Anais do Congresso Brasileiro de Iniciação Científica
(https://periodicos.unisanta.br/COB)

ISSN 2317-1316

DIPLOMACIA CIBERNÉTICA NO REINO UNIDO

CYBER DIPLOMACY IN THE UNITED KINGDOM

Henzo Lima Teixeira, Paloma Ramos de Lima, Jéssica Maria Grassi

Universidade Santa Cecília, Curso de Relações Internacionais
E-mail para contato: henzo.lteixeira@gmail.com

RESUMO – O artigo analisa a estruturação e a implementação das estratégias cooperativas e diplomáticas do Reino Unido para a construção de seu poder e segurança no ciberespaço. Diante da cooperação internacional, a pesquisa investiga como o Estado britânico articula suas capacidades domésticas avançadas para atuar nos principais fóruns internacionais. Mediante abordagem qualitativa e método hipotético-dedutivo, os resultados corroboram que o Reino Unido fortalece sua ciberdiplomacia para projetar liderança, defender a aplicação do Direito Internacional, difundir normas voluntárias de comportamento estatal responsável e impulsionar a governança multissetorial, integrando resiliência interna, cooperação defensiva e programas internacionais de capacitação cibernética.

Palavras-chave: Ciberdiplomacia; Reino Unido; Poder Cibernético; Governança Cibernética; Cooperação Internacional.

ABSTRACT – This article analyzes the structuring and implementation of the United Kingdom's cooperative and diplomatic strategies for building its power and security in cyberspace. In the face of international cooperation, the research investigates how the British State leverages its advanced domestic capabilities in key international forums. Using a qualitative approach and a hypothetical-deductive method, the results confirm that the UK strengthens its cyber diplomacy to project leadership, defend International Law, promote voluntary norms of responsible state behavior, and champion multistakeholder governance, integrating domestic resilience, defensive cooperation, and international cyber capacity building programs.

Keywords: Cyber Diplomacy; United Kingdom; Cyber Power; Cyber Governance; International Cooperation.

ISSN 2317-1316

1 INTRODUÇÃO

Nas últimas décadas, a rápida transformação digital e o adensamento da conectividade global converteram o ciberespaço em uma dimensão central para a política internacional, a segurança e a projeção do poder estatal (Attatfa et al., 2020; Barrinha; Renard, 2017). Ao extrapolar os domínios operacionais tradicionais - terrestre, marítimo, aéreo e espacial -, o ambiente cibernético instaurou um novo locus de competição geopolítica. A intrínseca transnacionalidade das redes virtuais, aliada à crescente dependência de infraestruturas críticas em setores vitais como energia, finanças e defesa, amplificou a vulnerabilidade dos Estados diante de ameaças complexas, tais como ciberespionagem, cibercrime sofisticado e campanhas de desinformação (Ayres Pinto; Grassi, 2021). Nesse cenário, o conceito de poder cibernético (*cyber power*) consolidou-se como a capacidade dos atores estatais de utilizarem recursos digitais para salvaguardar e promover seus interesses estratégicos (Nye Jr., 2011; Voo et al., 2022). Todavia, em função da hiperconectividade e da dificuldade de atribuição técnica dos ataques, a busca exclusiva pela segurança por meios estritamente militares revela-se insuficiente, tornando a coordenação internacional um pressuposto indispensável (Grassi; Ayres Pinto; Pagliari, 2024).

Nesse contexto de interdependência, a diplomacia cibernética emerge como um instrumento fundamental no portfólio de política externa e de defesa dos Estados (Christou, 2024). Conceituada como o emprego de recursos e canais diplomáticos para gerenciar conflitos, estabelecer normas de comportamento estatal responsável, construir medidas de fortalecimento da confiança (CBMs, do inglês *Confidence-Building Measures*) e estruturar a governança global da internet, a ciberdiplomacia diferencia-se do mero uso de ferramentas digitais no exercício diplomático tradicional (Barrinha; Renard, 2017). A ação diplomática no ciberespaço volta-se para a construção de um ambiente estável e previsível, buscando conciliar as visões soberanas dos Estados com a governança multissetorial (*multistakeholder*) da rede. Por conseguinte, a cooperação internacional, exercida em fóruns multilaterais como o Grupo de Peritos Governamentais (GGE/UN) e o Grupo de Trabalho de Composição Aberta das Nações Unidas (OEWG/UN), ou via arranjos plurilaterais e bilaterais, desempenha papel decisivo na mitigação de conflitos digitais (Sukumar et al., 2024).

