A COOPERAÇÃO INTERNACIONAL NO COMBATE ÀS AMEAÇAS CIBERNÉTICAS: UM ESTUDO COMPARATIVO ENTRE BRASIL E REINO UNIDO NO PERÍODO DE 2010 A 2020

INTERNATIONAL COOPERATION IN COMBATING CYBER THREATS: A COMPARATIVE STUDY BETWEEN BRAZIL AND THE UNITED KINGDOM FROM 2010 TO 2020

LA COOPERACIÓN INTERNACIONAL EN EL COMBATE A LAS AMENAZAS CIBERNÉTICAS: UN ESTUDIO COMPARATIVO ENTRE BRASIL Y EL REINO UNIDO EN EL PERÍODO DE 2010 A 2020

Emily Borges Honorato[1]

Resumo

O ciberespaço tornou-se um campo estratégico para a segurança nacional, exigindo cooperação internacional no combate às ameaças digitais. Este estudo analisa a cooperação entre Brasil e Reino Unido entre 2010 e 2020, destacando desafios e oportunidades dessa parceria. O Brasil enfrenta ameaças crescentes, como *phishing* e *ransomware*, enquanto o Reino Unido lida com ataques sofisticados a infraestruturas críticas. Ambos os países desenvolveram estratégias de segurança, como a *E-Ciber* no Brasil e a *National Cyber Strategy* no Reino Unido. A colaboração entre as nações inclui acordos bilaterais, troca de informações sobre ameaças e capacitação técnica. No entanto, desafios como a fragmentação institucional no Brasil e diferenças normativas dificultam a cooperação plena. Para fortalecer essa parceria, recomenda-se aprimorar a governança cibernética, estabelecer marcos regulatórios harmonizados e investir na capacitação de especialistas. A pesquisa conclui que a cooperação internacional é essencial para mitigar riscos cibernéticos e o alinhamento entre Brasil e Reino Unido pode fortalecer a segurança digital global.

Palavras-chave: ciberespaço; cooperação internacional; segurança cibernética; Brasil; Reino Unido.

Abstract

Cyberspace has become a strategic field for national security, requiring international cooperation to combat digital threats. This study analyzes the cooperation between Brazil and the United Kingdom from 2010 to 2020, highlighting the challenges and opportunities of this partnership. Brazil faces growing threats such as phishing and ransomware, while the UK deals with sophisticated attacks on critical infrastructure. Both countries have developed cybersecurity strategies, such as Brazil's E-Ciber and the UK's National Cyber Strategy. Collaboration includes bilateral agreements, threat information sharing, and technical training. However, challenges such as institutional fragmentation in Brazil and regulatory differences hinder full cooperation. To strengthen this partnership, it is recommended to improve cyber governance, establish harmonized regulatory frameworks, and invest in expert training. The research concludes that international cooperation is essential to mitigate cyber risks, and alignment between Brazil and the UK can enhance global digital security.

Keywords: cyberspace; international cooperation; cybersecurity; Brazil; United Kingdom.

Resumen

El ciberespacio se ha convertido en un campo estratégico para la seguridad nacional, lo que exige cooperación internacional frente a las amenazas digitales. Este estudio analiza la cooperación entre Brasil y el Reino Unido entre 2010 y 2020, destacando desafíos y oportunidades de esta asociación. Brasil enfrenta amenazas crecientes como el phishing y el ransomware, mientras que el Reino Unido lidia con ataques sofisticados a infraestructuras críticas. Ambos países han desarrollado estrategias de seguridad, como la E-Ciber en Brasil y la National Cyber Strategy en el Reino Unido. La colaboración incluye acuerdos bilaterales, intercambio de información sobre

[1] Graduanda em Relações Internacionais pelo Centro Universitário Internacional (UNINTER).

DOI: https://doi.org/10.22169/cadjud.v7n2.3481

amenazas y capacitación técnica. Sin embargo, desafíos como la fragmentación institucional en Brasil y las diferencias normativas dificultan una cooperación plena. Para fortalecer esta asociación, se recomienda mejorar la gobernanza cibernética, establecer marcos regulatorios armonizados e invertir en la formación de especialistas. La investigación concluye que la cooperación internacional es esencial para mitigar los riesgos cibernéticos y que el alineamiento entre Brasil y el Reino Unido puede fortalecer la seguridad digital global.

Palabras clave: ciberespacio; cooperación internacional; seguridad cibernética; Brasil; Reino Unido.

