil navega entre a necessidade de identificar agressores e a complexa decisão estratégica de proferir acusações formais.

2.1 Dimensões da Atribuição: Da Perícia Técnica à Decisão Política

A atribuição de uma operação cibernética é um exercício multidisciplinar que exige a convergência de inteligência de sinais, perícia forense e análise geopolítica. Conforme a definição estritamente técnica, a atribuição resume-se ao processo de determinar a identidade ou a localização do autor de uma operação cibernética maliciosa (SHELDON, 2024). Contudo, no âmbito da segurança internacional, essa conceituação puramente computacional mostra-se insuficiente.

Para estruturar esse entendimento, Rid e Buchanan (2015) propõem que a arte da atribuição deve ser compreendida e desmembrada em três níveis interdependentes: o tático

(focado no código e artefatos digitais), o operacional (focado na infraestrutura utilizada) e o estratégico (focado nas motivações e no autor intelectual por trás do ataque).

No nível tático, a análise forense debruça-se sobre os artefatos digitais deixados pelo invasor, o que engloba assinaturas de *malware*, metadados de arquivos e o mapeamento de Táticas, Técnicas e Procedimentos (TTPs). Entretanto, a confiança exclusiva no código apresenta severos riscos analíticos. Bibliotecas de programação podem ser livremente compartilhadas na rede e grupos de hackers copiam deliberadamente o estilo de outros atores para desviar investigações. As revelações históricas trazidas a público pelo WikiLeaks, a título de exemplo, demonstraram textualmente como agências de inteligência governamentais possuem capacidades avançadas para emular o "rastro digital" de outros países com o objetivo explícito de confundir os analistas internacionais (VELANDIA, 2017).

O nível operacional investiga a infraestrutura empregada no ataque, tais como servidores de Comando e Controle (C2), servidores maliciosos utilizados em ataques cibernéticos para controlar remotamente sistemas previamente comprometidos. É neste estágio que a ciberdiplomacia passa a ser requisitada, visto que a investigação frequentemente exige a cooperação de outros Estados para o acesso a *logs* de provedores de internet estrangeiros. O entrave reside no fato de que a obtenção de muitos desses dados depende de acordos de cooperação jurídica internacional, cujos trâmites burocráticos são substancialmente mais lentos do que a velocidade em que ocorrem as operações digitais.

Finalmente, a atribuição estratégica — que define o "quem" e o "porquê" — constitui um ato eminentemente político (RID; BUCHANAN, 2015). Embora a capacidade técnica e política de atribuir uma autoria seja desejável para a defesa nacional, a centralização desse anúncio pelo Itamaraty deve ser avaliada criticamente. A produção da prova técnica bruta depende de órgãos de inteligência e defesa, como o ComDCiber e o GSI, cabendo ao Itamaraty a filtragem e a posterior tradução jurídica e política desse dado (BROTHERHOOD, 2024).

Ademais, emerge mais um dilema estratégico fundamental: nem sempre será do interesse do país atacado publicizar a agressão sofrida. O Estado vítima deve realizar um cálculo rigoroso de custo-benefício. Em muitos cenários, a publicidade de um ataque exige a exposição indesejada das próprias brechas de segurança e vulnerabilidades estruturais que foram exploradas pelo agressor, o que poderia convidar novos atores maliciosos a explorarem as

mesmas falhas. Optar pelo silêncio estratégico pode ser necessário para proteger fontes de inteligência, fechar as vulnerabilidades internamente ou evitar uma escalada indesejada de tensões políticas.

Dessa forma, a atribuição no plano internacional funciona através de um modelo onde as decisões de divulgação são instrumentalizadas estrategicamente pelos governos (EGLOFF; SMEETS, 2023). A participação de atores não estatais, como empresas privadas de cibersegurança que proferem atribuições públicas céleres motivadas por interesses comerciais ou de visibilidade mercadológica, deve ser filtrada com cautela pela ciberdiplomacia, garantindo que a voz oficial do Estado brasileiro guie-se apenas por fatos verificáveis e pelo estrito interesse soberano (GARCIA, 2025).

Em resposta ao compreensível dilema da publicização, é válido reconhecer que nem sempre será do interesse imediato do Estado atacado romper o silêncio, especialmente pelo temor de que a denúncia revele aos adversários as brechas e vulnerabilidades sistêmicas que foram exploradas. Contudo, a literatura estratégica mais recente demonstra que o Estado possui soberania sobre a "modulação da transparência". O ato de publicização ou *name and shame* não exige que o governo invadido publique o seu código-fonte ou comprometa as metodologias de suas agências de inteligência (EGLOFF; SMEETS, 2023). A praxe diplomática moderna permite a liberação de relatórios estilizados, expondo apenas Indicadores de Comprometimento (IoCs) genéricos ou amparando-se no endosso probatório de empresas privadas de segurança transnacionais. Por outro lado, o silêncio crônico e a negação sistêmica instituem um perigoso "vácuo de dissuasão", barateando o custo do ataque para o ofensor, que passa a se beneficiar da certeza absoluta da impunidade (LIBICKI, 2009).

É importante relembrar que a explicitação e o reconhecimento público do ataque não são atos de repúdio vazios, mas o alicerce jurídico e normativo primário que legitima o Estado vítima e seus aliados a aplicarem contramedidas severas. A efetividade empírica e fática dessa premissa é observável em casos recentes onde a atribuição, em si mesma, desencadeou efeitos dissuasórios expressivos e a contenção do agressor. Um caso paradigmático ocorreu no embate entre os Estados Unidos e a China (2014-2015): após o roubo massivo de dados do *Office of Personnel Management* (OPM), atribuído a hackers ligados ao exército chinês, os EUA não recorreram a contra-ataques físicos ou cibernéticos destrutivos. Em vez disso, utilizaram a firme atribuição pública aliada à ameaça diplomática e jurídica de impor amplas sanções econômicas

(retaliação cruzada). O risco real ao prestígio comercial chinês e a elevação dos custos reputacionais levaram à assinatura do Acordo Bilateral de 2015, o que resultou em uma queda documentada nas campanhas de espionagem comercial do país nos anos subsequentes (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022; EGLOFF; SMEETS, 2023).

Similarmente, a União Europeia tem demonstrado a materialidade dessa estratégia por meio do *Cyber Diplomacy Toolbox*. Utilizando fóruns e acordos diplomáticos, a UE operacionalizou a atribuição coletiva e oficial para impor medidas punitivas severas — como o congelamento de fundos e ativos e restrições de viagem — contra entidades norte-coreanas, chinesas e a cúpula do GRU, o serviço de inteligência russo, responsáveis por ciberataques globais como o *WannaCry* e o *NotPetya* (KASPER; OSULA; MOLNÁR, 2021; SERRANO, 2022). Tais constatações fáticas evidenciam que a diplomacia fundamentada na atribuição não depende de paridade bélica para exercer retaliação; ela detém o poder autônomo de isolar atores ofensores e paralisar seus interesses sistêmicos, produzindo a dissuasão coercitiva no século XXI.

2.2 O Dilema da Prova e a Responsabilidade Internacional no Ciberespaço

A atribuição política carrega um severo ônus probatório. No cenário internacional, uma acusação formal de agressão cibernética exige um padrão de evidência robusto o suficiente para convencer a comunidade internacional e legitimar eventuais respostas diplomáticas ou jurídicas. Por essa razão, o Brasil atua como um defensor rigoroso de que qualquer atribuição de responsabilidade internacional deve ser devidamente fundamentada em fatos verificáveis (BRASIL, 2021). Esse rigorismo jurídico visa a prevenir que o mecanismo de atribuição seja utilizado de maneira arbitrária ou politizada como ferramenta de coerção unilateral por parte de potências hegemônicas.

O dilema da prova agrava-se sensivelmente com o uso generalizado de intermediários (*proxies*). Estados frequentemente utilizam grupos cibercriminosos descentralizados ou indivíduos terceirizados para executar suas operações táticas, o que lhes garante o que a literatura denomina "negação plausível" (*plausible deniability*). Nesses cenários, o Direito Internacional enfrenta o complexo desafio de estabelecer o nexo de controle efetivo. Segundo

os parâmetros discutidos no âmbito do *Tallinn Manual 2.0*, um Estado só é juridicamente responsável por uma operação cibernética se esta for conduzida diretamente por seus órgãos oficiais ou por pessoas agindo sob suas instruções escritas, direção ou controle estrito (SCHMITT, 2017). Provar esse nexo de comando dentro de ambientes criptografados e redes descentralizadas é um elevado desafio técnico e probatório.

Para mitigar esse impasse estrutural, a postura diplomática brasileira oferece uma solução intermediária de elevado valor estratégico através da Diligência Devida. Conforme reiterado pelo Itamaraty na sua contribuição voluntária à ONU, os Estados têm a obrigação internacional de não permitir conscientemente que sua infraestrutura ou território sejam utilizados para a prática de atos ilícitos que violem os direitos de outros Estados (BRASIL, 2021).

