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

ISSN 2317-1316

A CIBERDIPLOMACIA DAS POTÊNCIAS MUNDIAIS

THE CYBER DIPLOMACY OF WORLD POWERS

Nicoly Fontes Feitosa, Clara Marques Soares, Paloma Ramos de Lima, Giovanna Marcely Oliveira da Silva, Ana Luiza Lopes Fernandes Pitta, Jéssica Maria Grassi

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

RESUMO – A pesquisa analisa a ciberdiplomacia de potências mundiais, investigando como os Estados utilizam o ciberespaço para promover interesses nacionais, exercer influência internacional e fortalecer sua segurança. A pesquisa aborda estratégias, capacidades cibernéticas e mecanismos de cooperação, considerando seus impactos na governança global e nas relações internacionais. Os resultados indicam que a ciberdiplomacia é mais do que um complemento nas políticas de cibersegurança, ela integra o próprio processo de construção do poder cibernético dos Estados. Contudo, o modo como cada país a emprega varia conforme sua posição no sistema internacional e sua concepção de governança.

Palavras-chave: Ciberdiplomacia; Potências mundiais; Cibersegurança; Governança internacional; Relações Internacionais.

ABSTRACT – The study analyses the cyber diplomacy of world powers, investigating how states use cyberspace to advance national interests, exert international influence, and strengthen security. It addresses cyber strategies, capabilities, and cooperation mechanisms, considering their impacts on global governance and international relations. The findings indicate that cyber diplomacy is more than a complement to cybersecurity policies: it is an integral part of the process through which states build cyber power. However, the way each country employs it varies according to its position in the international system and its conception of governance.

Keywords: Cyber diplomacy; World powers; Cybersecurity; International governance; International relations.

1 INTRODUÇÃO

O ciberespaço se concentra como um domínio moldado pelo ser humano, sustentado por redes digitais, infraestruturas de comunicação e fluxos contínuos de informação. Pode ser definido como um domínio operacional usado para compartilhar informações via sistemas

ISSN 2317-1316

interconectados e suas infraestruturas associadas (Nye, 2011). Com a amplitude do ciberespaço e dos atores que atuam por meio dele, tem-se o surgimento da ciberdiplomacia, um campo específico da diplomacia que se formou em razão da necessidade dos Estado em assegurar seus interesses estratégicos no que diz respeito ao ciberespaço (Barrinha; Renard, 2017).

Ao definir a capacitação e o poder cibernético dos Estados, especialistas elencam uma série de dimensões e, entre elas, estão as capacidades diplomáticas (IISS, 2021; Voo; Hemani; Cassidy, 2022; ITU, 2024). Tendo isso em vista, o presente estudo busca analisar como os países com capacidades cibernéticas relevantes estruturam e implementam estratégias diplomáticas voltadas à construção de capacidades estatais, à projeção de poder e à promoção da segurança no ciberespaço. Para alcançar esse propósito, foram examinadas as práticas de ciberdiplomacia da França, do Reino Unido, da Rússia e da Indonésia. A escolha desses países foi baseada, principalmente, pela posição que ocupam no Global Cybersecurity Index (GCI) da União Internacional de Telecomunicações (UIT). O índice classifica os países pela maturidade de suas capacidades em segurança cibernética a partir de quatro pilares: medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidades e medidas de cooperação.

Por fim, o estudo tem como objetivo reforçar a relevância dos estudos da ciberdiplomacia no Brasil. O mapeamento e a sistematização de documentos, estratégias e práticas dos países analisados contribuem para aprofundar a compreensão da atuação diplomática no ambiente cibernético de suas implicações para as Relações Internacionais.