ISSN 2317-1316

A escolha do Reino Unido como objeto central desta investigação justifica-se por seu posicionamento de destaque no ecossistema cibernético global, figurando de maneira consistente nos primeiros lugares de diagnósticos internacionais como o Global Cybersecurity Index (GCI) da União Internacional de Telecomunicações (UIT) e o National Cyber Power Index (NCPI) do Belfer Center for Science and International Affairs da Harvard Kennedy School (Voo et al., 2022; Clark, 2025). O Estado britânico consolidou uma postura estratégica integrada mediante a publicação de diretrizes sucessivas, destacando-se a National Cyber Security Strategy 2016-2021 e a National Cyber Strategy 2022, respaldadas pela Revisão Integrada de Segurança, Defesa e Política Externa (Integrated Review) (United Kingdom, 2016, 2022b). Tais documentos articulam a cibersegurança doméstica à projeção externa de influência, combinando arranjos operacionais inovadores, como o National Cyber Security Centre (NCSC) e a National Cyber Force (NCF), com a meta explícita de posicionar o país como uma "potência cibernética democrática e responsável" (*responsible cyber power*) (United Kingdom, 2023).

Diante disso, o presente trabalho responde a seguinte pergunta de pesquisa: De que forma medidas cooperativas e diplomáticas têm sido estruturadas e implementadas pelo Reino Unido para a construção de poder e segurança cibernética? Como resposta provisória, sustenta-se a hipótese de que o Reino Unido, impulsionado por suas avançadas e consolidadas capacidades cibernéticas domésticas, vem fortalecendo políticas e estratégias de diplomacia cibernética a fim de projetar liderança, ditar padrões normativos e promover seus interesses de governança nos principais fóruns internacionais. Em vista disso, o objetivo geral do estudo consiste em analisar a estruturação e a implementação das estratégias cooperativas e diplomáticas britânicas voltadas à consolidação de seu poder cibernético e ao reforço da segurança internacional.

A relevância acadêmica e prática da pesquisa fundamenta-se na necessidade de adensar a compreensão empírica sobre a convergência entre capacidades cibernéticas e ação diplomática (Attatfa et al., 2020; Barrinha; Renard, 2017; Grassi, 2023). Ademais, a investigação oferece subsídios para o debate sobre a ciberdiplomacia no Brasil que, embora venha desenvolvendo normativas e instituições, ainda enfrenta desafios operacionais na implementação de estratégias diplomáticas proativas e no fortalecimento da cooperação regional (Ayres Pinto; Grassi, 2021; Grassi, 2023; Grassi et al., 2024). A análise do caso britânico fornece, assim, referências

ISSN 2317-1316

analíticas para o aprimoramento das políticas públicas e da inserção internacional brasileira no domínio cibernético.

2 MATERIAIS E MÉTODOS

A pesquisa adota uma abordagem qualitativa, de caráter exploratório, descritivo e analítico, orientada à interpretação das estratégias institucionais e ações diplomáticas do Estado no domínio digital (Attatfa et al., 2020; Schwether; Oliveira, 2024). O percurso investigativo estrutura-se a partir do método hipotético-dedutivo, tomando como ponto de partida o problema de pesquisa e a hipótese formulada, submetendo-a ao confronto sistemático com o material empírico reunido.