Soma-se à premissa da Diligência Devida uma tática emergente e altamente pragmática para contornar as severas barreiras probatórias exigidas para responsabilizar formalmente governos estrangeiros: a 'dissuasão personalizada' (*personalised deterrence*). Desenvolvida por Braw e Brown (2020), essa estratégia argumenta que a ciberdiplomacia deve direcionar as sanções e a responsabilização de forma direta aos indivíduos e aos *proxies* que executam as operações em nome de Estados patrocinadores. A lógica central dessa abordagem reside na assimetria de interesses: enquanto um governo busca vantagens geopolíticas invisíveis, o hacker terceirizado geralmente anseia por benefícios pessoais, como retorno financeiro, estilo de vida e mobilidade internacional (BRAW; BROWN, 2020). Dessa forma, ao utilizar arranjos diplomáticos multilaterais e mecanismos jurídicos para impor proibições de viagens internacionais, banimentos do sistema financeiro global e o congelamento de ativos a esses operadores, o Estado vítima afeta drasticamente a realidade material do executor. Segundo Braw e Brown (2020), essa estratégia altera o cálculo de custo-benefício em nível pessoal e tem o potencial de criar uma fratura estrutural entre o *proxy* e o Estado patrocinador, uma vez que o indivíduo passa a questionar se o anonimato prometido pelo governo mandante compensa os severos custos impostos à sua própria liberdade civil e econômica no exterior.

Essa conceituação amplia significativamente o leque de atuação da defesa nacional: mesmo que o Brasil não consiga provar em tempo hábil que um governo estrangeiro ordenou ou desenhou um código de ataque, o País pode atribuir responsabilidade política e jurídica ao Estado de origem caso reste demonstrado que este, tendo sido notificado ou possuindo

conhecimento da atividade maliciosa partindo de seus servidores, omitiu-se e não adotou as medidas necessárias para cessá-la. A negligência estatal passa a ser, portanto, o fato gerador da responsabilidade política, alterando o cálculo de custo-benefício de governos que toleram cibercriminosos em suas jurisdições.

A ausência de uma norma global consensual sobre o padrão exato de prova necessário para a atribuição gera um persistente "vácuo de dissuasão" (LIBICKI, 2009). Diante disso, analisa-se criticamente se a conversão de subsídios técnicos em posicionamentos diplomáticos formais no Itamaraty possui o condão real de dissuadir agressões. A imposição de uma "sanção reputacional" imediata afeta o capital político e a inserção do agressor nas dinâmicas multilaterais (EGLOFF; SMEETS, 2023). Contudo, é preciso reconhecer os limites empíricos dessa premissa.

Mesmo sob uma estrutura burocrática ágil e consistente no Brasil, a demonstração factual de que atribuições em fóruns diplomáticos resultam em um aumento mensurável da capacidade dissuasória ou na redução direta do volume de ataques é um tema intensamente debatido e difícil de comprovar empiricamente. Conforme adverte Libicki (2019), a dissuasão no ciberespaço raramente opera de forma absoluta, pois os atores maliciosos tendem a reconfigurar suas táticas e migrar para técnicas de maior anonimato em vez de cessarem completamente suas hostilidades.

A utilidade fática da atribuição em fóruns diplomáticos e multilaterais, portanto, não reside na expectativa de interrupção instantânea e absoluta de todas as agressões. Seu valor estratégico repousa na consolidação progressiva de precedentes internacionais, na estigmatização de condutas irresponsáveis e na construção de um arcabouço jurídico que dê amparo legal legítimo para que o Brasil e seus aliados apliquem contramedidas políticas e econômicas proporcionais (SCHMITT, 2017). Ao retirar o ataque da invisibilidade técnica e inseri-lo no debate político internacional, o Estado brasileiro eleva *gradualmente* os custos geopolíticos de longo prazo dos seus agressores, pavimentando o caminho para a consolidação de normas globais de comportamento seguro, conforme será examinado a seguir.

Mesmo o Brasil defendendo historicamente que a atribuição de um ciberataque deve ser fundamentada em "fatos verificáveis", emerge aqui uma tensão inerente à segurança digital e às limitações da perícia forense: o tempo exigido para uma investigação robusta e para a

obtenção de *logs* via cooperação jurídica internacional é frequentemente incompatível com a necessidade de uma resposta imediata para fins de dissuasão. Essa barreira técnica agrava-se devido ao uso generalizado de *proxies*, *botnets* e ferramentas de ofuscação por parte de Estados ofensores, o que torna a comprovação irrefutável do nexo de controle direto (ou seja, provar que o governo estrangeiro ordenou ativamente a invasão) uma tarefa ímpar e morosa.

Conclui-se, portanto, que o dilema da atribuição é fundamentalmente um desafio de governança e de integração. A transição da evidência forense bruta para a condenação política exige uma estrutura burocrática ágil dentro do Itamaraty, capaz de dialogar ininterruptamente com os setores técnicos de defesa e inteligência (BROTHERHOOD, 2024). Contudo, a mera agilidade e consistência institucional interna não são suficientes para garantir, de forma automática, a proteção da infraestrutura crítica nacional. Para que a superação burocrática desse dilema se converta em dissuasão real, é imperativo que a atribuição diplomática resulte na imposição de custos concretos capazes de alterar o cálculo racional do agressor.

CAPÍTULO 3 - ATRIBUIÇÃO E CIBERDIPLOMACIA

A transição da incerteza técnica para a decisão política, discutida no capítulo anterior, culmina no uso da diplomacia como ferramenta de projeção de poder e proteção do Estado. Uma vez que o anonimato é a principal vantagem tática dos atores maliciosos no ciberespaço, a quebra desse véu de impunidade constitui o cerne da defesa cibernética moderna.

Este capítulo analisa o nexo entre a atribuição e o fortalecimento da capacidade dissuasória do Estado brasileiro. O questionamento central levantado ao longo desta pesquisa — sobre a eficácia de publicizar e denunciar ataques em fóruns multilaterais — é respondido por meio da análise de como a imposição de custos diplomáticos altera o cálculo racional do agressor. Por fim, confrontam-se essas necessidades estratégicas com as recentes diretrizes da E-Ciber, avaliando o papel do Itamaraty nesse novo modelo de governança.

3.1 A Atribuição como Instrumento de Dissuasão

A dissuasão no ciberespaço difere fundamentalmente da dissuasão nuclear típica da Guerra Fria. Enquanto a estabilidade estratégica do século XX baseava-se na ameaça letal e simétrica da "destruição mútua assegurada", a dissuasão cibernética moderna opera predominantemente por meio de mecanismos não cinéticos, destacando-se a dissuasão por negação (capacidade de defesa e resiliência de sistemas) e a dissuasão por punição (imposição de custos) (NYE JR., 2017). Conforme pontua a literatura especializada, a punição no ciberespaço raramente assume um caráter bélico destrutivo; ela estrutura-se na retaliação diplomática, em embargos econômicos e, acima de tudo, no desgaste reputacional sistêmico (LIBICKI, 2009).

Contudo, para compreender como essa promessa de punição adquire eficácia real perante o adversário, é necessário recorrer à Teoria da Punição Legal. Segundo as formulações de Altman (2021) e estudos contemporâneos similares sobre a filosofia do direito e o enfrentamento de transgressões (LIPPKE, 2024), a força dissuasória de uma sanção não reside no seu nível de severidade letal ou na violência da retaliação, mas fundamentalmente na certeza inabalável da descoberta e na inevitabilidade da punição. No domínio digital, a maior vantagem tática do ofensor é a expectativa do anonimato; se a impunidade e a negação plausível forem

percebidas como a regra, a ameaça de qualquer retaliação perde todo o seu valor coercitivo e falha em inibir a agressão.

Dessa forma, para o Brasil e outras potências, a capacidade de atribuir publicamente um ataque a um ator específico — seja ele um Estado ou um *proxy* a seu serviço — torna-se a peça fundamental que confere credibilidade à punição. Ao institucionalizar a atribuição e oficializar a denúncia, o Estado-vítima não apenas documenta a falha, mas também materializa a 'certeza da revelação' exigida pela teoria de Altman (2021). A publicização diplomática destrói o escudo de invisibilidade do agressor e impõe um severo custo de imagem imediato, atuando como o gatilho indispensável para que a dissuasão coercitiva funcione e altere, na prática, o cálculo de custo-benefício do adversário.

Para compreender a profundidade e a eficácia dessa deslegitimação, é necessário afastar a concepção tradicional de que a diplomacia atua exclusivamente na dimensão do *Soft Power* (poder brando de persuasão e atração). Conforme demonstrado por Favero (2025) em sua análise sobre a instrumentalização da ciberdiplomacia pelas grandes potências globais, a atuação diplomática no ciberespaço transcende o mero diálogo pacífico para consolidar-se como uma autêntica fonte de *Smart Power* (poder inteligente). O *Smart Power* caracteriza-se pela capacidade do Estado de conjugar e alternar dinamicamente recursos de atração com mecanismos de pressão e sanção (*Hard Power*) para atingir seus objetivos estratégicos (FAVERO, 2025). Dessa forma, quando o Estado instrumentaliza a ciberdiplomacia para realizar a atribuição oficial de um ataque, ele não está apenas emitindo uma nota de repúdio; ele está mobilizando uma estrutura de *Smart Power*. A denúncia diplomática identifica claramente o adversário, constrange suas alianças, afeta seus interesses econômicos e serve de base legal coercitiva para isolá-lo no sistema internacional. Portanto, a ciberdiplomacia, longe de ser um instrumento brando, atua como uma ferramenta enérgica de poder nacional capaz de reverter o cálculo de impunidade dos ofensores (FAVERO, 2025).