2 MATERIAIS E MÉTODOS

Metodologicamente, o estudo adota uma abordagem qualitativa, de caráter descritivo-analítico, fundamentada em pesquisa bibliográfica e documental. O repertório da pesquisa foi composto por documentos oficiais, como estratégias nacionais de cibersegurança, doutrinas, legislações, declarações e relatórios governamentais, e por fontes secundárias, como artigos científicos, livros, teses e dissertações e relatórios de instituições internacionais. A análise combinou as duas categorias, de modo a confrontar o discurso oficial de cada país com a interpretação da literatura acadêmica e com os indicadores comparados dos índices internacionais - como o Global Cybersecurity Index (GCI), o National Cyber Security Index (NCSI) e o National Cyber Power Index (NCPI). Conforme mencionado na seção anterior, a

ISSN 2317-1316

escolha dos quatro países se deu pela posição que eles ocupam nesses índices.

A pesquisa foi desenvolvida no âmbito do Programa de Iniciação Científica (PICv) e do Grupo de Pesquisa de Ambiente Digital Aplicado às Relações Internacionais, vinculado ao Curso de Relações Internacionais da Unisanta. Desse modo, o desenvolvimento da pesquisa contemplou a participação dos integrantes em reuniões periódicas do grupo, o que contribuiu para novos apontamentos e discussões, compartilhamento de conhecimentos, aprofundamento das análises e revisão dos métodos e resultados. As fontes foram interpretadas em seu contexto de produção, buscando fidelidade ao material e imparcialidade analítica, inclusive diante de perspectivas divergentes sobre a governança do ciberespaço.

3 RESULTADOS E DISCUSSÃO

3.1 A ciberdiplomacia da França

A análise do caso francês demonstra que a cibersegurança foi incorporada gradualmente à estratégia de segurança nacional, deixando de ser uma questão predominantemente técnica para assumir caráter estratégico. O marco inicial foi o Livro Branco de Defesa e Segurança Nacional de 2008, seguido da criação da ANSSI, em 2009, responsável pela proteção dos sistemas do Estado e das infraestruturas críticas, e do COMCYBER, em 2017, encarregado das operações militares (Brangetto, 2015; IISS, 2021). Essa evolução foi impulsionada pelo ataque à emissora TV5Monde, em 2015, e pelo vazamento de e-mails da campanha presidencial de Emmanuel Macron, em 2017, ambos ligados a grupos russos, além dos efeitos da guerra na Ucrânia (Barichella, 2022; ANSSI, 2026).

No plano doutrinário, a Revue Stratégique de Cyberdéfense, de 2018, marcou a passagem de uma postura essencialmente defensiva para um modelo de defesa ativa. Em 2019, o país tornou públicos, pela primeira vez, elementos de sua doutrina militar ofensiva (Delerue; Desforges; Géry, 2019; IISS, 2021). Ao contrário de aliados como o Reino Unido, a França tradicionalmente prefere tratar a identificação dos responsáveis por ataques por canais diplomáticos. Essa postura começa a mudar, já que a estratégia nacional para 2026–2030 inclui a atribuição pública entre as opções de resposta (Delerue; Desforges; Géry, 2019; France, 2026). Paralelamente, a dependência de tecnologias estrangeiras passou a ser vista como vulnerabilidade estratégica, tornando a autonomia tecnológica complementar à autonomia

ISSN 2317-1316

estratégica do país (France, 2015, 2026).

No âmbito internacional, e sem integrar a aliança Five Eyes, a França ancora sua atuação sobretudo na União Europeia. No bloco, teve papel de liderança na adoção das primeiras sanções contra responsáveis por ataques cibernéticos, em 2020 (IISS, 2021). Na ONU, defende a plena aplicação do Direito Internacional ao ciberespaço e apoia os processos sobre normas de comportamento estatal responsável (France, 2020, 2024). Sua principal iniciativa própria é o Paris Call for Trust and Security in Cyberspace, lançado em 2018 para reunir Estados, empresas e sociedade civil em torno de princípios de comportamento responsável. Em janeiro de 2020, a iniciativa contava com mais de mil signatários, entre eles 76 países, mas sem Estados Unidos, China e Rússia, o que limitava seu impacto (Ruhl et al., 2020). Em 2024, a França lançou com o Reino Unido o Pall Mall Process, voltado ao enfrentamento da proliferação de ferramentas comerciais de intrusão cibernética (United Kingdom; France, 2024).

