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

ISSN 2317-1316

# A CIBERDIPLOMACIA NA CONSTRUÇÃO DE CAPACIDADES CIBERNÉTICAS DA RÚSSIA

# CYBER DIPLOMACY IN THE DEVELOPMENT OF RUSSIA'S CYBER CAPABILITIES

Kelvin do Nascimento Silva, Giovanna Marcely Oliveira da Silva, Jéssica Maria Grassi

Universidade Santa Cecília, Curso de Relações Internacionais
E-mail para contato: kelvinsilvaofficial5@gmail.com

*RESUMO – A pesquisa analisa como a atuação russa em fóruns internacionais e iniciativas de governança do ciberespaço molda o desenvolvimento de suas cibercapacidades. Parte-se da hipótese de que a ciberdiplomacia funciona como instrumento complementar às capacidades digitais e militares. Metodologicamente, utiliza-se uma abordagem qualitativa, descritivo-analítica, baseada em análise documental e revisão bibliográfica. Os resultados indicam que o país trata o ciberespaço como extensão de suas fronteiras soberanas, atua em organizações como ONU, OCX e BRICS e coopera principalmente com China, Irã e Belarus. Em suma, conclui-se que a soberania cibernética opera como discurso de legitimação externa e instrumento de controle político interno.*

**Palavras-chave:** Ciberdiplomacia; Rússia; Soberania Cibernética; Seguerança da Informação; Governança do ciberespaço.

*ABSTRACT – This study analyzes how Russia's engagement in international forums and cyberspace governance initiatives shapes the development of its cyber capabilities. It is based on the hypothesis that cyber diplomacy functions as a complementary instrument to digital and military capabilities. Methodologically, it adopts a qualitative, descriptive-analytical approach based on document analysis and a literature review. The findings indicate that Russia treats cyberspace as an extension of its sovereign borders, operates within organizations such as the UN, the SCO, and BRICS, and cooperates mainly with China, Iran, and Belarus. In sum, the study concludes that cyber sovereignty operates both as a discourse of external legitimation and as an instrument of domestic political control.*

**Keywords:** Cyberdiplomacy; Russia; Cyber Sovereignty; Information Security; Cyberspace Governance.

ISSN 2317-1316

# 1 INTRODUÇÃO

No cenário contemporâneo, a Federação Russa destaca-se como um dos principais atores nos debates relacionados à segurança cibernética, à governança do ciberespaço e à cooperação internacional. O ponto de partida para analisar suas capacidades está na trajetória de desenvolvimento tecnológico da União Soviética, que a partir do fim da década de 1940, estruturou um vasto aparato científico em computação, automação e cibernética e passou a encarar a informação como insumo estratégico da segurança nacional (Santos Júnior. 2013). Deste modo, com o fim da URSS, em 1991, esse patrimônio foi integrado a Rússia, que passou a interpretar o ciberespaço não como um ambiente técnico neutro, mas como prolongamento de seu território soberano e meio de projeção de poder (Rodrigues, 2006).

Nos primeiros anos do século XXI, Moscou passou a advogar pela criação de regras internacionais sobre segurança da informação, vinculando sua política externa ao princípio da soberania cibernética, que atribui a cada Estado autonomia plena sobre a infraestrutura de informação em seu território. Essa postura fez da ciberdiplomacia um componente da política externa russa, usado tanto para propor normas globais quanto para reforçar as defesas nacionais (United Nations Office For Disarmament Affairs, 2021). Dessa forma, a relevância do país é confirmada por índices internacionais, como o National Cyber Power Index (Voo; Hemani; Cassidy, 2022) e o Global Cybersecurity Index (ITU, 2024), nos quais aparece entre os Estados com destacado poder cibernético e com alto grau de compromisso institucional com a segurança cibernética – fato que justifica a escolha da Rússia para esta pesquisa.