Embora a punição reputacional seja o pilar da dissuasão diplomática, sua eficácia varia conforme o grau de inserção do agressor na comunidade internacional. Enquanto, para Estados integrados às cadeias globais, a exposição pública (*name and shame*) gera custos econômicos e perda de confiança digital, atores que já operam sob isolamento diplomático podem ser menos sensíveis a tais custos. Assim, para o Brasil, a atribuição deve ser acompanhada de uma articulação em blocos (como o BRICS ou o Mercosul) para que a 'sanção de imagem' se

converta em custos tangíveis de isolamento em negociações multilaterais, elevando o cálculo de custo-benefício do agressor para além da simples impunidade técnica.

Diferente de potências hegemônicas que utilizam a atribuição de autoria de forma unilateral e, por vezes, politizada como ferramenta de pressão geopolítica, a ciberdiplomacia brasileira defende que a atribuição deve servir primordialmente ao fortalecimento do Direito Internacional. Na prática, essa posição significa rejeitar o chamado "justiceirismo digital" e a aplicação precipitada de sanções unilaterais baseadas em presunções (GARCIA, 2025). Significa, outrossim, que o Estado brasileiro subordina qualquer acusação à apresentação de "fatos verificáveis" e privilegia a resolução pacífica de controvérsias e a denúncia de ataques através de fóruns multilaterais legítimos, notadamente nos debates do GGE e do OEWG da ONU (BROTHERHOOD, 2024; MARTINS, 2025).

Essa visão não é apenas discursiva, mas uma política de Estado firmemente institucionalizada que pode ser verificada em documentos oficiais e manifestações diplomáticas. O principal marco documental é a submissão voluntária intitulada *Position of Brazil on International Law Applicable to Cyber Operations*, enviada à ONU em 2021, que formalizou o entendimento jurídico inédito do país de que a soberania é uma norma autônoma aplicável ao ciberespaço. Adicionalmente, essa mesma postura encontra-se ratificada nas sucessivas declarações orais e escritas da delegação brasileira nas sessões do OEWG entre 2020 e 2024 (MARTINS, 2025), bem como nas diretrizes da Estratégia Nacional de Segurança Cibernética (E-Ciber), que pautam a atuação internacional do país pela ênfase no multilateralismo e no respeito irrestrito ao direito internacional (BRASIL, 2020).

Nesses documentos, ao ancorar o processo de atribuição nos ditames do Direito Internacional, o Brasil sinaliza à comunidade global que invasões contra sua infraestrutura crítica — como o sistema financeiro ou a rede elétrica — não serão toleradas como meros incidentes técnicos. Pelo contrário, são categorizadas como atos internacionalmente ilícitos e violações diretas da integridade territorial e da soberania nacional, gerando o direito à reparação (BRASIL, 2021). Essa clareza normativa converte-se, por si só, em um mecanismo dissuasório essencial. Ao balizar a sua reação institucional em regras internacionais amplamente aceitas, o Brasil reduz a "zona cinzenta" e a negação plausível das quais os agressores transnacionais se valem para operar na impunidade, conferindo legitimidade absoluta para que o Estado vítima

adote contramedidas legais e imponha severos custos políticos, econômicos e diplomáticos aos ofensores (ARAÚJO LISBOA; ZIEBELL DE OLIVEIRA, 2022).

Ademais, a rejeição brasileira a posturas agressivas no ciberespaço — como os chamados contra-ataques ofensivos (*hack-backs*) ou a excessiva militarização do domínio digital — encontra profundo respaldo nas lições extraídas do próprio histórico de segurança pública na América Latina. Conforme demonstrado na análise regional de Rosen e Cutrona (2023), a adoção sistemática de políticas de *mano dura* (mão de ferro) para o enfrentamento de crises de segurança, caracterizadas pela hipermilitarização e pela resposta estritamente punitiva, revelou-se ineficaz, resultando frequentemente em ciclos incontroláveis de escalada da violência, violações de garantias institucionais e fortalecimento de redes criminais. Transportando essa constatação empírica para o quinto domínio, torna-se evidente por que a governança brasileira repudia o 'justiceirismo digital' e a ciberguerra como opções primárias. Da mesma forma que a *mano dura* falha domesticamente ao gerar danos colaterais imprevisíveis, uma postura de '*ciber-mano dura*' — calcada no revide técnico precipitado ou no uso da força fora dos parâmetros diplomáticos — aumentaria drasticamente o risco de instabilidade sistêmica e de erro de cálculo entre os Estados. Portanto, a opção do Brasil em privilegiar a ciberdiplomacia como canal oficial para a resolução de ciberataques evita os erros históricos do hiperpunitivismo físico, garantindo que a resposta nacional seja proporcional, focada no estrangulamento político do agressor e perfeitamente amparada pelo Direito Internacional (ROSEN; CUTRONA, 2023).

Para além do cálculo estrito de custos materiais, a eficácia da atribuição diplomática também se sustenta na função expressiva da sanção. Conforme a Teoria da Punição Legal aprofundada por Altman (2021), a imposição de um ônus a um transgressor — que no cenário internacional traduz-se pelo constrangimento diplomático e sanções não cinéticas — atua primordialmente como uma forma de 'comunicação moral'. Segundo o autor, o ato de punir expressa publicamente a condenação da comunidade contra a violação de uma norma e reafirma a validade inviolável dos direitos da vítima. Transpondo essa lógica para o domínio cibernético, o silêncio do Estado agredido sinaliza aquiescência e enfraquece o arcabouço normativo global. Em contrapartida, quando o Itamaraty realiza a atribuição pública de um ataque, ele exerce a função expressiva da ciberdiplomacia: condena formalmente o ilícito, reafirma a inviolabilidade da soberania brasileira e sinaliza aos demais atores do sistema internacional que

o País não tolerará a degradação de sua infraestrutura crítica. Essa comunicação moral é, portanto, um componente indispensável para a consolidação de tabus normativos e para o restabelecimento da ordem e da confiança prejudicadas pela agressão (ALTMAN, 2021).

Essa dimensão expressiva é aprofundada e complementada por Lippke (2024), que articula uma teoria mista da sanção em que o papel principal da punição legal é atuar como um instrumento de 'comunicação moral' ancorado na censura. Segundo o autor, embora a redução de danos futuros (dissuasão) desempenhe uma função instrumental incontestável na justificação das penas, a sanção existe primordialmente para responsabilizar os infratores por seus 'erros públicos'. Ao punir, o Estado censura o ofensor de maneira tangível e comunica à vítima e à comunidade que as normas de convivência são inegociáveis. Transpondo esse arcabouço filosófico para a ciberdiplomacia, nota-se que a atribuição de autoria pelo Itamaraty cumpre exatamente esse papel de censura internacional. Ao 'nomear e constranger' publicamente um Estado patrocinador de ataques cibernéticos, a diplomacia brasileira não está apenas buscando um cálculo utilitarista de redução de ataques futuros; ela está exercendo a sua autoridade para comunicar moral e juridicamente que uma norma basilar do sistema internacional foi violada. Esse ato de censura diplomática invalida a narrativa de impunidade do agressor e reafirma o compromisso do Brasil em proteger ativamente os direitos e as infraestruturas de seus cidadãos (LIPPKE, 2024).

Para que a atribuição diplomática seja compreendida em sua real dimensão estratégica, contudo, é necessário superar o anacronismo do pensamento militar tradicional. O ceticismo quanto à eficácia da ciberdiplomacia deriva frequentemente da tentativa falha de aplicar o conceito de 'dissuasão absoluta' — herança da ameaça nuclear da Guerra Fria — ao quinto domínio. Tor (2015) argumenta que há uma crise de paradigma nos estudos de segurança cibernética: ao contrário da era nuclear, onde o objetivo da dissuasão era evitar a eclosão de um único ataque catastrófico, no ciberespaço as intrusões de baixo e médio impacto são rotineiras e inevitáveis. Por essa razão, Tor (2015) propõe a substituição da lógica de negação absoluta pelo paradigma da 'dissuasão cumulativa' (*cumulative deterrence*). Sob essa nova ótica, a dissuasão não falha necessariamente quando um ataque ocorre; em vez disso, ela é construída e calibrada progressivamente através de respostas e retaliações consistentes ao longo do tempo, cujo objetivo é limitar, moldar e desgastar as intenções do adversário durante um conflito contínuo.

A adoção dessa flexibilidade cumulativa é particularmente vital para a proteção das infraestruturas críticas nacionais. Conforme adverte Wilner (2017), o estabelecimento de 'linhas vermelhas' (*red lines*) estáticas e inflexíveis é uma estratégia ineficaz na segurança cibernética, pois os agressores transnacionais testam continuamente os limites das defesas estatais na zona cinzenta. Ao adotar a dissuasão cumulativa, o Estado liberta-se da armadilha de ter que iniciar uma escalada militar imediata a cada rede invadida. A diplomacia, nesse contexto, atua de forma cirúrgica e iterativa: cada nota de repúdio do Itamaraty, cada exposição forense em fóruns internacionais e cada sanção articulada não visam a neutralização definitiva do oponente, mas funcionam como vitórias táticas que, somadas, encarecem a agressão repetidamente até que o custo-benefício de atacar o Brasil torne-se politicamente insustentável para o ofensor (TOR, 2015; WILNER, 2017).