1 Introdução

O ciberespaço tornou-se um campo indispensável nas áreas de segurança, política e economia, e entender como as nações lidam com as ameaças cibernéticas por meio da colaboração é crucial. Nesse sentido, este artigo visa contribuir para este estudo a partir da análise das ações e acordos de cooperação cibernética entre Brasil e Reino Unido, destacando os principais desafios e oportunidades dessa colaboração. O foco desta pesquisa não é apenas os acordos, mas a compreensão das políticas e práticas adotadas para enfrentar as ameaças cibernéticas.

O problema de pesquisa relacionado ao objeto de pesquisa consiste na seguinte questão: como evoluíram as políticas e práticas de cooperação internacional entre Brasil e Reino Unido no combate às ameaças cibernéticas de 2010 a 2020? E quais são os principais desafios e sucessos dessa colaboração?

A pesquisa busca analisar as ações e acordos de cooperação cibernética entre Brasil e Reino Unido, identificando as principais dinâmicas dessa colaboração. Os objetivos específicos incluem: 1) Desenvolver uma breve contextualização sobre os principais tipos de ameaças cibernéticas enfrentadas por Brasil e Reino Unido no sec. XXI; 2) Pesquisar as políticas e estratégias de segurança cibernética adotadas por Brasil e Reino Unido entre 2010 a 2020; 3) Identificar e analisar as ações e acordos de cooperação cibernética entre Brasil e Reino Unido; 4) Identificar os principais desafios e oportunidades dessa cooperação entre 2010 a 2020; 5) Discorrer sobre recomendações para melhorar a cooperação cibernética entre Brasil e Reino Unido.

Uma vez que este artigo trata da cooperação internacional no combate às ameaças cibernéticas, a metodologia aqui utilizada é de abordagem qualitativa, fundamentada em pesquisa documental e bibliográfica, permitindo uma análise abrangente dos dados disponíveis.

2 Principais ameaças cibernéticas enfrentadas por Brasil e Reino Unido no século XXI

Nos últimos anos, tanto o Brasil quanto o Reino Unido têm enfrentado um aumento significativo nas ameaças cibernéticas, refletindo a crescente complexidade e sofisticação dos ataques. No Brasil, uma pesquisa realizada pela 24ª edição do *Internet Security Threat Report* (ISTR), relatório anual de segurança da Symante, coloca o Brasil em terceiro lugar globalmente

em termos de fontes de *malware*, *bots*, *spam* e ataques de *phishing,* sendo que na América Latina o Brasil está na primeira posição: recebe 4,11% dos ataques globais. Esses incidentes não apenas comprometem dados sensíveis, mas também ameaçam a confiança do público em serviços essenciais.

No documento da *Estratégia Nacional de Segurança Cibernética (E-Ciber)*, o Gabinete de Segurança Institucional (GSI) destaca que as ameaças cibernéticas, como a espionagem, são direcionadas a setores estratégicos do Brasil, incluindo instituições governamentais e empresas, o que gera riscos significativos para a segurança nacional. A proteção de dados sensíveis e a integridade das informações críticas são prioridades para garantir a resiliência do país contra ciberataques, com ênfase na necessidade de uma ação coordenada para mitigar as vulnerabilidades e fortalecer a defesa cibernética.

No Reino Unido, a situação é igualmente preocupante. Um relatório do National Cyber Security Centre (NCSC, 2023) indicou que os ataques cibernéticos aumentaram exponencialmente, especialmente durante a pandemia de covid-19. Os dados mostram que o Reino Unido é alvo constante de ameaças, com criminosos cibernéticos explorando a vulnerabilidade de sistemas remotos e digitais. O NCSC também destacou que o setor de saúde foi particularmente afetado, com tentativas de ataques direcionadas a serviços essenciais durante períodos críticos. Essa afirmação ressalta a abrangência e o impacto devastador que tais ações podem ter sobre a integridade e a soberania de um país, como no caso do Brasil e do Reino Unido.

Essas ameaças evidenciam a necessidade urgente de fortalecer as políticas de segurança cibernética, além de reforçar a cooperação internacional entre países. Iniciativas que incentivam o compartilhamento de informações sobre riscos cibernéticos e melhores práticas são essenciais para mitigar esses desafios e garantir a proteção das infraestruturas digitais de forma mais eficaz e colaborativa.

1.1 Tipos de ameaças cibernéticas: ataques mais comuns no Brasil

O Brasil tem enfrentado uma série de ameaças cibernéticas nos últimos anos, refletindo um cenário em evolução em relação à segurança digital. A Estratégia Nacional de Segurança Cibernética (*E-Ciber*), lançada em 2019, delineia um conjunto abrangente de objetivos e ações para mitigar os riscos associados às ameaças cibernéticas, buscando coordenar esforços entre diferentes setores do governo e da sociedade civil.