Cabe destacar que a ciberdiplomacia é definida como o campo que trata do desempenho das funções diplomáticas, utilização de recursos e de pessoal qualificado para atuar nos espaços de diálogo bilateral e multilateral, no nível regional e internacional, visando assegurar os interesses nacionais no que diz respeito ao ciberespaço. Essa difere de diplomacia digital, ou e-diplomacia, que diz respeito ao uso de novas tecnologias e mídias sociais por Chefes de Estado, Chefes de Governo, Ministros e Diplomatas no contexto de suas atividades diplomáticas (Barrinha; Renard, 2017). A literatura recente trata a ciberdiplomacia como extensão normativa da política externa, por meio da qual os Estados disputam narrativas estratégicas sobre a governança do ciberespaço (Barrinha, Turner, 2023). Nessa conjuntura, o poder cibernético é entendido como combinação de capacidades materiais e narrativas estratégicas (Neunfeld, 2021).

ISSN 2317-1316

No caso russo, estudos apontam que a pressão securitária percebida no eixo Euro-Atlântico, a centralidade dos Estados Unidos na governança técnica da internet e a coordenação normativa com os membros da Organização de Cooperação de Xangai estruturam essa atuação (Figueiredo, Rê, Menezes, 2021; Parepa, 2026). O Kremlin passou a ver a internet não como tecnologia neutra, mas como instrumento político a ser mantido sob controle estatal (Soldatov; Borogan, 2015).

Diante desse quadro, a pesquisa parte do seguinte questionamento: de que forma a participação da Rússia em fóruns internacionais e em iniciativas de governança do ciberespaço influencia a construção de suas cibercapacidades e a defesa de seus interesses estratégicos? Formula-se a hipótese de que essa participação, por meio de sua ciberdiplomacia, serve como ferramenta complementar, e não subordinada, ao aparato tecnológico e militar do país, procurando influenciar regras alinhadas à soberania cibernética e dar legitimidade tanto ao controle interno da informação, quanto à sua atuação internacional.

Desse modo, o estudo tem como objetivo analisar de que forma a participação da Rússia em fóruns internacionais e em iniciativas de governança do ciberespaço influencia construção de suas cibercapacidades e a defesa de seus interesses estratégicos. De modo específico, pretende-se examinar o contexto geopolítico e de segurança em que a Rússia se insere e identificar como a ciberdiplomacia vem sendo usada como ferramenta de Política Externa.

## 2 MATERIAIS E MÉTODOS

Metodologicamente, trata-se de uma pesquisa qualitativa de cunho descritivo-analítico, desenvolvida por meio de revisões bibliográficas e análise documental. A abordagem qualitativa foi adotada porque o objeto de estudo, a relação entre a atuação diplomática russa e a construção de suas cibercapacidades, envolve discursos, normas e posicionamentos oficiais que não são mensuráveis por indicadores quantitativos, exigindo interpretação do conteúdo e do contexto em que os documentos foram produzidos. O recorte recai sobre a Federação Russa, escolhida por seu papel central nos debates sobre segurança cibernética e por seu destaque em índices internacionais de cibersegurança.

As fontes primárias reúnem decretos presidenciais, leis federais e conceitos emitidos pelo governo russo entre 2011 e 2024, além de declarações apresentadas em fóruns multilaterais, como o Grupo de Trabalho de Composição aberta da ONU (OEWG), e documentos de

ISSN 2317-1316

cooperação com Belarus. Dessa forma, esses materiais foram examinados e sistematizados em quadros, organizados por ano, órgão responsável e finalidade. Já como fontes secundárias compreendem artigos científicos, capítulos de livros e obras especializadas.

Cabe mencionar que esta pesquisa foi desenvolvida no âmbito do Programa de Iniciação Científica da Unisanta (PIC) e também integrou o projeto "A Ciberdiplomacia das Potências Mundiais", desenvolvido no âmbito do Grupo de Pesquisa de Ambiente Digital Aplicado à Relações Internacionais, do Curso de Relações Internacionais da Unisanta.