Adicionalmente, a transição da resposta cibernética para o âmbito da política externa encontra amparo na necessidade crítica de se estabelecer um rigoroso controle de escalada (*escalation management*). Ao aprofundar a sua análise sobre a aplicação da dissuasão convencional ao ciberespaço, Fischerkeller (2017) alerta para o perigo estratégico de os Estados imporem a si mesmos limitações desnecessárias, presumindo equivocadamente que uma agressão inicial via ciberespaço restrinja a escolha das respostas subsequentes a esse mesmo domínio. Confinar a dissuasão a uma dinâmica reativa de 'ciber contra ciber' não apenas limita drasticamente o leque de retaliação do Estado vítima, como eleva o risco de uma escalada militar técnica cujos danos colaterais são altamente imprevisíveis. Nesse contexto, a atuação do Itamaraty funciona como uma válvula de segurança estratégica. Ao assumir a vanguarda do processo de atribuição, a diplomacia retira a exclusividade da resposta do domínio tático-militar e a eleva para a arena política. Isso viabiliza a retaliação cruzada, permitindo que o Brasil calibre a proporcionalidade de sua reação e imponha custos ao adversário por meio de instrumentos econômicos e diplomáticos, mitigando o risco de que um incidente digital deteriore rapidamente em um conflito cinético aberto (FISCHERKELLER, 2017).

Essa opção do Estado brasileiro por uma resposta não militarizada não deve ser interpretada como um sinal de fraqueza, mas sim como um alinhamento às tendências mais avançadas da segurança internacional, onde a práxis diplomática frequentemente precede a própria formulação teórica. Ao analisar a evolução da doutrina de cibersegurança de grandes potências, notadamente os Estados Unidos, Wilner (2019) demonstra que a teoria clássica de

'dissuasão por punição' — baseada na premissa de um revide bélico ou técnico direto — tornou-se insuficiente, sendo gradativamente substituída na prática pelo conceito de 'dissuasão por imposição de custos' (*deterrence by cost imposition*). Essa readequação conceitual reconhece formalmente a eficácia da dissuasão cruzada ou multidomínio (*cross-domain deterrence*). Ou seja, a retaliação a um ciberataque raramente se materializa na forma de um contra-ataque simétrico no próprio ciberespaço; a imposição de custos ocorre, invariavelmente, por meio da orquestração de instrumentos não cinéticos, englobando a denúncia oficial, processos de persecução penal, sanções financeiras severas e o isolamento comercial do agressor (WILNER, 2019). Evidencia-se, portanto, que a diplomacia não é um elemento acessório, mas o vetor operacional prioritário dessa doutrina: sem a atuação centralizadora do Itamaraty para coordenar a imposição política desses custos multidomínio, o Estado restringe-se a reparar passivamente as suas próprias redes, falhando de forma sistêmica em penalizar o atacante e em interromper o ciclo da agressão transnacional.

3.2 O Modelo Brasileiro: Entre a E-Ciber 2025 e a Prática Diplomática

O reconhecimento de que o ciberespaço é um domínio de conflito exigiu do Brasil a formulação de respostas institucionais coordenadas. Com a recente publicação da Estratégia Nacional de Cibersegurança, o País estabeleceu um arcabouço normativo que busca alinhar a defesa técnica à política externa.

A operacionalização da atribuição no Brasil encontra seu fundamento na E-Ciber de 2025. O nexo entre atribuição e ciberdiplomacia ocorre no momento em que a inteligência técnica é traduzida em linguagem jurídica e diplomática para ser levada a fóruns como o OEWG da ONU.

A E-Ciber 2025 inova ao propor a criação de protocolos de resposta a incidentes que incluem a dimensão internacional. Isso significa que o Brasil está construindo a capacidade de não apenas se defender (negação), mas de reagir no plano internacional (punição). A institucionalização desse processo pelo Itamaraty é o que garante a legitimidade da resposta. Como aponta Garcia (2025), o Brasil busca evitar o "justiceirismo digital", preferindo um

modelo onde a atribuição seja o prelúdio para consultas diplomáticas ou denúncias em organismos multilaterais.

Um desafio crítico para a ciberdiplomacia brasileira é a gestão das evidências em casos de ataques por atores não estatais sob patrocínio estrangeiro. A postura oficial brasileira, reforçada no documento de 2021 enviado à ONU, é de que a responsabilidade estatal é evocada sempre que um Estado falha em sua obrigação de "devida diligência" (BRASIL, 2021). Assim, a atribuição brasileira não foca apenas em "quem apertou o botão", mas em "quem permitiu que o botão fosse apertado" a partir de seu território, ou seja, não se limita aos executores diretos da ação, mas também aos atores estatais que se omitiram. Essa interpretação ampla do Direito Internacional amplia o leque de dissuasão do Brasil, pois coloca pressão sobre os Estados de origem para que monitorem e neutralizem grupos cibercriminosos em suas jurisdições.

A atribuição, portanto, deixa de ser um exercício de perícia digital para se consolidar como o ato soberano que viabiliza a estratégia de defesa nacional no ciberespaço. Ao romper o silêncio e oficializar a autoria de agressões, o Itamaraty não apenas busca a reparação de danos, mas reafirma a autoridade do Estado brasileiro sobre seu domínio virtual, transformando a fragilidade técnica do anonimato em uma oportunidade de afirmação normativa e dissuasão estratégica no cenário global.

Uma crítica frequente nos debates acadêmicos é a sobreposição de funções entre os órgãos estatais. Questiona-se, portanto, qual o papel exato do Ministério das Relações Exteriores frente à atuação do Comando de Defesa Cibernética (ComDCiber) e do Gabinete de Segurança Institucional (GSI). A literatura e a doutrina oficial esclarecem que as funções não são concorrentes, mas complementares (BRASIL, 2023).

Enquanto o ComDCiber e o GSI são responsáveis pela resposta a incidentes, pela coleta de inteligência forense e pela defesa das infraestruturas críticas (dissuasão por negação), o Itamaraty atua como a linha de frente da dissuasão por punição diplomática. A E-Ciber (BRASIL, 2025) reforça a necessidade de uma governança integrada. Quando a perícia técnica militar identifica a origem de uma ameaça, cabe à diplomacia avaliar a conveniência política de tornar essa informação pública ou de tratá-la em canais bilaterais sigilosos.

A consolidação dessa governança integrada, no entanto, exige a superação de obstáculos burocráticos profundos na estrutura do Estado brasileiro. A literatura sobre Relações

Internacionais e Estudos Estratégicos aponta historicamente para a fraca articulação entre o Ministério das Relações Exteriores e as Forças Armadas no Brasil. Conforme destaca Correia (2022), a política externa e o poder militar (defesa) desenvolveram-se no país como 'universos paralelos', operando frequentemente sem articulação mútua em virtude de distintas culturas organizacionais e de um prolongado isolacionismo institucional. Enquanto as agências de defesa focavam-se em um viés estritamente doméstico e securitário, a diplomacia monopolizou as funções de projeção externa (CORREIA, 2022). No âmbito das ameaças cibernéticas, a manutenção desse paralelismo é fatal para a capacidade de dissuasão. A estruturação preconizada pela E-Ciber e a necessidade de atribuição política exigem, de forma inédita, a reversão definitiva dessas trajetórias isoladas. Para que o Brasil se projete como uma potência cibernética capaz de defender seus interesses e impor custos aos seus adversários, é imperativo que o dado fático gerado pela perícia técnica do aparato militar de Defesa Cibernética e a narrativa jurídica formulada pelo Itamaraty convirjam em uma política de Estado uníssona, substituindo as lógicas corporativas isoladas por uma estratégia de dissuasão integrada (CORREIA, 2022).

Essa primazia conferida ao Itamaraty no processo de resposta e responsabilização cibernética não constitui um fenômeno isolado, mas reflete o amadurecimento de uma doutrina de Estado consolidada desde o fim da Guerra Fria. Ao analisar o debate sobre a segurança hemisférica e a reestruturação institucional brasileira na década de 1990, Pinto (2015) destaca que a primeira Política de Defesa Nacional (PDN), adotada em 1996 com forte envolvimento do corpo diplomático, já estabelecia o paradigma de que a vertente preventiva da defesa do país reside, primordialmente, na valorização da ação diplomática como instrumento primeiro de resolução de controvérsias. Assim, a atual delegação de poderes à ciberdiplomacia para orquestrar a atribuição de autoria não representa uma ruptura com as Forças Armadas, mas a transposição natural dessa doutrina histórica para o quinto domínio. Ao privilegiar a denúncia pública, as sanções e a negociação em foros multilaterais antes de qualquer cogitação de retaliação ofensiva, o Brasil mantém a coerência dos seus princípios de política externa e reforça a credibilidade e a previsibilidade de sua postura dissuasória no cenário internacional (PINTO, 2015).