No campo operacional, a capacidade de coordenação do arcabouço francês ficou evidente nos Jogos Olímpicos e Paralímpicos de Paris 2024. Na ocasião, a ANSSI tratou 548 eventos de cibersegurança sem que nenhum afetasse as cerimônias ou as competições (ANSSI, 2024). Nos índices internacionais, o país obteve 98,98 pontos no Global Cybersecurity Index de 2024 e foi classificado no Tier 1 — *Role-modelling,* ou seja, um país de referência. Já no National Cyber Power Index, passou da sexta para a nona posição entre 2020 e 2022. Segundo os autores do índice, essa variação indica uma mudança relativa em comparação com os demais países, e não um declínio absoluto de suas capacidades (ITU, 2024; Voo et al., 2020; Voo; Hemani; Cassidy, 2022).

Compreende-se, portanto, que a ciberdiplomacia francesa não depende de alianças de inteligência, como o Five Eyes, mas da combinação entre a ancoragem europeia, uma estrutura institucional própria e a capacidade de formular normas. Esse arranjo amplia a influência do país na governança do ciberespaço sem que ele abra mão do controle sobre suas capacidades (Delerue; Desforges; Géry, 2019; France, 2026), o que caracteriza sua diplomacia como instrumento de soft power.

3.2 A ciberdiplomacia do Reino Unido

A ciberdiplomacia britânica caracteriza-se pela participação ativa em mecanismos multilaterais de governança e segurança cibernética. Na Organização das Nações Unidas, o Reino Unido defende a aplicação do Direito Internacional ao ciberespaço e a adoção de normas

ISSN 2317-1316

de comportamento estatal responsável. Na Organização do Tratado do Atlântico Norte, sua atuação concentra-se no fortalecimento da defesa coletiva, enquanto a parceria Five Eyes amplia o compartilhamento de inteligência e a cooperação contra ameaças cibernéticas. Mesmo após o Brexit, o país mantém mecanismos de diálogo e cooperação com a União Europeia, evidenciando a continuidade de suas parcerias estratégicas (Voo; Hemani; Cassidy, 2022; European Parliamentary Research Service, 2026).

Além da participação institucional, o Reino Unido busca influenciar a formulação de normas internacionais para o uso responsável de tecnologias cibernéticas. Essa estratégia é exemplificada pelo Pall Mall Process, projeto em parceria com a França iniciado em 2024 para enfrentar a proliferação e o uso irresponsável de ferramentas comerciais de intrusão, como o *spyware*. A iniciativa promove princípios de transparência, supervisão e responsabilização, reunindo governos e representantes de outros setores. Paralelamente, a atuação britânica no G7 e na Commonwealth contribui para ampliar sua participação na governança digital e para fortalecer as capacidades cibernéticas de países parceiros (United Kingdom; France, 2024; United Kingdom, 2025).

Dentro do campo operacional, a ciberdiplomacia britânica manifesta-se pela atribuição pública de ataques cibernéticos e pela cooperação internacional em defesa digital. Os casos envolvendo os grupos Seaborgium e APT31 ilustram o uso da atribuição pública como instrumento de responsabilização diplomática diante de atividades maliciosas. O Reino Unido também promove iniciativas de capacitação e assistência técnica, incluindo apoio à Ucrânia e projetos de fortalecimento da governança cibernética no Brasil (United Kingdom, 2025).