O *phishing*, por exemplo, continua a ser uma das táticas mais utilizadas por cibercriminosos, visando enganar usuários para que revelem informações sensíveis, como senhas e dados bancários. Em 2021, o Brasil registrou um aumento significativo nos casos de *ransomware*, que envolvem a criptografia de dados das vítimas e a exigência de pagamento para a restauração do acesso. Esses ataques têm afetado tanto instituições públicas quanto privadas, causando prejuízos financeiros significativos e comprometendo a confiança dos usuários. Como afirma Zanellato:

> A internet é um suporte (ou meio) que permite trocar correspondência, arquivo, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos (Zanellato, 2002, p. 173)

Essa versatilidade da internet não apenas facilita a interação entre indivíduos e organizações, mas também a torna vulnerável a uma variedade de ataques cibernéticos, que exploram essas funcionalidades para comprometer dados e sistemas.

O Brasil tem enfrentado desafios relacionados à ciberespionagem, especialmente em setores estratégicos, como o governo e a infraestrutura crítica. A falta de uma abordagem consolidada para a segurança cibernética tem resultado em uma fragmentação das iniciativas de proteção, dificultando uma resposta efetiva às ameaças emergentes. O Brasil tem buscado integrar esforços com organizações internacionais, como indicado no Press Release da OEA (IACHR... 2020) e no V Diálogo Estratégico Brasil-Reino Unido (Brasil, 2020), que destacam a participação do país em iniciativas multilaterais de cooperação cibernética.

Assim, embora o Brasil tenha avançado na formulação de políticas de segurança cibernética, os ataques cibernéticos continuam a representar um desafio significativo, demandando uma colaboração mais robusta entre os setores público e privado, além de um engajamento ativo em iniciativas de ciberdiplomacia.

1.2 Cenário de ameaças cibernéticas no Reino Unido: desafios e tendências

Segundo o documento *National cyber security strategy 2016-2021* publicado pelo HM Government, o Reino Unido enfrenta um ambiente cibernético cada vez mais desafiador, com ameaças cibernéticas evoluindo em sofisticação e volume, identificando que o país se tornou alvo de uma série de ataques direcionados, incluindo espionagem cibernética, cibercrime e ciberterrorismo. Esses ataques visam setores estratégicos como telecomunicações, energia, defesa e finanças.

Ataques de *ransomware* e DDoS aumentaram significativamente nos últimos anos, refletindo a crescente sofisticação das ameaças digitais, conforme relatado pelo *Relatório Global de Incidentes de Ransomware* da Ransomware Task Force (2023) e pelo estudo *Global Cybersecurity Threat Trends* da Deloitte (2023).

Para enfrentar esses desafios, a estratégia britânica se concentra em três pilares: defesa, dissuasão e desenvolvimento de capacidades cibernéticas. A defesa envolve o fortalecimento das infraestruturas críticas do país, enquanto a dissuasão busca evitar que adversários avancem com ataques cibernéticos, seja por meio de sanções ou de cooperação internacional.

De acordo com a *National Cyber Strategy* (United Kingdom, 2022), o governo britânico tem buscado fortalecer sua posição como um poder cibernético responsável, investindo na resiliência digital e promovendo um ambiente seguro para o desenvolvimento da economia digital.

2 Políticas e estratégias de segurança cibernética: Brasil e Reino Unido (2010-2020)

As políticas de segurança cibernética têm se tornado fundamentais em um mundo em que a digitalização e a interconexão global estão em constante crescimento. Tanto o Brasil quanto o Reino Unido adotaram abordagens distintas para enfrentar os desafios impostos pelas ameaças cibernéticas. Durante o período de 2010 a 2020, ambos os países desenvolveram e implementaram estratégias que refletem suas prioridades e contextos geopolíticos únicos.

As ameaças cibernéticas enfrentadas por ambos os países têm se tornado cada vez mais sofisticadas, o que exigiu uma resposta robusta e estratégica. De acordo o documento "*Cyber capabilities and national power – volume 2: Brazil*" do International Institute for Strategic Studies (IISS, 2023), o Brasil tem buscado integrar suas iniciativas de segurança cibernética em um contexto mais amplo de defesa nacional, refletindo uma mudança de paradigma em resposta à crescente complexidade das ameaças digitais. O relatório destaca que, apesar dos avanços, o país ainda enfrenta desafios significativos, como a fragmentação das iniciativas de segurança entre diferentes agências governamentais e a necessidade de uma estratégia mais coesa para lidar com os riscos emergentes.