A superação definitiva desse isolamento burocrático e a integração estabelecida pela nova Estratégia Nacional de Cibersegurança reforçam a premissa teórica de que militares e

diplomatas atuam como elementos indissociáveis na projeção da política externa e de defesa (SILVA, V., 2017). Historicamente, a forte especialização e as distintas culturas organizacionais — a vocação do Itamaraty para a acomodação pacífica e a vocação das Forças Armadas para a ação e a defesa — geraram um distanciamento e um monopólio de agendas em suas respectivas áreas de atuação (SILVA, V., 2017). Contudo, a complexidade transnacional do ciberespaço exige a fusão de ambas as expertises. Como argumenta Silva, V. (2017), o diplomata pode ter a primazia legal na condução da política externa, mas não detém a exclusividade sobre ela, necessitando intrinsecamente do conhecimento tático e operacional produzido pelas agências de defesa. É precisamente essa simbiose que legitima o modelo de dissuasão cibernética do Brasil: o perito militar (soldado cibernético) fornece a prova material irrefutável do ataque, enquanto o diplomata traduz essa prova em poder de persuasão e constrangimento internacional, unificando a defesa nacional e a política externa em um único instrumento de Estado frente às ameaças globais.

A institucionalização desse processo enfrenta desafios. A diplomacia brasileira historicamente pauta-se pelos princípios da não intervenção e da resolução pacífica de controvérsias (GARCIA, 2025). Diante disso, a adoção de posturas de atribuição pública acarreta uma quebra de paradigma na cultura do Itamaraty, que precisa equilibrar o uso assertivo da denúncia (*name and shame*) com a manutenção de seu *soft power* e de sua tradição mediadora.

A urgência dessa transição paradigmática — de uma abordagem reativa para uma política de Estado focada na dissuasão diplomática — é comprovada pela análise empírica dos graves incidentes recentes que atingiram o país. A partir de 2020, a infraestrutura crítica nacional foi alvo de algumas das piores agressões cibernéticas de sua história. Destacam-se os severos ataques de *ransomware* direcionados ao Superior Tribunal de Justiça (STJ) e a subsidiárias do setor nuclear, a invasão e o sequestro de dados do aplicativo ConectaSUS do Ministério da Saúde em meio à crise pandêmica, além de um vazamento massivo que expôs informações sensíveis de mais de 220 milhões de cidadãos (HUREL, 2022). Adicionalmente, durante as eleições municipais de novembro de 2020, o próprio Tribunal Superior Eleitoral (TSE) foi alvo de uma investida cibernética combinada a uma campanha de desinformação orquestrada para minar a integridade do processo democrático nacional (HUREL, 2022).

A impunidade verificada nesses episódios decorre diretamente da forma estrutural como o Estado enquadrou sua resposta. Historicamente, o Brasil tende a tratar a esmagadora maioria das intrusões transnacionais sob a ótica estritamente criminal e de segurança pública interna (HUREL, 2022). Ao restringir a resposta à investigação policial, o país esbarra nas intransponíveis limitações jurisdicionais do ambiente digital, uma vez que grupos criminosos frequentemente atuam como *proxies* ou encontram abrigo em Estados lenientes. Sem a elevação do incidente ao patamar geopolítico mediante a atribuição formal pelo Itamaraty balizada na premissa da Devida Diligência, os Estados que hospedam essas ameaças não sofrem sanções internacionais ou desgaste reputacional. Esses casos práticos atestam de forma cabal que a manutenção de uma abordagem meramente penal é ineficaz para alterar o cálculo de custo-benefício do atacante, confirmando a premissa de que a dissuasão crível exige a institucionalização do poder de responsabilização pela via diplomática.

Essa realidade de assimetria evidencia que, para os países fora do eixo hegemônico, a ciberdiplomacia transcende a mera representação política, configurando-se como um mecanismo vital de sobrevivência estatal. Ao analisarem os desafios de segurança cibernética em Moçambique, Cepik e Marcelino (2021) demonstram que as nações do Sul Global compartilham vulnerabilidades estruturais profundas, tais como a obsolescência de infraestruturas críticas, a escassez de profissionais especializados e a fragmentação institucional na governança do ciberespaço. Devido a essas limitações materiais severas, esses Estados tornam-se alvos atrativos, rentáveis e de baixíssimo risco tanto para a criminalidade transnacional quanto para operações de espionagem de potências estrangeiras, que se aproveitam do déficit de defesas locais para operar com a garantia da impunidade (CEPIK; MARCELINO, 2021).

Diante dessa crônica escassez de recursos para o exercício da dissuasão por negação (defesas técnicas impenetráveis) ou do uso da força ofensiva, a pesquisa de Cepik e Marcelino (2021) corrobora a tese de que a segurança dos países em desenvolvimento depende intrinsecamente da cooperação internacional e da construção de capacidades (*capacity building*). A mitigação dessas assimetrias exige a inserção ativa do Estado em regimes internacionais, a ratificação de tratados de assistência mútua e a articulação de respostas conjuntas. Sob essa ótica, a hipótese de que o Brasil deve instrumentalizar o Itamaraty para centralizar e proferir a atribuição política alinha-se perfeitamente à necessidade sistêmica do

Sul Global: é imperativo compensar as deficiências operacionais de defesa por meio da articulação normativa. Ao invocar o Direito Internacional e elevar os custos diplomáticos da agressão, o Estado transforma a diplomacia na sua principal e mais impactante linha de frente, estabelecendo uma dissuasão crível que independe da paridade tecnológica com o agressor.

O sucesso da ciberdiplomacia brasileira dependerá de sua capacidade de converter inteligência técnica em posicionamentos diplomáticos críveis e irrefutáveis. Ao fundamentar suas acusações rigorosamente no Direito Internacional (BRASIL, 2021; SCHMITT, 2017), o Brasil evita o uso banalizado e politizado da atribuição, consolidando sua imagem como um ator global responsável. Conclui-se que o modelo em consolidação no Brasil reconhece que a dissuasão não depende apenas de *firewalls* impenetráveis, mas da certeza imposta ao adversário de que sua identidade será revelada e que a agressão terá um alto custo político e econômico.

CONCLUSÃO

A pesquisa investigou um dos nexos prementes da segurança internacional contemporânea: a intersecção entre a ciberdiplomacia e a capacidade estatal de dissuasão estratégica, sob a ótica da política externa brasileira, liderada pelo Ministério das Relações Exteriores (Itamaraty). Diante do avanço exponencial de operações hostis no ciberespaço — domínio transversal que abarca não apenas a rede mundial de computadores, mas também todo o espectro eletromagnético e suas respectivas camadas físicas e lógicas (BRASIL, 2023) —, o problema central deste estudo consistiu em analisar de que maneira a institucionalização da atribuição política pelo Itamaraty fortaleceria a capacidade de dissuasão de ameaças cibernéticas transnacionais.

A hipótese levantada defendia que a conversão de subsídios técnicos em posicionamentos diplomáticos formais e acusações públicas rompe com a impunidade gerada pelo anonimato e eleva substancialmente o custo reputacional de atores maliciosos, alterando seu cálculo de custo-benefício e alinhando o Brasil à lógica da dissuasão pela punição. Ao término desta reconstrução analítica, conclui-se que a hipótese de trabalho foi corroborada pelas evidências disponíveis. Porém, por se tratar de uma interpretação, é preciso considerar sempre que os resultados da pesquisa são provisórios, tanto pela necessidade de estudos adicionais quanto pelo viés de confirmação que caracteriza estudos de natureza interpretativa e prescritiva.

Os objetivos específicos delineados na introdução foram alcançados. No primeiro capítulo, estabeleceu-se a distinção analítica precisa entre a diplomacia digital — entendida como o uso instrumental de plataformas e redes de tecnologia para a comunicação e consecução da política externa (FREY, 2024; GÓES, 2017) — e a ciberdiplomacia. Adotando a conceituação proposta por Attatfa, Renaud e De Paoli (2020) e Salvi, Tiirmaa-Klaar e Lewis (2024), consolidou-se a ciberdiplomacia como a vertente de segurança e regulação internacional em que o ciberespaço é o próprio objeto temático da agenda externa, superando leituras puramente focadas em governança multissetorial que seriam inócuas para dar suporte analítico a estratégias de defesa. Foi possível mapear, sob esse prisma, a evolução da postura brasileira, que transitou de uma atuação tradicional voltada à arquitetura civil da rede para uma firme afirmação normativa sobre a aplicabilidade do Direito Internacional (BRASIL, 2021; MARTINS, 2025).

No segundo capítulo, destrinchou-se o dilema da atribuição com base no modelo tripartido de Rid e Buchanan (2015), diferenciando as camadas técnicas (tática e operacional) e políticas (estratégica) da quebra do anonimato. Demonstrou-se que, enquanto a perícia forense busca traçar assinaturas de códigos e registros lógicos (SHELDON, 2024), a atribuição internacional é um ato eminentemente político e soberano, que exige ponderação de custos por parte do Estado vítima. Esclareceu-se que o silêncio estratégico pode ser preferível em cenários em que denunciar o ataque exporia vulnerabilidades críticas da infraestrutura digital interna ou comprometeria fontes sigilosas de inteligência (EGLOFF; SMEETS, 2023). Ademais, a pesquisa inovou ao destacar que o princípio da Diligência Devida (*Due Diligence*), contido na posição oficial brasileira de 2021, equaliza o fardo probatório: o Estado hospedeiro que conscientemente se omite em cessar ataques provenientes de seu território torna-se juridicamente responsável, contornando a dificuldade técnica de comprovar o controle estrito sobre intermediários descentralizados (*proxies*) e redes mercenárias (BRASIL, 2021; SCHMITT, 2017).