O mapeamento documental evidencia a convergência entre as capacidades nacionais e a atuação internacional do Reino Unido. No Global Cybersecurity Index de 2024, o país obteve 100 pontos e foi classificado no Tier 1 — *Role-modelling*. Já o National Cyber Power Index de 2022 o posicionou como a quarta maior potência cibernética, atrás dos Estados Unidos, Rússia e da China. Em conjunto, esses indicadores e a participação britânica em mecanismos de governança internacional sustentam a interpretação de que o ciberpoder do país ultrapassa a dimensão técnica, constituindo também um instrumento de projeção de poder e influência geopolítica (ITU, 2024; Voo; Hemani; Cassidy, 2022).

As atuações do Reino Unido dentro do campo da ciberdiplomacia demonstram como a cooperação técnica e a identificação pública de ameaças são incorporadas à estratégia de defesa

ISSN 2317-1316

dos interesses nacionais e de fortalecimento de parcerias e cooperações estratégicas internacionais. Essas ideias comprovam a proposta do Reino Unido em oferecer e aplicar um uso responsável do seu poder cibernético (Devanny, 2021).

3.3 A ciberdiplomacia da Rússia

Ao analisar a Federação Russa percebe-se que o ciberespaço é visto como extensão de suas fronteiras soberanas. Dessa forma, o país utiliza fóruns multilaterais como o Open-Ended Working Group (OEWG) e o Group of Governmental Experts (GGE) da Organização das Nações Unidas (ONU), a Organização para Cooperação de Xangai (OCX) e o BRICS para projetar sua agenda e incentivar outros Estados a reivindicarem maior controle sobre o ambiente digital (Parepa, 2026; Russian Federation, 2019). Seus principais aliados nessa agenda são China, Irã e Belarus, que compartilham a defesa de normas internacionais de governança baseadas na soberania estatal (Cyber Security Brazil, 2026; TV BRICS, 2025; Republic of Belarus, 2023).

A análise documental revelou, ademais, que Moscou evita termos comumente utilizados pelo Ocidente como “ciberespaço”, “cibersegurnaça” e “ciberdiplomacia”, adotando “espaço informacional”, “segurança da informação” e “segurança internacional da informação” (Russian Federation, 2021), o que desloca o debate para um terreno em que seu modelo de controle doméstico aparece como referência. Esse modelo também tem um lado positivo, pois favorece a cooperação no combate ao ciberterrorismo e ao uso criminoso das TICs – Tecnologias de Informação e Comunicação (Russian Federation, 2024).

Por outro lado, a rejeição russa ao modelo multissetorial ou *multistakeholder*, que inclui empresas e sociedade civil na governança cibernética internacional, é vista como uma falha de alto risco, pois detém infraestruturas críticas cujo comprometimento afetaria a economia e a sociedade civil ficaria afastada do debate, tornando-se mais vulnerável a vazamentos por desconhecer como proteger seus dados. Levando, inclusive, a atingir as infraestruturas governamentais, mesmo com a Estratégia para o Desenvolvimento da Sociedade da Informação (Soldatov; Borogan, 2015)

Por fim, ainda de acordo com os autores Soldatov e Borogan (2015), o Caso Snowden deu à Rússia poder de narrativa, ao evidenciar a espionagem norte-americana e permitir que Moscou se apresentasse como defensora da privacidade e da soberania informacional, com ressonância no Sul Global. Contudo, esse discurso é contraditório, já que o controle do ambiente

ISSN 2317-1316

digital é usado internamente para perseguir opositores e bloquear informações que revelam o autoritarismo do regime. A pesquisa conclui que a soberania cibernética opera em dois registros: externamente, como discurso normativo de legitimação e internamente, como instrumento de controle político (Soldatov; Borogan, 2015; Lucena, 2023).