Para a constituição empírica (os materiais), empregam-se os procedimentos de revisão bibliográfica e levantamento documental. As fontes primárias oficiais compreendem os principais documentos estratégicos publicados pelo governo do Reino Unido e por suas agências, destacando-se a National Cyber Security Strategy 2016-2021, a National Cyber Strategy 2022, os relatórios da Integrated Review, a Government Cyber Security Strategy 2022-2030, as publicações operacionais do National Cyber Security Centre (NCSC) e da National Cyber Force (NCF), além das submissões oficiais do país ao Grupo OEWG da ONU (United Kingdom, 2016, 2020, 2022a, 2022b, 2023). As fontes secundárias englobam relatórios de centros de pesquisa internacionais, livros e artigos científicos especializados em Relações Internacionais, segurança internacional e ciberdiplomacia (Clark, 2025; Lațici, 2020; Niestadt, 2026; Christou, 2024; Barrinha; Renard, 2017).

Os procedimentos de análise organizam-se mediante a técnica de análise documental e categorial-discursiva, efetuando-se a triagem e o mapeamento dos objetivos estratégicos e dos posicionamentos diplomáticos britânicos em instâncias como a ONU, a OTAN, e a OSCE. O estudo diferencia claramente as análises da literatura acadêmica especializada, responsável por fornecer a interpretação conceitual da política internacional e da governança digital, dos dados e diretrizes contidos nos documentos oficiais britânicos, que provêm as evidências empíricas sobre as capacidades, instituições e iniciativas diplomáticas do país.

3 RESULTADOS E DISCUSSÃO

ISSN 2317-1316

3.1 A construção do poder cibernético britânico

A análise sobre a formação e a projeção do poder cibernético do Reino Unido exige compreender que o poder digital não se reduz à mera acumulação de ativos tecnológicos ou infraestruturas computacionais (Nye Jr., 2011; Steed, 2021; Schwether; Oliveira, 2024). O relatório *Cybersecurity in the UK*, elaborado pela *House of Commons Library*, e a *National Cyber Strategy 2022* evidenciam que a postura estratégica britânica evoluiu de um foco reativo em "segurança cibernética" na estratégia de 2016 para a afirmação categórica do "poder cibernético" (*cyber power*) na diretriz de 2022 e na *Integrated Review* (Clark, 2025; United Kingdom, 2016, 2022b). O governo britânico define formalmente o poder cibernético como "a capacidade de proteger e promover interesses nacionais no e através do ciberespaço" (United Kingdom, 2022b). Essa conceituação integra capacidades técnicas, resiliência institucional e legitimidade normativa como componentes indissociáveis do poder estatal.

A pedra angular dessa construção estratégica repousa sobre a definição institucional do Reino Unido como uma "potência cibernética democrática e responsável" (*leading democratic and responsible cyber power*) (United Kingdom, 2022b, 2023; Steed, 2021). Essa diretriz autodeclarada orienta a conduta interna e externa do Estado, estabelecendo uma clara diferenciação em relação a atores enquadrados pelo discurso oficial britânico como "competidores sistêmicos" (como Rússia e China), cujas ações no ciberespaço são associadas ao autoritarismo digital e à desestabilização da ordem baseada em regras (United Kingdom, 2022b, 2024). A busca por poder cibernético no Reino Unido é, assim, vinculada à defesa da prosperidade econômica, da democracia, do Estado de Direito e dos direitos humanos.

A autoridade e a credibilidade do Reino Unido no cenário internacional dependem intrinsecamente do fortalecimento de sua resiliência cibernética doméstica, conforme sinaliza a *Government Cyber Security Strategy 2022-2030* (United Kingdom, 2022a). A criação do *National Cyber Security Centre* (NCSC) em 2016, enquanto autoridade técnica nacional no âmbito do *Government Communications Headquarters* (GCHQ), centralizou a resposta a incidentes e estabeleceu um canal permanente de cooperação entre o governo, o setor privado, a academia e a sociedade civil (Clark, 2025; United Kingdom, 2016). Essa arquitetura operacional viabiliza a implementação da abordagem "*whole-of-society*" (toda a sociedade) consagrada na *National Cyber Strategy 2022* (United Kingdom, 2022b). Por meio de instrumentos como o Cyber Assessment Framework (CAF) e o programa *Active Cyber Defence*

ISSN 2317-1316

(ACD), o Estado compartilha a responsabilidade pela segurança com operadores de infraestruturas críticas e grandes empresas de tecnologia, consolidando a resiliência nacional como uma prática institucionalizada.