A partir do amparo teórico da dissuasão cibernética fundamentado em Nye Jr. (2017) e Araújo Lisboa e Ziebell de Oliveira (2022), as seções finais permitiram amadurecer algumas possíveis respostas críticas aos questionamentos, sintetizados em três grandes conclusões analíticas:

Primeiramente, delimitou-se o alvo e o escopo da dissuasão diplomática brasileira. O mecanismo de atribuição pública e a imposição de custos políticos e reputacionais não se destinam a criminosos comuns ou a grupos motivados exclusivamente por ganho financeiro; para esses agentes transnacionais menores, o desincentivo opera por meio do sistema clássico de repressão penal, cooperação policial e tratados de extradição (ONU, 2024). A dissuasão, com a participação do MRE, visa precipuamente Estados estrangeiros, seus braços de inteligência militar e grupos de ameaças persistentes avançadas (*Advanced Persistent Threats* — APTs) por eles patrocinados ou tolerados.

Em segundo lugar, desmistificou-se a eficácia do isolamento e das sanções reputacionais. Em um sistema internacional interconectado, o reconhecimento público de que um Estado viola as normas básicas de comportamento no ciberespaço acarreta consequências econômicas e políticas tangíveis. O "*name and shame*" diplomático corrói a confiança digital, elemento essencial para a celebração de parcerias de investimento, acordos comerciais

preferenciais e transferências de tecnologia sensível (GARCIA, 2025). Para o Brasil, proferir acusações formais fundamentadas em evidências sólidas não é um ato de revide cinético ou de retaliação bélica inviável contra superpotências, mas sim o exercício de salvaguarda jurídica autorizado pelo Direito Internacional que legitima a aplicação de contramedidas proporcionais, sanções financeiras e restrições multilaterais, forçando o agressor a recalcular os ganhos marginais de suas campanhas de ciberespionagem ou ciberguerra (EGLOFF; SMEETS, 2023; SCHMITT, 2017).

Por fim, reconheceu-se o limite analítico da teoria. A literatura contemporânea adverte que mensurar empiricamente o número de ataques evitados por uma postura diplomática assertiva é uma tarefa metodologicamente complexa, uma vez que o recuo do agressor raramente se manifesta como ausência completa de atividade, mas sim como uma alteração ou sofisticação de suas técnicas de camuflagem (LIBICKI, 2019). A utilidade da atribuição pelo Itamaraty, portanto, repousa na consolidação de precedentes estritos de comportamento no ciberespaço e no rompimento da negação plausível automática por parte dos agressores.

Para que essa engrenagem estratégica funcione com a tempestividade exigida pelas crises cibernéticas, a recém-lançada Estratégia Nacional de Cibersegurança (E-Ciber) de 2025 representa um avanço institucional necessário, mas requer vigilância contínua. O maior desafio nacional reside em aprimorar o fluxo de "tradutibilidade" burocrática entre o aparato militar e de inteligência do Comando de Defesa Cibernética (ComDCiber) e do Gabinete de Segurança Institucional (GSI), responsáveis pela prova forense bruta, e a Divisão de Defesa e Segurança Cibernética (DCiber) do Itamaraty, responsável pela redação jurídica da acusação diplomática (BROTHERHOOD, 2024). Sem um protocolo ágil de compartilhamento interagências, o dado técnico envelhece, inviabilizando uma reação política oportuna.

No Capítulo 3, apresentou-se uma possível solução estratégica por meio do nexo entre a atribuição e a ciberdiplomacia. Ao analisar a postura assertiva do Brasil em fóruns como o OEWG e a ONU, o capítulo demonstrou que a atribuição política funciona como uma 'sanção reputacional'. Ficou provado que a capacidade de apontar o agressor, fundamentada em fatos verificáveis, confere eficácia coercitiva às normas internacionais, transformando a diplomacia em uma ferramenta ativa de defesa nacional.

Nesse sentido, verifica-se a validação da hipótese deste trabalho. A institucionalização da atribuição política pelo Itamaraty fortalece a dissuasão cibernética precisamente porque altera o cálculo de custo-benefício do agressor. No ambiente anárquico do ciberespaço, agentes maliciosos operam sob a lógica da impunidade garantida pelo anonimato. Quando o Estado brasileiro converte subsídios técnicos em posicionamentos diplomáticos oficiais, rompe essa lógica. A impunidade gerada pelo anonimato é mitigada quando o agressor percebe que sua identidade — e, consequentemente, sua reputação e seu capital político — estão em risco. O custo de ser identificado como violador das normas internacionais, sujeito a contramedidas e ao isolamento diplomático, sobrepõe-se aos ganhos táticos de uma operação cibernética maliciosa.

As implicações para a Política Externa Brasileira (PEB) são profundas e exigem uma reconfiguração do perfil do corpo diplomático. O diplomata brasileiro do século XXI deixa de ser apenas um negociador de textos para tornar-se um 'diplomata-analista'. Para sustentar falas em fóruns de alto nível na ONU ou no âmbito do SELA, este profissional deve ser capaz de interpretar relatórios complexos do Gabinete de Segurança Institucional (GSI) e das Forças Armadas, traduzindo evidências de '*bits e bytes*' em argumentos jurídicos e políticos soberanos. A ciberdiplomacia exige, portanto, uma simbiose sem precedentes entre a inteligência técnica e a sensibilidade geopolítica, consolidando o Itamaraty como a linha de frente da defesa cibernética nacional.

Por fim, ao lançar um olhar sobre as considerações futuras, observa-se que a ciberdiplomacia nunca estará 'pronta', pois é um processo contínuo de adaptação. O surgimento de novas tecnologias, como a Inteligência Artificial (IA) generativa — capaz de automatizar ataques e criar desinformação em escala — e a computação quântica — que ameaça a criptografia atual —, por exemplo, apresenta desafios que testarão a resiliência dos protocolos brasileiros. A atribuição automatizada por IA pode acelerar a identificação de agressores, mas exigirá normas ainda mais rigorosas para evitar acusações injustas.

O Brasil, buscando consenso e respeito ao Direito Internacional, está bem posicionado para liderar esse debate. Contudo, a segurança digital exige vigilância e investimento em capacidades próprias. A jornada aqui descrita reafirma que a dissuasão não se faz apenas com *firewalls*, mas com uma diplomacia assertiva, capaz de iluminar as sombras do ciberespaço e de garantir que a soberania brasileira seja respeitada em todas as dimensões do poder.

REFERÊNCIAS

ALTMAN, Matthew C. **A theory of legal punishment**: deterrence, retribution, and the aims of the state. New York: Routledge, 2021. ISBN 978-1-003-14335-2.

ARAÚJO LISBOA , C.; ZIEBELL DE OLIVEIRA, G. . O Conceito de dissuasão cibernética: relevância e possibilidades . **OASIS**, [S. l.], n. 35, p. 53–78, 2022. DOI: 10.18601/16577558.n35.04. Disponível em: https://doi.org/10.18601/16577558.n35.04. Acesso em: 10 maio 2025.

ATTATFAA, Amel; RENAUDA, Karen; PAOLI, Stefano De. Cyber Diplomacy: A Systematic Literature Review. **Elsevier B. V.**, [s. l.], v. 176, p. 60-69, 2020. Disponível em: https://doi.org/10.1016/j.procs.2020.08.007. Acesso em: 3 out. 2025.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. **Estratégia Nacional de Cibersegurança**. Brasília, DF: Presidência da República, 2025,. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber. Acesso em: 22 dez. 2025.

BRASIL. **Livro Branco de Defesa Nacional**. Brasília, DF: Ministério da Defesa, 2024. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro-branco-de-defesa-nacional-lbdn-1/arquivos/livro-branco-de-defesa-nacional/livro_branco_de_defesa_nacional.pdf. Acesso em: 22 dez. 2025.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. MD31-M-07: **Doutrina Militar de Defesa Cibernética**. 2. ed. Brasília, DF: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 22 dez. 2025.

BRASIL. Ministério da Defesa. **Política Cibernética de Defesa (MD31-P-02)**. 1. ed. Brasília: Ministério da Defesa, 2012.

BRASIL. [Voluntary national contribution: Brazil]. In: ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral. **Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States**: submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. A/76/136. Nova York: ONU, 13 jul. 2021. p. 17-22. Disponível em: https://digitallibrary.un.org/?ln=en. Acesso em: 16 mar. 2025.

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

Políticas, Universidade de Lisboa, Lisboa, 2024. Disponível em: http://hdl.handle.net/10400.5/29755. Acesso em: 3 out. 2025.

BRAW, Elisabeth; BROWN, Gary. Personalised Deterrence of Cyber Aggression. **The RUSI Journal**, [S. l.], p. 1-7, 18, mar. 2020.

BUENO, Guilherme. Diplomacia Digital: Uma nova Disciplina e Possibilidade. **Escola Superior de Relações Internacionais (ESRI)**, 13 mar. 2024. Disponível em: https://esri.net.br/diplomacia-digital/. Acesso em: 3 out. 2025.

CEPIK, Marco Aurélio Chaves; MARCELINO, Henriques Manuel. Segurança cibernética em Moçambique: conceitos, infraestrutura e desafios de implementação. **Revista Carta Internacional**, Belo Horizonte, v. 16, n. 3, e1130, p. 1-25, 2021. DOI: 10.21530/ci.v16n3.2021.1130.