3.4 A ciberdiplomacia da Indonésia

Quanto a análise realizada sobre o caso da Indonésia, é possível reconhecer que o país conquistou destaque no cenário internacional – e, particularmente, regional -, relacionando a cibersegurança como um dos pilares centrais de sua segurança nacional. Cabe destacar que a Indonésia foi escolhida para este estudo por estar classificada no *Tier* 1 do *Global Cybersecurity Index*, índice desenvolvido pela União Internacional de Telecomunicações (UIT), sendo considerado um "*Role-modelling*". Essa posição no índice global representou um avanço expressivo em relação aos anos anteriores (ITU, 2024). Além disso, o país é considerado uma potência digital em ascensão no G20. Até 2017, a política cibernética era pouco desenvolvida, com instituições, coordenação e base legal mais frágeis. No entanto, em 2017 foi criada a Agência Nacional de Cibernética e Criptografia (BSSN) e, em 2018, foi publicada a primeira estratégia nacional de cibersegurança (IISS, 2021).

Ademais, foi possível analisar que a campanha hacktivista que que a Indonésia sofreu entre 1997 a 1999 foram um marco para o país e demonstraram fragilidades institucionais para respostas rápidas ao enfrentamento das ameaças cibernéticas sofridos no país. Desta forma, compreende-se que a Indonésia vem buscando ampliar suas capacidades no âmbito cibernético, demonstrando um amplo interesse em ações bilaterais e multilaterais com o objetivo de reconhecer e responder de forma ágil ciberataques (CBS News, 1999; Indonesia, 2023a; IISS, 2021).

Diante disso, foi possível mapear 6 acordos bilaterais firmados pelo país, sendo esses com Austrália, Reino Unido, Estados Unidos, Países Baixos, Coreia do Sul e China. Esses acordos demonstram de fundamental relevância para construção de sua defesa cibernética em conjunto com parceiros estratégicos (Vientiane Times, 2021; Antara News, 2022; Indonesia, 2023b; Saffa, 2023; Herryanto, 2024; Australian Embassy Indonesia, 2025). No que se refere à atuação da Indonésia em fóruns internacionais, o Estado atua em diversas organizações estratégicas voltadas ao fortalecimento e ao aprimoramento de medidas de resposta a incidentes do setor cibernético. Destaca-se, nesse sentido, sua participação no Grupo de Especialistas

ISSN 2317-1316

Governamentais (GGE) da ONU (2019-2021) e, especialmente, na Associação das Nações do Sudeste Asiático (ASEAN). Em relação à ASEAN, a Indonésia tem participado de programas multilaterais destinados a avaliar as cibercapacidades dos países-membros, como o ASEAN - *Japan Online Cyber Exercise*, um programa multilateral voltado à criação de exercícios de resposta a ataques cibernéticos, contribuindo tanto para o fortalecimento das capacidades técnicas quanto para a consolidação da confiança estratégica entre eles (Naciones Unidas, 2021; Saputri; W.; Risman, 2020; Waskita; Sidik, 2023).

Diante dos resultados analisados, compreende-se que a Indonésia vem ampliando gradualmente sua atuação internacional, consolidando-se como um Estado relevante na cooperação internacional. Além disso, o fenômeno da "diplomatização" contribuiu para a construção e projeção de uma imagem internacional associada à influência e à capacidade de atuação da Indonésia nos espaços de negociação. Com isso, conclui-se que a Indonésia, embora seja um país em desenvolvimento, dispõe de sua postura diplomática capaz de sustentar um papel regional relevante no setor cibernético. Com isso, o país contribui para desenvolver capacidades cibernéticas e enfrentar vulnerabilidades institucionais que ainda persistem em países em desenvolvimento (IISS, 2021; Barrinha; Renard, 2017; Waskita; Sidik, 2023).