Como limitação, grande parte dos documentos oficiais está em russo, o que exigiu cautela na leitura e na tradução dos trechos analisados, ainda que sujeita a eventuais imprecisões. Além disso, não há divulgação oficial de valores destinados exclusivamente a operações cibernéticas, o que restringe a análise da dimensão orçamentária. Por fim, o procedimento descrito, com a identificação das fontes, dos critérios de organização e dos eixos de análise, permite que o estudo seja replicado por outros pesquisadores.

## 3 RESULTADOS E DISCUSSÃO

Evidencia-se, por meio de índices globais que medem as capacidades cibernéticas dos países - como o Global Cybersecurity Index (GCI), da União Internacional de Telecomunicações (ITU), e o National Cyber Power Index (NCPI), elaborado pelo Belfer Center for Science and International Affairs da Universidade de Harvard -, as altas posições que a Rússia se encontra nos rankings, mostrando a desenvoltura de suas capacidades no âmbito cibernético internacional por meio de critérios técnicos, estabelecidos para medir sua infraestrutura tecnológica, desenvolvimento de políticas de cibersegurança e cooperação internacional.

Inicialmente, é importante destacar que o Estado Russo, em documentos oficiais, não costuma usar os termos "ciberespaço", "cibersegurança" e "ciberdiplomacia" como os países ocidentais, e sim "espaço informacional", "segurança da informação" e "segurança internacional da informação".

No que tange à governança do ciberespaço, a Federação Russa realça maior projeção às suas visões de controle estatal, utilizando as organizações internacionais, fóruns multilaterais e outros tipos de plataformas que podem servir de intermédio para convencer os demais Estados a rejeitarem o modelo multissetorial ou *multistakeholder* – que estabelece a participação dos

ISSN 2317-1316

Estados, academias, empresas privadas e sociedade no referido debate. A oposição ao modelo *multistakeholder* foi reforçada pelo diplomata russo Andrey Vladimirovich Krutskikh; conforme Soldatov e Borogan (2015, p. 218, tradução nossa): "Ele defendia as Nações Unidas porque a organização era composta por governos, e não por empresas, e muitos desses governos eram favoráveis ao desejo da Rússia de exercer maior controle sobre a Internet dentro de suas próprias fronteiras."[1]

Algumas das organizações e plataformas internacionais de governança do ciberespaço que a Rússia busca projetar seus ideais são: por parte da ONU, há o Grupo de Trabalho de Composição Aberta sobre Segurança e o uso das Tecnologias da Informação e Comunicação (OEWG, do inglês *Open-Ended Working Group*), analisando que a atuação amplia a participação multilateral e o auxílio na proposição de mecanismos como diretório de pontos de contrato e normas de comportamento estatal, e também, o Grupo de Especialistas Governamentais (GGE, do inglês *Group of Governmental Experts*), que defende a continuidade do diálogo sem adoção imediata de normas rígidas, ambas as plataformas da ONU atuam em defesa de um instrumento jurídico internacional vinculante sobre segurança da informação, servindo para o Kremlin como um intermédio de promoção da defesa da soberania estatal sob o ciberespaço. Em adição, temos a Organização de Cooperação de Xangai (OCX), que Moscou busca maior produção normativa global com base na soberania digital e coordenação entre Estados. Por outro lado, e não menos importante, o BRICS, cuja atuação russa se observa como cooperação técnica, institucional e de cibersegurança junto aos integrantes do bloco, bem como o alinhamento de posição e de sua influência normativa.

Já no âmbito das relações bilaterais e regionais da cooperação cibernética, os maiores aliados da Rússia são: China, Belarus e Irã. A parceria entre China e Rússia converge por interesses mútuos de governança e soberania estatal da internet, bem como no controle do fluxo informacional por uma questão geopolítica (Cyber Security Brazil, 2026). São destacados, nesse sentido, os episódios nos quais os EUA se utilizaram desse meio para interferir em governos considerados contrários aos interesses americanos (como, por exemplo, os episódios da primavera árabe e as espionagens durante o mandato de Dilma Rousseff no Brasil). A

[1] No original: "[…] *He favored the United Nations because it was filled with governments, not companies, and many of them were sympathetic to Russia's desire to control the Internet within their borders*". (Soldatov; Borogan, 2015, p. 218)".