CEPIK, Marco; CANABARRO, Diego Rafael; FERREIRA, Thiago Borne. Cyberwar: Clausewitzian encounters. **Space & Defense**, [S. l.], v. 8, n. 1, p. 19-33, 2015.

CORREIA, Gustavo Luiz de Lima. **A diplomacia de defesa como fator de projeção do poder nacional**. 2022. 67 f. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, 2022.

COUNCIL OF EUROPE. **Convention on Cybercrime**: special edition dedicated to the drafters of the Convention (1997-2001). Strasbourg: Council of Europe, 2022. Disponível em: https://parliament.gov.fj/wp-content/uploads/2022/10/Special-edition-Budapest-Convention-EN-2022-1.pdf. Acesso em: 10 out. 2025.

CYBER DIPLOMACY TOOLBOX. **Cyber diplomacy links**. Zurique: Cyber Risk GmbH, [s. d.]. Disponível em: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_Links.html. Acesso em: 26 maio 2025.

CYBER DIPLOMACY TOOLBOX. **What is cyber diplomacy?** Zurique: Cyber Risk GmbH, [s. d.]. Disponível em: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html. Acesso em: 10 out. 2025.

DELFINO, Pedro Henrique. **A modernização do aparato de defesa brasileiro versus o dilema de segurança**: avanços e desafios. 2014. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais e Integração) – Instituto Latino Americano de Economia, Sociedade e Política, Universidade Federal da Integração Latino-Americana, Foz do Iguaçu, 2014. Disponível em: https://dspace.unila.edu.br/handle/123456789/356. Acesso em: 3 out. 2025.

EGLOFF, Florian J. Contested public attributions of cyber incidents and the role of academia. **Contemporary Security Policy**, [S. l.], v. 41, n. 1, p. 55-81, 2020. DOI: 10.1080/13523260.2019.1677324. Disponível em: https://doi.org/10.1080/13523260.2019.1677324. Acesso em: 3 out. 2025.

EGLOFF, Florian J.; SMEETS, Max. Publicly attributing cyber attacks: a framework. **Journal of Strategic Studies**, [S. l.], v. 46, n. 3, p. 502-533, 2023. DOI:

10.1080/01402390.2021.1895117. Disponível em: https://doi.org/10.1080/01402390.2021.1895117. Acesso em: 10 out. 2025.

ESRI. **Diplomacia Digital**: uma nova disciplina e possibilidade. [S. l.]: ESRI, 13 mar. 2024. Disponível em: https://esri.net.br/diplomacia-digital/. Acesso em: 3 out. 2025.

FAVERO, Pedro Henrique Paulette. **A diplomacia cibernética como fonte de poder**: uma análise do caso estadunidense e chinês entre 2010 e 2024. 2025. 129 f. Dissertação (Mestrado em Relações Internacionais) – Centro Socioeconômico, Universidade Federal de Santa Catarina, Florianópolis, 2025. Disponível em: https://repositorio.ufsc.br/handle/123456789/265150. Acesso em: 3 out. 2025.

FISCHERKELLER, Michael. Incorporating offensive cyber operations into conventional deterrence strategies. **Survival**, [S. l.], v. 59, n. 1, p. 103-134, fev. 2017. DOI: 10.1080/00396338.2017.1282679.

FREY, Carola. Digital diplomacy: the impact of technology on modern diplomacy and foreign policy: current realities and future prospects. **Romanian Journal of European Affairs**, [S. l.], v. 24, n. 1, jun. 2024. Disponível em: http://rjea.ier.gov.ro/wp-content/uploads/2024/06/Art.-5_Digital-diplomacy_Frey_2024_final.pdf. Acesso em: 3 out. 2025.

GADEGAST, Manuella da Costa. **Potência cibernética**: atributos e implicações. 2022. 73 f. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022.

GARCIA, Marcel Furtado. Rumo a um regime global de segurança cibernética. **Cadernos de Política Exterior, Brasília**, ano 11, n. 16, p. 233-272, jun. 2025. DOI: 10.61623/cpe.v11n16.a10. Disponível em: https://funag.gov.br/biblioteca-nova/produto/1-1314-1. Acesso em: 26 maio 2026.

GODINHO, Renato Domith. Diplomacia em tempo de redes. **CEBRI-Revista**, [S. l.], ano 3, n. 11, p. 148-170, jul./set. 2024. Disponível em: https://cebri.org/revista/br/artigo/175/diplomacia-em-tempo-de-redes. Acesso em: 12 mai. 2025.

GÓES, Eduardo Kraemer. Diplomacia digital: a internet como ferramenta da política externa. In: ENCONTRO NACIONAL DA ABRI, 6., 2017, Belo Horizonte. **Anais eletrônicos [...]**. Belo Horizonte: ABRI, 2017. Disponível em: http://www.encontro2017.abri.org.br/resources/anais/8/1498489143_ARQUIVO_ArtigoABRI2017-DiplomaciaDigital-EduardoKraemerGoes.pdf. Acesso em: 3 out. 2025.

GRÖHS, Lauren Giordani. **Ciberdiplomacia e Multistakeholder Diplomacy**: uma análise introdutória. Orientador: Fabricio Pontin. 2024. 19. TCC (Graduação) - Curso de Relações Internacionais, Universidade La Salle, Canoas, 2024. Disponível em: https://svr-net20.unilasalle.edu.br/handle/11690/4034. Acesso em: 3 out. 2025.

HEALEY, Jason. **Beyond Attribution**: Seeking National Responsibility in Cyberspace. Washington, DC: Atlantic Council, 22 fev. 2012. Issue Brief. Disponível em:

https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF. Acesso em: 3 out. 2025.

HUREL, Louise Marie. Unpacking Brazil's Cyber Diplomacy. **EU Cyber Direct**, 14 mar. 2022. Blog. Disponível em: https://eucyberdirect.eu/blog/unpacking-brazil-s-cyber-diplomacy. Acesso em: 16 maio 2026.

JACCARD, James; JACOBY, Jacob. **Theory construction and model-building skills**: a practical guide for social scientists. 2. ed. New York: The Guilford Press, 2020.

KAARBO, Juliet; THIES, Cameron G. (org.). **The Oxford Handbook of Foreign Policy Analysis**. Oxford: Oxford University Press, 2024.

KAISER, Karen. Protecting respondent confidentiality in qualitative research. **Qualitative Health Research**, [s. l.], v. 19, n. 11, p. 1632-1641, nov. 2009. DOI: https://doi.org/10.1177/1049732309350879.

KALPOKAITE, Neringa; RADIVOJEVIC, Ivana. Demystifying qualitative data analysis for novice qualitative researchers. **The Qualitative Report**, [s. l.], v. 24, n. 13, p. 44-57, 2019. DOI: https://doi.org/10.46743/2160-3715/2019.4120. Disponível em: https://nsuworks.nova.edu/tqr/vol24/iss13/5. Acesso em: 03 jul. 2025.

KASPER, Agnes; OSULA, Anna-Maria; MOLNÁR, Anna. EU cybersecurity and cyber diplomacy. **IDP: Revista de Internet, Derecho y Política**, [s. l.], n. 33, p. 1-16, dez. 2021. DOI: https://doi.org/10.7238/idp.v0i33.391629. Disponível em: https://raco.cat/index.php/IDP/article/view/n34-kasper. Acesso em: 21 nov. 2025.

LANCELOT, Jonathan F. Cyber-diplomacy: cyberwarfare and the rules of engagement. **Journal of Cyber Security Technology**, [s. l.], v. 4, n. 4, p. 240-254, 3 ago. 2020. DOI: https://doi.org/10.1080/23742917.2020.1798155. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23742917.2020.1798155?scroll=top&needAccess=true. Acesso em: 10 mai. 2025.

LEKATIS, George. **The EU Cyber Diplomacy Toolbox**: an in-depth analysis of cyber diplomacy. [s. l.]: Cyber Risk GmbH, 2026. Disponível em: https://www.cyber-diplomacy-toolbox.com/. Acesso em: 3 out. 2025.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica: RAND Corporation, 2009.

LIBICKI, Martin C. Expectations of cyber deterrence. **Strategic Studies Quarterly**, [s. l.], v. 13, n. 1, p. 10-23, primavera 2019. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-1/Libicki.pdf . Acesso em: 3 nov 2025.

LINDSAY, Jon R. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. **Journal of Cybersecurity**, [S. l.], v. 1, n. 1, p. 53–67, nov. 2015. Disponível em: https://doi.org/10.1093/cybsec/tyv003. Acesso em: 26 maio 2025.

LIPPKE. **Theory legal punishment**. [S. l.: s. n.], 2024. ISBN 9781032661667.

MAČÁK, Kubo; DIAS, Talita; KASPER, Ágnes. **Handbook on developing a national position on international law and cyber activities**: a practical guide for states. [S. l.]: University of Exeter; NATO Cooperative Cyber Defence Centre of Excellence, 2025. Disponível em: https://ccdcoe.org/. Acesso em: 3 out. 2025.

MARTINS, Bárbara Cordeiro. **O Brasil e a construção normativa do ciberespaço no âmbito das Nações Unidas (GGE e OEWG)**. 2025. Trabalho de Conclusão de Curso (Bacharelado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2025.