4 CONCLUSÃO

O estudo buscou compreender como países com capacidades cibernéticas relevantes estruturam estratégias diplomáticas para construir capacidades, projetar poder e promover segurança no ciberespaço. A análise de França, Reino Unido, Rússia e Indonésia indica que a ciberdiplomacia deixou de ser um complemento da política de cibersegurança e passou a integrar a própria construção do poder cibernético dos Estados, variando conforme a posição de cada país no sistema internacional e sua concepção de governança. Para potências consolidadas, como França e Reino Unido, ela serve à articulação de parcerias e à influência normativa; para a Rússia, à legitimação de um modelo de governança centrado na soberania estatal; e para países em desenvolvimento, como a Indonésia, ao acesso à cooperação técnica e à compensação de fragilidades institucionais. Essa diversidade reflete a ausência de consenso sobre os princípios que devem orientar o ciberespaço, que se torna espaço de cooperação e de disputa entre projetos concorrentes de ordem digital. Os casos mostram, ainda, que capacidade técnica não se converte automaticamente em influência: o Paris Call encontrou limites sem a

ISSN 2317-1316

adesão das grandes potências, enquanto a Indonésia ampliou seu peso pela cooperação regional na ASEAN. A posição de um país no ciberespaço depende, assim, também de sua habilidade diplomática para converter capacidades em influência. Agradecemos à Profa. Dra. Jéssica Maria Grassi pela orientação, ao Grupo de Pesquisa de Ambiente Digital Aplicado às Relações Internacionais da Unisanta, ao NPSeD/UFSC e à Dra. Bruna Toso de Alcântara pelas trocas acadêmicas e atividades formativas.

5 DECLARAÇÃO DE USO DE IA

Durante a elaboração deste trabalho, utilizaram-se as ferramentas NotebookLM, Claude e ChatGPT para a tradução de documentos e obras em francês, russo e indonésio, para a organização dos tópicos da pesquisa e para a revisão do texto. O conteúdo gerado foi revisado, editado e validado pelos autores, que assumem total responsabilidade pelo texto final.

6 REFERÊNCIAS

ANSSI – Agence Nationale De La Sécurité Des Systèmes D'information. Bilan cyber des Jeux Olympiques et Paralympiques de Paris 2024. Paris: ANSSI, 10 set. 2024. Disponível em: https://cyber.gouv.fr/actualites/bilan-cyber-des-jeux-olympiques-et-paralympiques-de-paris-2024/. Acesso em: 13 out. 2026.

ANSSI – Agence Nationale De La Sécurité Des Systèmes D'information. Cyber threat overview 2025. Paris: ANSSI, 2026. (CERTFR-2026-CTI-003).

ANTARA NEWS. BSSN, South Korean agency ink pact to boost cyberspace security. Antara News, Yogyakarta, 21 jul. 2022. Disponível em: https://en.antaranews.com/news/240601/bssn-south-korean-agency-ink-pact-to-boost-cyberspace-security. Acesso em: 15 out. 2026.

AUSTRALIAN EMBASSY INDONESIA. Australia and Indonesia strengthen cyber cooperation. Jakarta, 21 ago. 2025. Disponível em: https://indonesia.embassy.gov.au/jakt/MR25_075.html. Acesso em: 15 out. 2026.

BARICHELLA, Arnault. Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe. Paris: Jacques Delors Institute, set. 2022. (Policy Paper, n. 281).

BARRINHA, André; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, [S. l.], 28 dez. 2017. Disponível em: https://doi.org/10.1080/23340460.2017.1414924. Acesso em: 16 out. 2026.

BRANGETTO, Pascal. National cyber security organisation: France. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

ISSN 2317-1316

CBS News. CYBERATTACK on Indonesia? CBS News, 18 ago. 1999. Disponível em: https://www.cbsnews.com/news/cyberattack-on-indonesia/. Acesso em: 14 out. 2026.

CYBER SECURITY BRAZIL. China e Rússia ampliam cooperação em IA, cibersegurança e sistemas de satélite para reduzir dependência do Ocidente. Cyber Security Brazil, 24 maio 2026. Disponível em: [conferir endereço eletrônico original]. Acesso em: 26 jul. 2026.