No âmbito defensivo e ofensivo avançado, a consolidação da *National Cyber Force* (NCF) em 2020 — integrando o Ministério da Defesa (MOD), o GCHQ, o *Secret Intelligence Service* (SIS/MI6) e o *Defence Science and Technology Laboratory* (DSTL) — representa um marco na capacidade operacional do país para conduzir operações cibernéticas de disrupção contra ameaças graves (United Kingdom, 2023; Clark, 2025). O documento oficial *The National Cyber Force: Responsible Cyber Power in Practice* estabelece que o emprego de capacidades ofensivas é estritamente pautado pela proporcionalidade, necessidade e conformidade com o Direito Internacional (United Kingdom, 2023). A conduta da NCF é submetida a marcos legais consolidados, como a *Intelligence Services Act 1994* e a *Investigatory Powers Act 2016*, exigindo autorizações ministeriais, supervisão do *Investigatory Powers Commissioner* e fiscalização parlamentar (United Kingdom, 2023; Clark, 2025). A publicação aberta dessa doutrina busca demonstrar transparência e estabelecer padrões comportamentais para a condução responsável de operações cibernéticas estatais.

Essa visão holística do poder cibernético organiza-se formalmente nos cinco pilares da *National Cyber Strategy 2022* (United Kingdom, 2022b):

1. Fortalecimento do ecossistema cibernético nacional;
2. Construção de resiliência e prosperidade digital;
3. Liderança e soberania em tecnologias críticas;
4. Ampliação da liderança e influência global;
5. Detecção, disrupção e dissuasão de adversários.

Ao integrar a inovação tecnológica interna (Pilar 3) à projeção diplomática externa (Pilar 4), o Reino Unido estrutura uma estratégia na qual a resiliência doméstica e a capacidade operacional sustentam a sua liderança internacional.

3.2 Governança internacional e diplomacia cibernética no Reino Unido

A diplomacia cibernética constitui o principal vetor de projeção externa e de afirmação estratégica do Reino Unido no cenário digital (Steed, 2021; Christou, 2024). Conforme

ISSN 2317-1316

estipulado no Pilar 4 da *National Cyber Strategy 2022*, o Estado britânico direciona suas ações diplomáticas para a promoção de um ciberespaço livre, aberto, pacífico e seguro (United Kingdom, 2022b). A ciberdiplomacia britânica atua como um instrumento proativo projetado para moldar as regras do ambiente digital, expandir alianças e converter a capacitação técnica do país em autoridade política internacional (Steed, 2021; United Kingdom, 2022b).

No âmbito das Nações Unidas, o engajamento multilateral do Reino Unido destaca-se por sua atuação propositiva no Grupo de Peritos Governamentais (UN GGE) e no Grupo de Trabalho de Composição Aberta (OEWG) (United Kingdom, 2020; Sukumar et al., 2024). A diplomacia britânica figura como defensora central do acervo (acquis) de segurança cibernética da ONU, priorizando o cumprimento e a universalização das 11 normas voluntárias e não vinculantes de comportamento estatal responsável pactuadas nos relatórios de consenso do UN GGE (United Kingdom, 2020). A prioridade britânica consiste em operacionalizar as normas existentes, opondo-se à criação de novos tratados juridicamente vinculantes que possam fragmentar os consensos alcançados.