Por outro lado, o Reino Unido tem se posicionado como um líder em segurança cibernética global, com uma abordagem que combina inovação tecnológica e cooperação internacional. O relatório anual da National Cyber Security Centre 2023 (NCSC, 2023, p. 15) enfatiza que o país está comprometido em fortalecer sua infraestrutura cibernética por meio de parcerias estratégicas com outras nações e setores privados. Essa estratégia é orientada por um foco em tecnologias

emergentes e no compartilhamento de inteligência cibernética, visando não apenas proteger seus ativos, mas também contribuir para a segurança cibernética global. A colaboração com aliados, como os Estados Unidos e países da União Europeia, é fundamental para sua abordagem, permitindo uma resposta mais eficaz a incidentes cibernéticos e ameaças transnacionais.

As ameaças cibernéticas enfrentadas por ambos os países têm se tornado cada vez mais sofisticadas, exigindo uma resposta robusta e estratégica. O ciberespaço, por sua própria natureza, nunca será 100% seguro, pois sempre haverá vulnerabilidades que podem ser exploradas, e a evolução das ameaças será contínua. Nesse sentido, o objetivo mais realista é a resiliência cibernética, que garante que uma organização possa responder rapidamente a ataques inevitáveis, minimizando a interrupção das operações.

2.1 Políticas de segurança cibernética no Brasil: evolução e implementação

No Brasil, a evolução das políticas de segurança cibernética ganhou destaque com a criação da Estratégia Nacional de Segurança Cibernética (*E-Ciber*), que busca integrar esforços entre diferentes setores do governo e da sociedade civil. Lançada em 2020, foi desenvolvida por meio de um processo colaborativo que envolveu diversos *stakeholders*, conforme descrito no *Fifth Brazil–United Kingdom High-Level Strategic Dialogue Joint Communique* (Brasil, 2020). O foco está na proteção de infraestruturas críticas e no fortalecimento da resposta a incidentes cibernéticos, criando uma abordagem colaborativa e multidisciplinar.

Recentemente, o governo brasileiro instituiu a Política Nacional de Cibersegurança, que fortalece ainda mais a governança em segurança cibernética, criando o Comitê Nacional de Cibersegurança (CNCiber) para supervisionar as atividades e promover a cooperação interinstitucional. Esse desenvolvimento é visto como um passo importante para consolidar a capacidade do país de lidar com ameaças cibernéticas em um cenário de crescente digitalização.

O relatório do International Institute for Strategic Studies (IISS, 2023) e a análise do Carnegie Endowment for International Peace (Devanny; Buchan, 2023) destacam que a implementação da estratégia ainda apresenta lacunas, especialmente na coordenação entre as diversas entidades governamentais.

2.2 Estratégias de defesa cibernética no Reino Unido: uma abordagem comparativa

O Reino Unido possui uma das mais robustas estratégias de segurança cibernética do mundo, com ênfase em proteção e resiliência. A *National Cyber Security Strategy* (NCSS), que abrange o período de 2022 a 2025, é orientada por cinco pilares principais (United Kingdom,

2022): fortalecer o ecossistema cibernético do Reino Unido, construir um ambiente digital seguro e próspero, liderar no desenvolvimento de tecnologias críticas, promover a influência global e detectar, desmantelar e dissuadir adversários cibernéticos.

O NCSS atua como o órgão central na coordenação da defesa cibernética em vários setores, promovendo a colaboração entre governo, indústria e academia. Essa abordagem tem mostrado resultados significativos, com o Reino Unido investindo fortemente na capacitação de profissionais de segurança cibernética e na promoção de uma cultura de segurança em todos os níveis da sociedade.

O Brasil está em um processo de construção e aprimoramento de suas políticas, o Reino Unido já possui um sistema mais maduro, o que pode ser um ponto de aprendizado valioso para a implementação de iniciativas similares no Brasil.

3 Ações e acordos de cooperação cibernética entre Brasil e Reino unido

A cooperação cibernética entre Brasil e Reino Unido tem se intensificado ao longo dos últimos anos, refletindo uma preocupação mútua com as crescentes ameaças cibernéticas. O Brasil, ao adotar uma abordagem mais holística em sua Estratégia Nacional de Segurança Cibernética (*E-Ciber*), busca alinhar-se com padrões internacionais, incluindo aqueles promovidos pelo Reino Unido. A *E-Ciber* enfatiza a importância de expandir acordos de cooperação em segurança cibernética, destacando a necessidade de uma abordagem coordenada para combater o crime cibernético e melhorar a resiliência digital do país.