DELERUE, François; DESFORGES, Alix; GÉRY, Aude. A close look at France's new military cyber strategy. ISN Blog, Zurique, 2019. Publicado originalmente em: War on the Rocks, 23 abr. 2019. Disponível em: https://isnblog.ethz.ch/cyber/a-close-look-at-frances-new-military-cyber-strategy. Acesso em: 10 set. 2026.

DEVANNY, Joseph. How the UK Can Be a Responsible Cyber Power. Londres: King's College London, 2021.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE. Cybersecurity. Bruxelas, 2026.

FRANCE. Premier Ministre. French national digital security strategy. Paris, 2015.

FRANCE. Permanent Mission of France to the United Nations. We need to intensify our efforts to prevent crises in the cyberspace. Statement by Mrs. Anne Gueguen at the Security Council Arria-formula meeting. New York, 22 maio 2020. Disponível em: https://onu.delegfrance.org/We-need-to-intensify-our-efforts-to-prevent-crises-in-the-cyberspace. Acesso em: 20 abr. 2026.

FRANCE. Permanent Mission of France to the United Nations. International law is fully applicable to cyberspace. Statement by Mr. Nicolas de Rivière to the Security Council. New York, 20 jun. 2024. Disponível em: https://onu.delegfrance.org/international-law-is-fully-applicable-to-cyberspace. Acesso em: 20 abr. 2026.

FRANCE. Secrétariat Général de la Défense et de la Sécurité Nationale. National cybersecurity strategy 2026–2030. Paris: SGDSN, 2026.

HERRYANTO, Eris. Enam strategi dan tiga rekomendasi kerja sama keamanan siber Indonesia dengan Amerika Serikat. Eris Herryanto, 23 dez. 2024. Disponível em: https://erisherryanto.com/2024/12/23/enam-strategi-dan-tiga-rekomendasi-kerja-sama-keamanan-siber-indonesia-dengan-amerika-serikat/. Acesso em: 15 out. 2026.

IISS - INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. Cyber capabilities and national power: a net assessment. London: IISS, 2021.

INDONÉSIA. Peraturan Presiden nº 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Jacarta, 2023(a). Disponível em: https://peraturan.bpk.go.id/Read/312229/Perpres%20Nomor%2047%20Tahun%202023.pdf

INDONESIA, the Netherlands forge cyber partnership. INP: Indonesian National Police, Jakarta, 1 nov. 2023(b). Disponível em: https://inp.polri.go.id/artikel/indonesia-the-netherlands-forge-cyber-partnership. Acesso em: 15 out. 2026.

ISSN 2317-1316

ITU - International Telecommunication Union. Global Cybersecurity Index 2024. 5. ed. Geneva: ITU, 2024.

LUCENA, André. Há 10 anos, Edward Snowden revelou um mundo sitiado pela espionagem americana. CartaCapital, 2023. Disponível em: https://www.cartacapital.com.br/mundo/ha-10-anos-edward-snowden-revelou-um-mundo-sitiado-pela-espionagem-americana/. Acesso em: 17 fev. 2026.

NACIONES UNIDAS. Asamblea General. Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional: nota del Secretario General. Nueva York: Naciones Unidas, 14 jul. 2021. 30 p. Disponível em: https://docs.un.org/es/a/76/135. Acesso em: 16 out. 2026.

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

PAREPA, Laura-Anca. The Shanghai Cooperation Organization: Coordinated Cyber Statecraft and Norm-Building in a Fragmented World. In: PAREPA, Laura-Anca (ed.). Statecraft and Governance in Cyberspace: Strategies, Challenges and Trends. Singapore: Springer Nature Singapore, 2026. cap. 9, p. 187-220. Disponível em: https://link.springer.com/chapter/10.1007/978-981-95-8341-6_9. Acesso em: 29 jul. 2026.