O Reino Unido defende formalmente que o Direito Internacional vigente aplica-se integralmente ao ciberespaço, incluindo a Carta das Nações Unidas, a proibição do uso ou ameaça da força (Artigo 2º, § 4º), o princípio de não intervenção (Artigo 2º, § 7º), o direito de legítima defesa (Artigo 51) e o Direito Internacional Humanitário em contextos de conflito armado (United Kingdom, 2020). Além disso, o país recorre à atribuição política pública *(naming and shaming*) de ciberataques maliciosos promovidos por atores estatais adversários para elevar os custos reputacionais das violações (Clark, 2025). Essa postura estendeu-se às negociações da Convenção da ONU contra o Cibercrime, nas quais o Reino Unido condicionou sua cooperação à inclusão de salvaguardas expressas relativas aos direitos humanos (Clark, 2025; United Kingdom, 2022b).

Paralelamente, o Reino Unido promove firmemente o modelo de governança multissetorial (*multistakeholder*), advogando que a gestão da internet deve incorporar o setor privado, a academia e a sociedade civil em fóruns como a ICANN e o Internet Governance Forum (IGF) (United Kingdom, 2022b; Radanliev, 2025). Essa posição contrapõe-se às propostas de "soberania cibernética estatal restritiva" promovidas por blocos como a Organização para Cooperação de Xangai (SCO). Em uma iniciativa plurilateral de destaque, o

ISSN 2317-1316

Reino Unido e a França lançaram em 2024 o Pall Mall Process, reunindo governos, empresas de tecnologia e sociedade civil para estabelecer marcos de transparência e prestação de contas no combate à proliferação irresponsável de ferramentas comerciais de intrusão cibernética (*spyware*) (United Kingdom, 2024).

No campo da segurança regional e das alianças defensivas, o Reino Unido utiliza acordos plurilaterais e bilaterais para garantir a interoperabilidade estratégica e a contenção de ameaças. No âmbito do *Five Eyes*, o país mantém cooperação contínua via *Five Eyes Cyber Crime Working Group* (Clark, 2025). Na OTAN, desempenhou papel determinante na consolidação do ciberespaço como domínio operacional oficial a partir da Cúpula de Varsóvia de 2016 e na implementação do *Cyber Defence Pledge*, disponibilizando voluntariamente capacidades cibernéticas operacionais da NCF para a Aliança (Olech; Štrucl, 2025; United Kingdom, 2023). Na Organização para a Segurança e Cooperação na Europa (OSCE), impulsionou a aplicação de Medidas de Fortalecimento da Confiança (CBMs) para prevenir erros de cálculo (United Kingdom, 2020). No contexto pós-Brexit, a cooperação digital com a União Europeia evolui pragmaticamente em fóruns de resiliência e combate a ameaças híbridas (Niestadt, 2026; Lațici, 2020), articulando-se às diretrizes da *Commonwealth Cyber Declaration* e a parcerias bilaterais com Estados Unidos, Japão, Austrália, Índia, Polônia e França (United Kingdom, 2022b).

Por fim, a política de capacitação cibernética internacional (CCB, do inglês *Cyber Capacity Building*) constitui um elemento estratégico da diplomacia britânica. Como membro do *Global Forum on Cyber Expertise* (GFCE), o Reino Unido financia programas globais como o *Digital Access Programme*, voltado ao fortalecimento da governança e resiliência digital em países em desenvolvimento na África, Ásia e América Latina, incluindo ações no Brasil (United Kingdom, 2022b). O governo britânico também apoiou a aplicação do modelo de maturidade CMM (*Cybersecurity Capacity Maturity Model*), desenvolvido pelo *Global Cyber Security Capacity Centre* (GCSCC) da Universidade de Oxford, em mais de cem nações (Global Cyber Security Capacity Centre, 2016; Radanliev, 2025). Ao elevar a resiliência institucional de parceiros no Sul Global, o Reino Unido reduz vulnerabilidades em cadeias de suprimento digitais, previne o avanço de modelos autoritários de controle da rede e consolida uma comunidade internacional alinhada a um ciberespaço estável e baseado no Direito Internacional.