ISSN 2317-1316

cooperação com o Irã, por outro lado, envolve mais aproximação e iniciativas de cooperação governamental em temáticas ligadas ao escopo da segurança da informação, como inteligência artificial, cibersegurança e demais tecnologias da informação. Tal cooperação se estreitou ainda mais por conta do BRICS (TV BRICS, 2025). Com Belarus, a parceria foi reforçada em 2023, através da aprovação do Conceito de Segurança da Informação do Estado da União, tendo articulações conjuntas e favoráveis na formulação de normas do controle estatal do ciberespaço propostas pela Rússia nas esferas internacionais (Republic of Belarus, 2023).

Por meio de plataformas da ONU, tendo ênfase no Grupo de Trabalho de Composição Aberta sobre a Segurança e o uso das Tecnologias da Informação e Comunicação (OEWG, do do inglês *Open-Ended Working Group*), a Rússia usa do seu aparato ciberdiplomático para defender a criação de mecanismos jurídicos internacionais e de confiança entre os Estados para promover e estabelecer normas de comportamento no espaço digital. Através de declarações oficiais, Moscou ressalta que o uso malicioso das tecnologias de comunicação e informação (TICs) pode configurar como violação da soberania estatal, e consequentemente, poderá causar escaladas e conflitos internacionais por conta de intervenções em assuntos internos dos países. Ademais, a Rússia argumenta que há a necessidade de maior inclusão dos países em desenvolvimento nas discussões por conta do fato de que as desigualdades tecnológicas deixam os países desse enquadramento cada vez mais dependentes de tecnologias estrangeiras, fazendo-os submissos às potências detentoras de maior influência no ciberespaço (Russian Federation, 2019; UNODA, 2021).

Em conexão com a crítica de Moscou em relação à dependência tecnológica dos países em desenvolvimento, a Rússia utiliza o termo “cibercolonialismo” para caracterizar essa problemática e desequilíbrio internacional nas limitações de desenvolvimento de capacidades cibernéticas e proteção digital dos países que carecem de infraestrutura digital própria para isso. Além disso, propõe maior assistência técnica e cooperação internacional com esses países, mas priorizando e respeitando a soberania de cada um, fazendo com que os interesses geopolíticos da Rússia sejam associados e reivindicados por outros Estados no sistema internacional (Russian Federation, 2013; Russian Federation, 2019).

Além do mais, o Kremlin também usa narrativas para convencer os demais Estados a seguirem seus ideais em relação ao ciberespaço, como por exemplo, as revelações feitas por Edward Snowden sobre os programas de vigilância dos Estados Unidos, propagando a ideia de

ISSN 2317-1316

desconfiança da maior potência do planeta aos demais países. Tal episódio foi utilizado pela Rússia para reforçar e alimentar uma imagem de "Rússia defensora da soberania informacional e da privacidade de dados". Moscou ainda denunciou a alta concentração de poder tecnológico na mão de empresas privadas do ramo, ampliando suas propostas em plataformas internacionais e criticando a atual governança global do ciberespaço por potências ocidentais através de empresas privadas que detém alto poder de controle informacional, visando uma nova ordem com normas do direito internacional que orientem o ciberespaço como fronteiras de nações soberanas (Soldatov; Borogan, 2015; Lucena, 2023).