O Reino Unido tem se mostrado um parceiro ativo, ajudando o Brasil a desenvolver suas capacidades cibernéticas por meio de diversas iniciativas. Através de diálogos estratégicos, como os ocorridos na última década, ambos os países têm trabalhado juntos em áreas como a troca de informações sobre ameaças, capacitação em resposta a incidentes cibernéticos e intercâmbio de melhores práticas. O diálogo também abrange a necessidade de um arcabouço legal robusto que permita a cooperação efetiva em investigações de crimes cibernéticos, um desafio comum que enfrenta ambos os países.

3.1 Acordos bilaterais em segurança cibernética: Brasil e Reino Unido

Os acordos bilaterais firmados entre Brasil e Reino Unido incluem tratados que estabelecem um quadro para a assistência mútua em investigações cibernéticas, bem como a troca de informações sobre ameaças emergentes. Um exemplo disso é o Memorando de Entendimento sobre Segurança Cibernética, que visa fortalecer a cooperação técnica e

operacional entre as agências de segurança dos dois países. Esse acordo é um passo significativo, pois não só formaliza a colaboração, mas também permite que ambos os países compartilhem dados e recursos, aumentando a capacidade de resposta a incidentes cibernéticos de forma conjunta.

A participação do Brasil em fóruns internacionais, como os promovidos pela Organização dos Estados Americanos (OEA), tem sido crucial para o fortalecimento das relações com o Reino Unido. Esses fóruns proporcionam oportunidades de *networking* e troca de experiências, essenciais para a construção de um ecossistema de segurança cibernética mais robusto.

No Comunicado Conjunto do Diálogo Estratégico de Alto Nível Brasil-Reino Unido (2020), foi destacado que a cooperação bilateral entre os dois países serve como um exemplo de como nações podem trabalhar juntas em diversas áreas. O Brasil e o Reino Unido reafirmaram seu compromisso:

> Ambos concordaram em fortalecer a cooperação em segurança para conter ameaças regionais e internacionais. Os ministros saudaram o aprofundamento da colaboração bilateral em relação ao uso de inteligência artificial, proteção de dados, economia digital e acesso digital, implementação da rede 5G e cibersegurança, inclusive por meio do próximo Diálogo Digital e de Segurança Cibernética, que o Brasil e o Reino Unido pretendem realizar no primeiro semestre de 2021 (Brasil, 2020)

3.2 Ações conjuntas de cooperação cibernética: estudos de caso

Um estudo de caso notável é a participação do Reino Unido nos exercícios internacionais de cibersegurança, como o *Locked Shields*, em cooperação com a North Atlantic Treaty Organization (NATO). Esses exercícios testam a prontidão e as capacidades de resposta de diferentes países a incidentes cibernéticos simulados, permitindo que as equipes aprendam com a experiência de outros participantes, incluindo o Brasil. A colaboração nesse contexto demonstra não apenas um compromisso com a segurança cibernética, mas também a disposição para enfrentar desafios globais de forma coordenada.

As ações conjuntas entre Brasil e Reino Unido também se manifestam em projetos de educação e conscientização sobre segurança cibernética, que visam capacitar os cidadãos e as empresas a se protegerem contra as ameaças cibernéticas. A iniciativa britânica de promover a "ciber-higiene" no Brasil, por exemplo, tem sido bem recebida e integrada às estratégias locais, aumentando a resiliência cibernética da sociedade civil e das empresas.

Essas ações e acordos não só fortalecem a segurança cibernética de ambos os países, mas também estabelecem um modelo de cooperação que pode ser replicado em outras parcerias internacionais, contribuindo para um ambiente digital mais seguro a nível global.

4 Desafios e oportunidades na cooperação cibernética entre Brasil e Reino Unido (2010-2020)

A cooperação cibernética entre Brasil e Reino Unido enfrenta uma série de desafios que refletem não apenas as diferenças institucionais e normativas entre os dois países, mas também a complexidade das ameaças cibernéticas emergentes. Um dos principais desafios é a fragmentação das iniciativas de segurança cibernética em ambos os países.

No Brasil, por exemplo, a falta de coordenação entre os setores público e privado resulta em níveis variados de maturidade cibernética, o que pode comprometer a eficácia das estratégias de defesa. As diferentes capacidades técnicas e operacionais dificultam a implementação de uma abordagem unificada e eficiente para o combate a ameaças cibernéticas, como *malware* e *ransomware*, que têm aumentado em complexidade e frequência.