MASCHMEYER, Lennart. Deception and detection: why artificial intelligence empowers cyber defense over offense. **International Security**, [Cambridge], v. 50, n. 3, p. 86-126, 2026. Disponível em: http://direct.mit.edu/isec/article-pdf/50/3/86/2586942/isec.a.398.pdf. Acesso em: 26 mai. 2025.

MAZANEC, Brian; THAYER, Bradley A. **Deterring cyber warfare**: towards solving the attribution puzzle. 2015. 42 f. Trabalho apresentado na Annual ISA Convention, New Orleans, 2015.

MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (org.). **Segurança e defesa cibernética**: da fronteira física aos muros virtuais. Recife: Editora UFPE, 2014. 196 p. (Coleção Defesa e Fronteiras Virtuais, v. 1). ISBN 978-85-415-0459-1.

MORGAN, Patrick M. **Deterrence now**. Cambridge: Cambridge University Press, 2003. (Cambridge studies in international relations, 89).

MUREȘAN, Radu Constantin. CURRENT APPROACHES OF DIPLOMACY IN THE CYBERSPACE. **Studia Universitatis Babes-Bolyai Studia Europaea**, [S. l.], v. 62, n. 2, p. 31–43, 2017. DOI: 10.24193/subbeuropaea.2017.2.03. Disponível em: https://studia.reviste.ubbcluj.ro/index.php/subbeuropaea/article/view/2188. Acesso em: 3 out. 2025.

NYE JR., Joseph S. Deterrence and dissuasion in cyberspace. **International Security**, [Cambridge], v. 41, n. 3, p. 44-71, 2017. Disponível em: https://doi.org/10.1162/ISEC_a_00266. Acesso em: 3 mai. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção das Nações Unidas sobre Cibercrime**: reforço da cooperação internacional para o combate a determinados crimes cometidos por meio de sistemas de tecnologia da informação e comunicação e para o compartilhamento de provas em formato eletrônico de crimes graves. Nova York: ONU, 2024. Disponível em: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html.

PAVÃO, João; BASTARDO, Rute; CARREIRA, Dário; ROCHA, Nelson Pacheco. Ciber-resiliência no contexto da segurança e defesa nacionais. **RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação**, [S. l.], n. 53, p. 359-371, 2024.

PINTO, Paulo Cordeiro de Andrade. **Diplomacia e política de defesa**: o Brasil no debate sobre a segurança hemisférica na década pós-Guerra Fria (1990-2000). Brasília: FUNAG, 2015. 262 p. (Coleção CAE). ISBN 978-85-7631-566-7.

QUIVY, Raymond; VAN CAMPENHOUDT, Luc. **Manual de investigação em ciências sociais**. Lisboa: Gradiva, 2008.

RADANLIEV, Petar. Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. **Journal of Cyber Security Technology**, [S. l.], v. 9, n. 1, p. 28-78, 2024. Disponível em: https://doi.org/10.1080/23742917.2024.2312671. Acesso em: 3 out. 2025.

REALPE DÍAZ, M. E. La ciberdiplomacia en relación con el ciberpoder: mecanismos y estrategias para la consecución de intereses nacionales. **Novum Jus**, [S. l.], v. 18, n. 2, p. 279–304, 2024. Disponível em: https://doi.org/10.14718/NovumJus.2024.18.2.11. Acesso em: 26 mai. 2025.

RID, Thomas; BUCHANAN, Ben. Attributing cyber attacks. **The Journal of Strategic Studies**, [S. l.], v. 38, n. 1-2, p. 4-37, 2015. Disponível em: http://dx.doi.org/10.1080/01402390.2014.977382. Acesso em: 23 mar. 2025.

ROSEN, Jonathan D.; CUTRONA, Sebastián A. (org.). **Mano dura policies in Latin America**. New York: Routledge, 2023. (Routledge Studies in Latin American Politics). ISBN 978-1-003-39841-7.

SABIR, Muhammad Imtiaz. Assessing Attribution and Credible Deterrence in Cyberspace. **BTTN Journal** , [S. l.], v. 3, n. 1, p. 132–147, 2024. DOI: 10.61732/bj.v3i1.87. Disponível em: https://bttn.org.pk/ojs/index.php/BTTN_Journal/article/view/87. Acesso em: 16 mai. 2025.

SALINAS, Melissa Montes. La evolución de la comunicación diplomática: su transformación en el tiempo y la nueva "ciberdiplomacia". **Revista Relaciones Internacionales**, El Salvador, v. 5, 2023. Disponível em:https://revistas.ues.edu.sv/index.php/reinter/article/view/2701. Acesso em: 3 out. 2025.

SALVI, Andrea; TIIRMAA-KLAAR, Heli; LEWIS, James Andrew (org.). **A handbook for the practice of cyber diplomacy**. Luxemburgo: Publicações da União Europeia, 2024. Disponível em: https://doi.org/10.2815/2444567.

SCHMITT, Michael N. (ed.). T**allinn Manual 2.0 on the international law applicable to cyber operations**. 2. ed. Cambridge: Cambridge University Press, 2017.

SENOL, Mustafa; KARACUHA, Ertugrul.Creating and Implementing an Effective and Deterrent NationalCyber Security Strategy. **Journal of Engineering,** Istanbul, Turkey, vol

2020, 9 páginas, junho, 2020. Disponível em: https://doi.org/10.1155/2020/5267564. Acesso em: 3 out. 2025.

SERRANO, Inês Isabel Baião. **Cibersegurança na União Europeia**: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. 2022. Dissertação (Mestrado em Relações Internacionais e Estudos Europeus) – Escola de Ciências Sociais, Universidade de Évora, Évora, 2022. Disponível em: https://dspace.uevora.pt/rdpc/handle/10174/32108. Acesso em: 3 out. 2025.

SHELDON, Robert. **What is cyber attribution?**. TechTarget, 31 jul. 2024. Disponível em:https://www.techtarget.com/searchsecurity/definition/cyber-attribution. Acesso em: 22 dez. 2024.

SILVA, Antonio Ruy de Almeida. A diplomacia de defesa na política internacional. **Revista da Escola de Guerra Naval**, [S. l.], v. 21, n. 2, p. 181-204, 2015.

SILVA, Vinícius Lemos da. **A diplomacia militar e sua contribuição para a política externa brasileira**. 2017. Artigo (Especialização em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2017.

SISTEMA ECONÓMICO LATINOAMERICANO Y DEL CARIBE (SELA). **Manual de Ciberdiplomacia para la convergencia regional**. Caracas: SELA, 2024. Disponível em: https://sela.org/wp-content/uploads/2024/08/manual-ciberdiplomacia-para-la-convergencia-regional.pdf. Acesso em: 3 out. 2025.

SOUSA MATOS, Erico. Diplomacia pública y América del Sur: de los conceptos a la práctica: Telesur y el caso venezolano. **Desafios**, Bogotá, v. 28, n. 1, p. 399-426, 2016. DOI: https://doi.org/10.12804/desafios28.1.2016.10. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-40352016000100012. Acesso em: 26 maio 2026.

TASENȚE, T.; STAN, M.-I. South American digital diplomacy: approaches before and after the Russian-Ukrainian crisis. **Cuadernos.info**, [S. l.], n. 57, p. 46–68, 2024. DOI: 10.7764/cdi.57.66393. Disponível em: https://cuadernosinfo.uc.cl/index.php/cdi/article/view/66393. Acesso em: 3 out.. 2025.

TOR, Uri. 'Cumulative deterrence' as a new paradigm for cyber deterrence. **Journal of Strategic Studies**, [S. l.], v. 40, n. 1-2, p. 1-26, 2015. DOI: 10.1080/01402390.2015.1115975.

TSAGOURIAS, Nicholas; FARRELL, Michael. Cyber Attribution: Technical and Legal Approaches and Challenges. **The European Journal of International Law**, [s. l.], v. 31, n. 3, p. 941-967, ago. 2020. Disponível em: https://doi.org/10.1093/ejil/chaa057. Acesso em: 10 mai. 2025.

ÜLGEN, Sinan. **Governing cyberspace**: a road map for transatlantic leadership. Brussels: Carnegie Europe, 2016. Disponível em: https://carnegieendowment.org/research/2016/01/governing-cyberspace-a-road-map-for-transatlantic-leadership?lang=en.

UNIÃO EUROPEIA. Comissão Europeia; Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança. **The EU's Cybersecurity Strategy for the Digital Decade**: joint communication to the European Parliament and the Council. Bruxelas, 16 dez. 2020. JOIN(2020) 18 final. Disponível em: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. Acesso em: 10 mai 2025.

UNITED NATIONS. General Assembly. **Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security**: note by the Secretary-General. New York: UN, 22 July 2015. 17 p. (A/70/174). Disponível em: [https://docs.un.org/en/a/70/174]. Acesso em: 31 mar. 2025.

VELANDIA, Karenina. Quais são as sofisticadas armas cibernéticas da guerra do século 21? **BBC News Brasil**, [s. l.], 5 mar. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-39149203. Acesso em: 10 dez. 2025.

WILNER, Alex. Cyber deterrence and critical-infrastructure protection: expectation, application, and limitation. **Comparative Strategy**, [S. l.], v. 36, n. 4, p. 309-318, 2017. DOI: 10.1080/01495933.2017.1361202.

WILNER, Alex S.. US cyber deterrence: practice guiding theory. **The Journal of Strategic Studies**, [S. l.], 2019. DOI: 10.1080/01402390.2018.1563779.