As atuações internacionais da Rússia nesse campo estão diretamente ligadas com as domésticas, tendo em vista os documentos e instrumentos regulatórios criados pelo governo russo para fortalecer suas infraestruturas críticas, conferindo maior controle do ambiente digital ao Estado russo. Dentre os principais documentos estão: a Doutrina de Segurança da Informação de 2016, a Lei Federal nº 187, de 2017, relacionada à segurança das infraestruturas críticas, a Lei Federal nº 90-FZ, de 2019, associada à chamada soberania da internet, e a Estratégia de Segurança Nacional da Federação Russa, de 2021. É de suma importância também destacar a Estratégia para o Desenvolvimento da Sociedade da Informação, que foi um marco no que tange a alfabetização dos russos no ambiente digital, o que de certa forma expandiu as capacidades do Kremlin de monitorar/regular informações que possam desestabilizar sua política por meio de protestos (Russian Federation, 2016; Soldatov; Borogan, 2015).

Ademais, o documento denominado Fundamentos da Política Estatal da Federação Russa no Campo da Segurança Internacional da Informação, de 2021, considerado o documento mais diretamente ligado à ciberdiplomacia publicado pelo país, descreve quais são as ameaças identificadas pela Rússia, além de apontar as diretrizes e objetivos para a atuação russa no que tange à segurança internacional da informação. Mais recentemente foram publicadas a Estratégia de Desenvolvimento Científico e Tecnológico e a Estratégia Nacional de Inteligência Artificial, ambas de 2024, as quais discutem a ideia de "soberania tecnológica" como central para a segurança russa.

Em observação, a estratégia russa de política interna e diplomacia gera uma certa contradição, por mais que Moscou aborde pautas de não interferência e de soberania digital e informacional, é notório que o controle que a nação tem sob o ciberespaço é usado para vigiar, perseguir e repreender pessoas que pensem diferentes da visão do governo russo. E colocar

ISSN 2317-1316

limites na participação da sociedade, empresas e outros atores pode acabar não auxiliando na construção de um ciberespaço mais seguro ou mais resiliente, em razão de que esses atores também possuem informações e infraestruturas críticas que devem ser bem zeladas, evidenciando que o Kremlin não consegue equilibrar adequadamente a segurança coletiva do ciberespaço e os seus próprios interesses em torno dele (Figueiredo; Rê; Menezes, 2021).

Por fim, infere-se que a ciberdiplomacia russa é um meio a qual o país integra às suas capacidades tecnológicas, institucionais e militares, visando promover normas para a governança global do ciberespaço, buscando influenciar países a se associarem à ideia de que o Estado deve ser o ator a exercer o maior controle sobre o ciberespaço, preservando sua soberania nesse ambiente. As atuações da Rússia para difundir suas ideias e visões ocorrem, principalmente, no âmbito da ONU, da Organização de Cooperação de Xangai (OCX), do BRICS e por meio de acordos bilaterais. A ciberdiplomacia desenvolve suas capacidades cibernéticas por via da cooperação internacional e articulação política com os demais países como meio de atingir os interesses russos, entretanto, é necessário sempre estar avaliando o que de fato vai ser benéfico na contribuição da construção de um ciberespaço seguro e o que pode eventualmente colocar os interesses pessoais da Rússia a frente das discussões em prol de um ciberespaço mais seguro, estável e resiliente (Barrinha; Turner, 2023; Neuenfeld, 2021; Russian Federation, 2021).

# 4 CONCLUSÃO

Em síntese, o trabalho examinou de que forma a participação da Rússia em fóruns internacionais e em iniciativas de governança do ciberespaço influencia a construção de suas cibercapacidades e a defesa de seus interesses estratégicos, e os resultados confirmam a hipótese de que a ciberdiplomacia opera como complemento ao poderio tecnológico e militar do país. A Rússia recorre a espaços multilaterais como a ONU (OEWG e GGE), a OCX e o BRICS, além de arranjos bilaterais com China, Irã e Belarus, defendendo a soberania sobre a internet. Ao optar pelo termo “segurança da informação” ou “segurança internacional da informação” em lugar de “ciberdiplomacia”, Moscou leva a discussão para um campo em que seu modelo de controle estatal surge como exemplo, principalmente em contextos regionais orientais. Verificou-se também que a soberania cibernética funciona em dois planos: no exterior, como discurso normativo que busca legitimidade junto ao Sul Global, fortalecido pelo Caso Snowden,

ISSN 2317-1316

e, no interior, como mecanismo de vigilância e controle político, o que torna contraditória a imagem de defensora da privacidade. O estudo colabora, portanto, com um campo ainda pouco explorado no Brasil. Em pesquisas futuras, recomenda-se examinar o papel do setor privado e da sociedade civil na governança cibernética russa e acompanhar o desenvolvimento de organizações recentes.