A relação política entre Brasil e Reino Unido tem suas próprias nuances que influenciam a cooperação cibernética. O Brasil, sob diferentes administrações, tem buscado um alinhamento estratégico tanto com nações ocidentais quanto com países do BRICS. Isso cria um cenário de incerteza, especialmente em relação à segurança cibernética e à privacidade de dados, uma vez que interesses geopolíticos podem impactar a confiança mútua necessária para uma colaboração eficaz.

O contexto global, marcado pela rivalidade entre Estados Unidos e China, também influencia a forma como Brasil e Reino Unido abordam questões de segurança cibernética, exigindo um equilíbrio delicado nas suas políticas externas e internas.

4.1 Principais desafios na cooperação cibernética: questões de confiança e alinhamento

As questões de confiança são fundamentais para a cooperação cibernética eficaz entre Brasil e Reino Unido. A desconfiança pode ser alimentada por divergências políticas, por experiências passadas de espionagem cibernética e pela falta de transparência nas práticas de segurança cibernética. A natureza global das ameaças cibernéticas requer uma resposta coletiva, mas a confiança mútua é essencial para garantir que as informações sejam compartilhadas de maneira segura e eficaz. A falta de um quadro normativo harmonizado pode dificultar a implementação de estratégias conjuntas. O Brasil, por exemplo, ainda está em processo de consolidação de sua Estratégia Nacional de Segurança Cibernética (*E-Ciber*), que busca estabelecer diretrizes claras para a proteção de dados e a resposta a incidentes cibernéticos.

A necessidade de um alinhamento nas prioridades de segurança cibernética é outro desafio significativo. Enquanto o Reino Unido tem uma abordagem bem definida e

institucionalizada para a segurança cibernética, o Brasil está ainda desenvolvendo sua capacidade e infraestrutura nesse campo.

Em um relatório do International Institute for Strategic Studies (IISS), é mencionado que "O Brasil ainda enfrenta desafios significativos em sua estratégia de segurança cibernética, que inclui a necessidade de alinhar suas capacidades de defesa com as melhores práticas internacionais" (IISS, 2020).

Essa afirmação é crucial para discutir os desafios e oportunidades na cooperação cibernética, pois enfatiza a necessidade de um alinhamento contínuo das políticas entre Brasil e Reino Unido para lidar com as ameaças cibernéticas. A ausência de normas e procedimentos operacionais comuns pode levar a ineficiências e lacunas na resposta a incidentes, dificultando a capacidade de ambos os países de lidar com ameaças complexas que podem atravessar fronteiras nacionais.

4.2 Oportunidades para ampliar a cooperação cibernética entre Brasil e Reino Unido

Apesar dos desafios, existem oportunidades significativas para expandir a cooperação cibernética entre Brasil e Reino Unido. Um dos principais pontos de alavancagem é a crescente necessidade de uma resposta coordenada às ameaças cibernéticas, que requer um intercâmbio de conhecimentos e melhores práticas entre as duas nações. A participação do Brasil em fóruns internacionais, como o Grupo de Trabalho da ONU sobre Cibersegurança, oferece uma plataforma para que o país se posicione como um ator relevante nas discussões sobre normas e regulamentações cibernéticas.

A parceria com o Reino Unido pode ser um catalisador para o desenvolvimento de capacidades técnicas e a troca de informações sobre novos desafios emergentes, como a segurança de infraestruturas críticas e a proteção de dados pessoais. Iniciativas conjuntas de capacitação e *workshops* em segurança cibernética podem fortalecer a formação de profissionais e as capacidades de resposta a incidentes no Brasil. A cooperação em projetos de pesquisa e inovação na área de cibersegurança também pode resultar em soluções tecnológicas mais robustas que beneficiem ambos os países.

Essas oportunidades não apenas melhoram a resiliência cibernética dos dois países, mas também constroem uma base mais sólida para um relacionamento bilateral de confiança, essencial em um cenário cibernético global em rápida evolução. Com o aumento das ameaças cibernéticas, a colaboração proativa pode se transformar em um pilar fundamental para a segurança nacional e a proteção dos cidadãos em ambas as nações.

5 Recomendações para fortalecer a cooperação cibernética entre Brasil e Reino Unido

A crescente interdependência entre países na era digital torna imperativa a adoção de uma abordagem colaborativa para a segurança cibernética. Uma das principais recomendações é a criação de um fórum bilateral que facilite o intercâmbio de informações e melhores práticas entre as nações. Esse fórum deve incluir representantes dos setores público e privado, assim como especialistas em segurança cibernética, para abordar questões comuns e desenvolver estratégias conjuntas.