ISSN 2317-1316

4 CONCLUSÃO

Esta pesquisa alcançou seu objetivo geral ao analisar como as medidas cooperativas e diplomáticas do Reino Unido têm sido estruturadas e implementadas para a construção de seu poder e segurança cibernética, demonstrando que a cooperação internacional e o engajamento normativo constituem pilares centrais dessa arquitetura. Os resultados respondem diretamente ao problema de pesquisa e corroboram a hipótese inicial de que o Estado britânico instrumentaliza suas avançadas capacidades domésticas para projetar liderança, difundir padrões comportamentais e promover seus interesses de governança nos principais fóruns internacionais. O estudo evidencia que a autoridade digital britânica não decorre apenas do acúmulo de recursos técnicos operacionais, mas de uma ação diplomática abrangente pautada pela afirmação da identidade de "potência cibernética democrática e responsável", pela defesa do acervo normativo da ONU (GGE e OEWG), pelo fortalecimento de alianças defensivas (OTAN e Five Eyes), pelo apoio ao modelo *multistakeholder* e pela difusão de capacitação cibernética no Sul Global. Como desdobramento deste trabalho, recomenda-se a realização de pesquisas futuras dedicadas à análise comparada sobre a recepção e os impactos da ciberdiplomacia britânica em países em desenvolvimento, bem como ao acompanhamento dos efeitos de arranjos plurilaterais emergentes na governança global. Por fim, registra-se o sincero agradecimento pelo apoio financeiro concedido pela Bolsa PICd — Programa de Iniciação Científica da Universidade Santa Cecília (Unisanta), à orientadora, Profa. Dra. Jéssica Maria Grassi, pela orientação e pelo acompanhamento acadêmico, e à Paloma Ramos de Lima, parceira de pesquisa no projeto guarda-chuva "A Ciberdiplomacia das Potências Mundiais" — desenvolvido no âmbito do Grupo de Pesquisa de Ambiente Digital Aplicado às Relações Internacionais da Unisanta —, pela colaboração prestada ao longo do trabalho.

5 DECLARAÇÃO DE USO DE IA

Declaração de Uso de IA: Durante a elaboração deste trabalho, utilizou-se a ferramenta NotebookLM para auxiliar na síntese, organização e documentação das fontes bibliográficas e documentais, e a ferramenta ChatGPT como recurso auxiliar na revisão textual. O conteúdo gerado foi revisado, editado e validado pelos autores, que assumem total responsabilidade pelo texto final.

ISSN 2317-1316

6 REFERÊNCIAS

ATTATFA, Amel; RENAUD, Karen; DE PAOLI, Stefano. Cyber diplomacy: a systematic literature review. **Procedia Computer Science**, v. 176, p. 60–69, 2020. DOI: https://doi.org/10.1016/j.procs.2020.08.007. Acesso em: 10 out. 2026.

AYRES PINTO, Danielle; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, p. 28–38, 2021. DOI: https://doi.org/10.26792/rbed.v7n2.2020.75178. Acesso em: 10 out. 2026.

BARRINHA, André; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**, v. 3, n. 4-5, p. 353–364, 2017. DOI: https://doi.org/10.1080/23340460.2017.1414924. Acesso em: 10 out. 2026.

CHRISTOU, George. **Cyber diplomacy: from concept to practice**. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2024. (Tallinn Paper, n. 14). Disponível em: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf. Acesso em: 10 out. 2026.

CLARK, Adam. **Cybersecurity in the UK**. House of Commons Library, CBP-9821, 23 dez. 2025. Disponível em: https://commonslibrary.parliament.uk/research-briefings/cbp-9821/. Acesso em: 10 out. 2026.

GLOBAL CYBER SECURITY CAPACITY CENTRE. **Cybersecurity capacity review of the United Kingdom**. Oxford: University of Oxford, nov. 2016. Disponível em: https://gcscc.ox.ac.uk/files/cybersecuritycapacityreviewoftheunitedkingdompdf. Acesso em: 10 out. 2026.