## 5 DECLARAÇÃO DE USO DE IA

Declaração de Uso de IA: Durante a elaboração deste trabalho, utilizou-se a ferramenta ChatGPT para auxílio na captação de materiais oficiais (como documentos e declarações), mapeamento de quais organizações internacionais/plataformas internacionais o país da pesquisa integra e na formulação das referências bibliográficas no padrão e em conformidade com as normas da ABNT. O conteúdo gerado foi revisado, editado e validado pelos autores, que assumem total responsabilidade pelo texto final.

## 6 REFERÊNCIAS

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

BARRINHA, André; TURNER, Ryan. Strategic narratives and the multilateral governance of cyberspace: the cases of European Union, Russia, and India. Contemporary Security Policy, v. 45, n. 1, 2023. DOI: 10.1080/13523260.2023.2266906.

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: https://www.cybersecbrazil.com.br/post/china-e-r%C3%BAssia-ampliam-coopera%C3%A7%C3%A3o-em-ia-ciberseguran%C3%A7a-e-sistemas-de-sat%C3%A9lite-para-reduzir-depend%C3%AAn. Acesso em: 26 jul. 2026.

ISSN 2317-1316

FIGUEIREDO, Danniel Garcia Barbosa; RÊ, Eduardo de; MENEZES, Thássia Barbosa de. Gigante de Mãos de Aço: As Capacidades Russas no Jogo de Poder no Ciberespaço. In: AYRES PINTO, Danielle Jacon; PAGLIARI, Graciela de Conti; GRASSI, Jéssica Maria (orgs.). A geopolítica das estratégias em defesa cibernética: como os EUA, China, Rússia e Israel protegem seu ciberespaço. Rio de Janeiro: Alpheratz, 2021.

ITU - INTERNATIONAL TELECOMMUNICATION UNION. Global Cybersecurity Index 2024. 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.

NEUENFELD, Matheus Eduardo. Estratégia nacional e poder cibernético: o ressurgimento da Rússia no cenário internacional. 2021. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Universidade Federal de Santa Catarina, Centro Socioeconômico, Florianópolis, 2021. Disponível em: https://repositorio.ufsc.br/handle/123456789/223132. Acesso em: 9 jun. 2026.

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.

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.

ISSN 2317-1316

RODRIGUES, Robério Paulino. O colapso da URSS: um estudo das causas. 2006. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2006. Disponível em: https://teses.usp.br/teses/disponiveis/8/8137/tde-11072007-112541/. Acesso em: 9 jun. 2026.

RUSSIAN FEDERATION. Doctrine of Information Security of the Russian Federation. Moscow, 2016.

RUSSIAN FEDERATION. Концепция стратегии кибербезопасности Российской Федерации [Projeto do Conceito de Estratégia de Cibersegurança da Federação Russa]. Moscou, 2013. Disponível em: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. Acesso em: 11 jun. 2026.

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 nº 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. 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. Open-Ended Working Group on Security of and in the Use of ICTs, 2019. Disponível em: https://www.mid.ru/ru/foreign_policy/news/1463020/?lang=en. Acesso em: 10 jun. 2026.

SANTOS JUNIOR, Roberto Lopes dos. Uma história do sistema computacional na ex-União Soviética. Ciência Hoje, Rio de Janeiro, v. 52, n. 309, p. 22-25, nov. 2013.

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

**ISSN 2317-1316**

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 NATIONS OFFICE FOR DISARMAMENT AFFAIRS (UNODA). Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. New York: United Nations, 2021. Disponível em: https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021. Acesso em: 6 jun. 2025.

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