A troca de informações sobre ameaças emergentes e incidentes cibernéticos é crucial para aprimorar a resposta a ataques e fortalecer as defesas cibernéticas. Estudos indicam que países com uma comunicação clara e eficaz sobre ameaças cibernéticas experimentam menores taxas de incidentes.Outra recomendação importante é o desenvolvimento de um quadro legal harmonizado que trate da cooperação cibernética e da resposta a incidentes. A falta de um marco jurídico claro pode dificultar a colaboração e a implementação de políticas eficazes.

Ambos os países devem trabalhar para alinhar suas legislações em torno de normas comuns de segurança cibernética, considerando as legislações existentes, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o *Data Protection Act* 2018. Isso ajudaria a criar uma base sólida para acordos futuros e garantir que as informações sejam compartilhadas em conformidade com as leis de proteção de dados.

5.1 Melhoria da cooperação técnica e do compartilhamento de informações

Para fortalecer a cooperação técnica, Brasil e Reino Unido devem estabelecer programas de treinamento conjuntos em segurança cibernética. Esses programas poderiam ser projetados para capacitar profissionais em ambos os países sobre novas tecnologias e práticas de segurança cibernética, promovendo uma abordagem mais robusta na defesa contra ciberameaças. A realização de exercícios de simulação de ciberataques permitiria que as equipes de resposta a incidentes aprimorassem suas habilidades e se preparassem para cenários do mundo real. Como enfatiza Stoltenberg (2023), a OTAN está perfeitamente posicionada para compartilhar informações, disseminar inovação e coordenar nossa defesa coletiva no ciberespaço. Nesse contexto, a cooperação internacional se torna essencial para enfrentar as crescentes ameaças digitais.

A promoção de iniciativas de pesquisa conjunta também é fundamental. Ambas as nações têm expertise em cibersegurança, e a colaboração em projetos de pesquisa pode levar ao desenvolvimento de soluções inovadoras para problemas cibernéticos compartilhados. Essa

colaboração deve incluir universidades, centros de pesquisa e indústrias de tecnologia, criando um ecossistema que fomente a inovação e a troca de conhecimento. Essa visão destaca a importância de construir relações pessoais e redes de contato que possibilitem uma resposta mais rápida e eficaz às ameaças cibernéticas.

A promoção de iniciativas de pesquisa conjunta também é fundamental. Ambas as nações têm expertise em cibersegurança, e a colaboração em projetos de pesquisa pode levar ao desenvolvimento de soluções inovadoras para problemas cibernéticos compartilhados. Essa colaboração deve incluir universidades, centros de pesquisa e indústrias de tecnologia, criando um ecossistema que fomente a inovação e a troca de conhecimento.

5.2 Propostas para a criação de novos acordos e políticas colaborativas

Brasil e Reino Unido devem considerar a formalização de acordos de cooperação que detalhem áreas específicas de colaboração, como resposta a incidentes cibernéticos, troca de informações sobre ameaças e vulnerabilidades, e a criação de um protocolo para lidar com cibercrimes. Esses acordos devem ser orientados por um compromisso mútuo em promover a segurança cibernética e a resiliência das infraestruturas críticas. É essencial que ambos os países se comprometam a participar ativamente em fóruns internacionais de cibersegurança, como a Convenção de Budapeste sobre Cibercrime, para garantir que suas preocupações e interesses sejam representados no cenário global.

O envolvimento em discussões multilaterais pode proporcionar uma plataforma para que Brasil e Reino Unido compartilhem suas experiências e colaborem em questões que transcendem fronteiras nacionais, ampliando a eficácia de suas estratégias de segurança cibernética.

6 Considerações finais

O estudo demonstrou a importância crescente dessa parceria frente aos desafios impostos por um ambiente digital cada vez mais vulnerável e interconectado. A análise das ameaças cibernéticas enfrentadas por ambos os países revelou não apenas a sofisticação dos ataques, mas também a necessidade de uma abordagem integrada e colaborativa para enfrentá-los.

No decorrer da pesquisa, ficou evidente que, enquanto Reino Unido apresenta uma estrutura mais consolidada em termos de estratégias de segurança cibernéticas, o Brasil ainda enfrenta dificuldades relacionadas à fragmentação institucional e à implementação de políticas eficazes. Apesar disso, os avanços observados, como a criação da Estratégia Nacional de

Segurança Cibernética (*E-Ciber*), mostram o compromisso do Brasil em alinhar-se às melhores práticas internacionais.

A cooperação entre os dois países, materializada por meio de acordo bilaterais e ações conjuntas, destaca-se como um modelo promissor para enfrentar ameaças cibernéticas globais. A troca de informações, o fortalecimento de capacidades e a promoção de iniciativas de conscientização são passos fundamentais para a construção de uma resiliência cibernética robusta.