GRASSI, Jéssica Maria. **A construção de capacidades cibernéticas e os processos cooperativos no contexto geopolítico sul-americano: políticas e estratégias de Argentina, Brasil e Colômbia.** 2023. 251 f. Tese (Doutorado em Relações Internacionais) – Centro Socioeconômico, Programa de Pós-Graduação em Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/253958. Acesso em 17 out. 2026

GRASSI, Jéssica Maria; AYRES PINTO, Danielle Jacon Ayres; PAGLIARI, Graciela de Conti. Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas. **Relações Internacionais**, n. 82, p. 11–27, jun. 2024. DOI: https://doi.org/10.23906/ri2024.82a02. Acesso em: 10 out. 2026.

LAȚICI, Tania. **Understanding the EU's approach to cyber diplomacy and cyber defence**. European Parliamentary Research Service (EPRS), Briefing PE 651.937, maio 2020. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282020%29651937. Acesso em: 10 out. 2026.

ISSN 2317-1316

NIESTADT, Maria. **EU-UK digital cooperation**. European Parliamentary Research Service (EPRS), At a glance, PE 785.655, mar. 2026. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282026%29785655. Acesso em: 10 out. 2026.

NYE JR., Joseph S. **The future of power**. New York: Public Affairs, 2011.

OLECH, Aleksander; ŠTRUCL, Damjan. **The evolution of cyber forces in NATO countries**. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2025. Disponível em: https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf. Acesso em: 10 out. 2026.

RADANLIEV, Petar. Cyber diplomacy: defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. **Journal of Cyber Security Technology**, v. 9, n. 1, p. 28–78, 2025 [publicado online em 2024]. DOI: https://doi.org/10.1080/23742917.2024.2312671. Acesso em: 10 out. 2026.

SCHWETHER, Natália Diniz; OLIVEIRA, Marcos Aurélio Guedes de. A cibernética na grande estratégia: um estudo comparado de Reino Unido, França e Portugal. **Relações Internacionais**, n. 82, p. 29–43, jun. 2024. DOI: https://doi.org/10.23906/ri2024.82a03. Acesso em: 10 out. 2026.

STEED, Danny. The UK's Integrated Review and the future of cyber. **Elcano Royal Institute**, ARI 63/2021, 1 jul. 2021. Disponível em: https://www.realinstitutoelcano.org/en/analyses/the-uks-integrated-review-and-the-future-of-cyber/. Acesso em: 10 out. 2026.

SUKUMAR, Arun; BROEDERS, Dennis; KELLO, Monica. The pervasive informality of the international cybersecurity regime: geopolitics, non-state actors and diplomacy. **Contemporary Security Policy**, v. 45, n. 1, p. 7–44, 2024. DOI: https://doi.org/10.1080/13523260.2023.2296739. Acesso em: 10 out. 2026.

UNITED KINGDOM. **National Cyber Security Strategy 2016 to 2021**. London: HM Government, 2016. Disponível em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. Acesso em: 10 out. 2026.

UNITED KINGDOM. **Contribution made in February 2020 by United Kingdom to the Open-Ended Working Group (OEWG)**. 2020. Disponível em: https://eucyberdirect.eu/atlas/sources/contribution-by-united-kingdom-to-the-oewg. Acesso em: 10 out. 2026.

UNITED KINGDOM. Cabinet Office. **Government Cyber Security Strategy 2022–2030**. London: HM Government, 2022a. Disponível em: https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf. Acesso em: 10 out. 2026.

ISSN 2317-1316

UNITED KINGDOM. Cabinet Office. **National Cyber Strategy 2022: pioneering a cyber future with the whole of the UK**. London: HM Government, 2022b. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf. Acesso em: 10 out. 2026.

UNITED KINGDOM. National Cyber Force. **The National Cyber Force: responsible cyber power in practice**. HM Government, 2023. Disponível em: https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf. Acesso em: 10 out. 2026.

UNITED KINGDOM. **Cybersecurity Policy**. London: GOV.UK, compilação atualizada em maio de 2024.

VOO, Julia; HEMANI, Irfan; CASSIDY, Daniel. **National Cyber Power Index 2022**. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, set. 2022. Disponível em: https://www.belfercenter.org/publication/national-cyber-power-index-2022. Acesso em: 10 out. 2026.