REPUBLIC OF BELARUS. Ministry of Foreign Affairs. Belarus and Russia approve the Information Security Concept of the Union State. Minsk: Ministry of Foreign Affairs of the Republic of Belarus, 1 mar. 2023. Disponível em: https://www.mfa.gov.by/en/press/news_mfa/cac0ee302b706cd8.html. Acesso em: 26 jul. 2026.

RUHL, Christian; HOLLIS, Duncan; HOFFMAN, Wyatt; MAURER, Tim. Cyberspace and geopolitics: assessing global cybersecurity norm processes at a crossroads. Washington, DC: Carnegie Endowment for International Peace, fev. 2020. (Working Paper).

RUSSIAN FEDERATION. Conselho de Segurança da Federação Russa. Основы государственной политики Российской Федерации в области международной информационной безопасности [Fundamentos da Política Estatal da Federação Russa no Campo da Segurança Internacional da Informação]. Aprovado pelo Decreto do Presidente da Federação Russa n. 213, de 12 de abril de 2021. Moscou, 2021. Disponível em: http://www.scrf.gov.ru/security/information/document114/. Acesso em: 15 ago. 2026.

RUSSIAN FEDERATION. Ministry of Foreign Affairs. Statement by the Russian Federation at the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG on ICTs), 3 June. 2019. Disponível em: https://www.mid.ru/ru/foreign_policy/news/1463020/?lang=en. Acesso em: 10 jun. 2026.

RUSSIAN FEDERATION. Ministry of Foreign Affairs. The signing of a UN Convention against Cybercrime. Moscow: Ministry of Foreign Affairs of the Russian Federation, 27 dez. 2024. Disponível em: https://www.mid.ru/2055536/?lang=pt. Acesso em: 29 jul. 2026.

ISSN 2317-1316

SAFFA, Azizah. Indonesia and UK strengthen cybersecurity cooperation. OpenGov Asia, 30 jun. 2023. Disponível em: https://archive.opengovasia.com/2023/06/30/indonesia-and-uk-strengthen-cybersecurity-cooperation/. Acesso em: 15 out. 2026.

SAPUTRI, Dessy Permatasari; W., Surryanto D.; RISMAN, Helda. Indonesian Cyber Diplomacy: Asean-Japan Online Cyber Exercise. Technium Social Sciences Journal, v. 9, p. 453-464, jul. 2020.

SOLDATOV, Andrei; BOROGAN, Irina. The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries. New York: PublicAffairs, 2015.

TV BRICS. Irã e Rússia firmam acordo de colaboração em IA e cibersegurança. TV BRICS, 9 dez. 2025. Disponível em: https://tvbrics.com/pt/news/ira-e-russia-firmam-acordo-de-colaboracao-em-ia-e-ciberseguranca/. Acesso em: 26 jul. 2026.

UNITED KINGDOM. House of Commons Library. Cybersecurity Policy. Londres, 2025.

UNITED KINGDOM; FRANCE. The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. London, 6 fev. 2024.

VIENTIANE TIMES. China, Indonesia strengthen ties to develop cyber security capacity and technology. Vientiane Times, Vientiane, 22 jan. 2021. Disponível em: https://www.vientianetimes.org.la/freeContent/FreeConten_China15.php. Acesso em: 16 out. 2026.

VOO, Julia; HEMANI, Irfan; CASSIDY, Daniel. National Cyber Power Index 2022. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022.

VOO, Julia; HEMANI, Irfan; JONES, Simon; DESOMBRE, Winnona; CASSIDY, Daniel; SCHWARZENBACH, Anina. National Cyber Power Index 2020. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, set. 2020.

WASKITA, Allisa Salsabilla; SIDIK, Hasan. Diplomasi siber Indonesia dalam penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. Padjadjaran Journal of International Relations (PADJIR), [S. l.], p. 142-164, ago. 2023. Disponível em: https://journals.unpad.ac.id/padjir/article/download/41337/20519. Acesso em: 16 out. 2026.