Recomenda-se que futuros estudos aprofundem a análise de como as diferenças culturais, institucionais e tecnológicas influenciam essa cooperação, assim como explorem o impacto de novas tecnologias emergentes nesse cenário. Além disso, é essencial que políticas e acordos sejam constantemente revisados para acompanhar a evolução rápida das ameaças cibernéticas.

Referências

BRASIL. Decreto n.º 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, seção 1, Brasília, DF, ano 157, n. 26, p. 1, 6 fev. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 08 ago. 2025.

BRASIL. Decreto n.º 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**: seção 1, Brasília, DF, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 08 ago. 2025.

BRASIL. Ministério das Relações Exteriores. Fifth Brazil–United Kingdom High–Level Strategic Dialogue – Joint Communiqué. **Ministério das Relações Exteriores**, Brasília, DF, 09 out. 2020. Disponível em: https://www.gov.br/mre/en/contact-us/press-area/press-releases/fifth-brazil-united-kingdom-high-level-strategic-dialogue-joint-communique. Acesso em: 08 ago. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Brasil fortalece parceria com Reino Unido na transformação digital do setor público. **Ministério da Gestão e da Inovação em Serviços Públicos**, Brasília, DF, 14 nov. 2023. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/novembro/brasil-fortalece-parceria-com-reino-unido-na-transformacao-digital-do-setor-publico. Acesso em: 08 ago. 2025.

BRASIL. Secretaria de Comunicação Social. O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais. **Secretaria de Comunicação Social**, Brasília, DF, 29 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais. Acesso em: 08 ago. 2025.

DELOITTE. Cybersecurity threat trends. **Deloitte**, 14 ago. 2023. Disponível em: https://www.deloitte.com/us/en/insights/topics/risk-management/global-cybersecurity-threat-trends.html. Acesso em: 11 ago. 2025.

DEVANNY, J; BUCHAN, R. Brazil's cyber strategy under Lula: not a priority, but progress is possible. **Carnegie Endowment for International Peace**, 08 ago. 2023. Disponível em: https://carnegieendowment.org/research/2023/08/brazils-cyber-strategy-under-lula-not-a-priority-but-progress-is-possible?lang=en. Acesso em: 08 ago. 2025.

HM GOVERNMENT. **Estratégia nacional de segurança cibernética 2016-2021**. London: Cabinet Office, 2016. Disponível em: https://assets.publishing.service.gov.uk/media/5a82408d40f0b62305b934bb/Brazilian_Portuguese_translation_-_National_Cyber_Security_Strategy_2016.pdf. Acesso em: 08 ago. 2025.

IISS - The International Institute for Strategic Studies. **Cyber Capabilities and National Power**, v. 2**.** Brazil. Disponível em: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_04-brazil.pdf. Acesso em: 08 ago. 2025.

NATO COMMUNICATIONS AND INFORMATION AGENCY. **NCIA participates in cyber defence exercise Locked Shields**. Bruxelas, 25 abr. 2024. Disponível em: https://www.ncia.nato.int/about-us/newsroom/ncia-participates-in-cyber-defence-exercise-locked-shields. Acesso em: 08 ago. 2025.

NATIONAL CYBER SECURITY CENTRE (NCSC). **Annual Review 2023**. [S. l.], [s. d.]. Disponível em: https://www.ncsc.gov.uk/collection/annual-review-2023.

CIDH adota medidas cautelares de proteção para membros do povo indígena Munduruku no Brasil. **OEA**, 16 dez. 2020. Disponível em: https://www.oas.org/pt/cidh/prensa/notas/2020/302.asp. Acesso em: 08 ago. 2025.

RANSOMWARE TASK FORCE. **2023 Global Ransomware Incident Map**. Security and Technology, 2023. Disponível em: https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map/. Acesso em: 08 ago. 2025.

STOLTENBERG, J. **Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference.** Berlim: NATO, 2023. Disponível em: https://www.nato.int/cps/en/natohq/news_219850.htm. Acesso em: 08 ago. 2025.

UNITED KINGDOM. Cabinet Office. **National Cyber Strategy 2022**. London, 15 dez. 2021. Atualizado em: 15 dez. 2022. Disponível em: https://www.gov.uk/government/publications/national-cyber-strategy-2022. Acesso em: 08 ago. 2025.

ZANELLATO, M. A. Condutas ilícitas na sociedade digital**. Revista de Direito do Consumidor**, São Paulo, v. 11, n. 44, p. 206-261, out. 2002.

Data de submissão: 11 de dezembro de 2024
Data de aceite: 26 de março de 2025