



DESAFIOS DE INTELIGÊNCIA

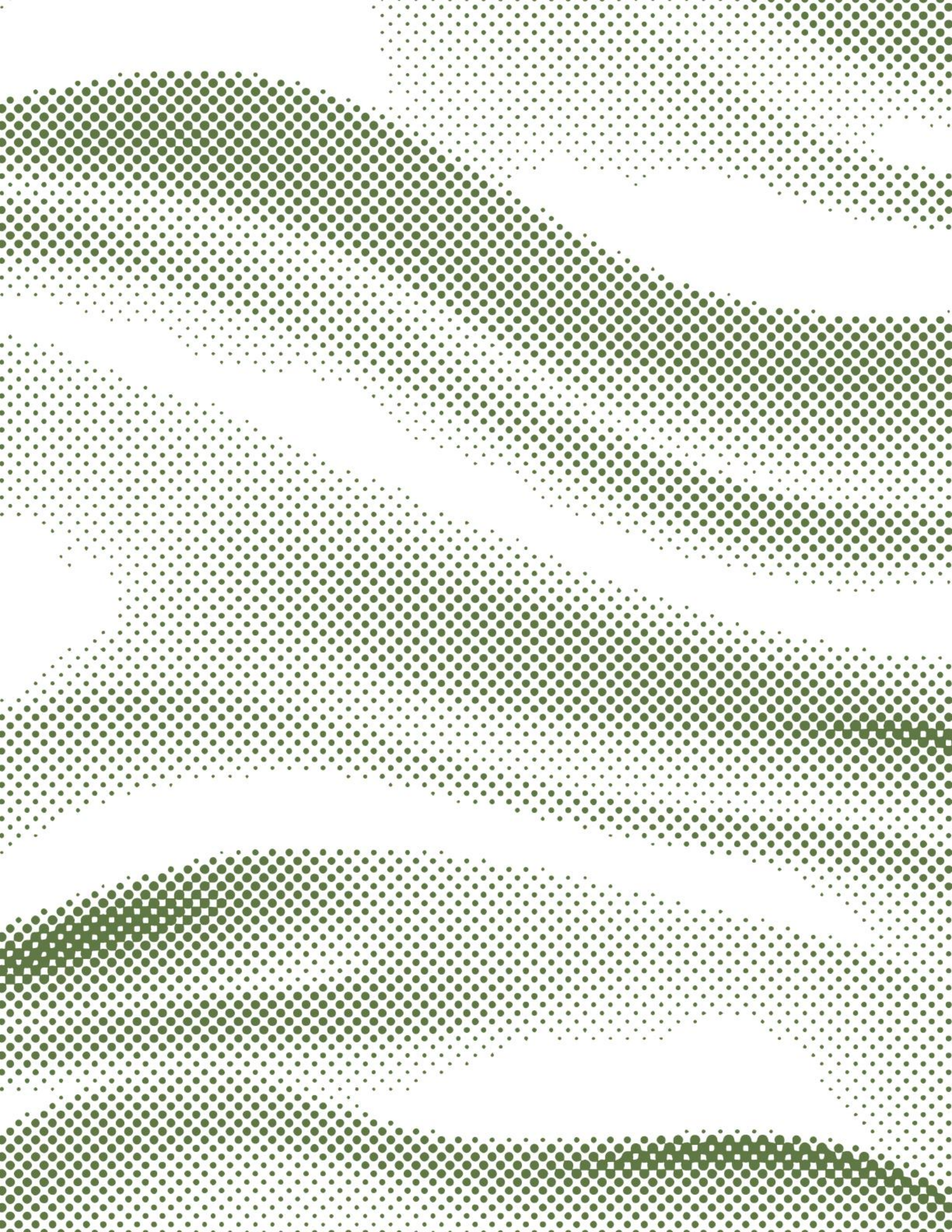
EDIÇÃO 2026

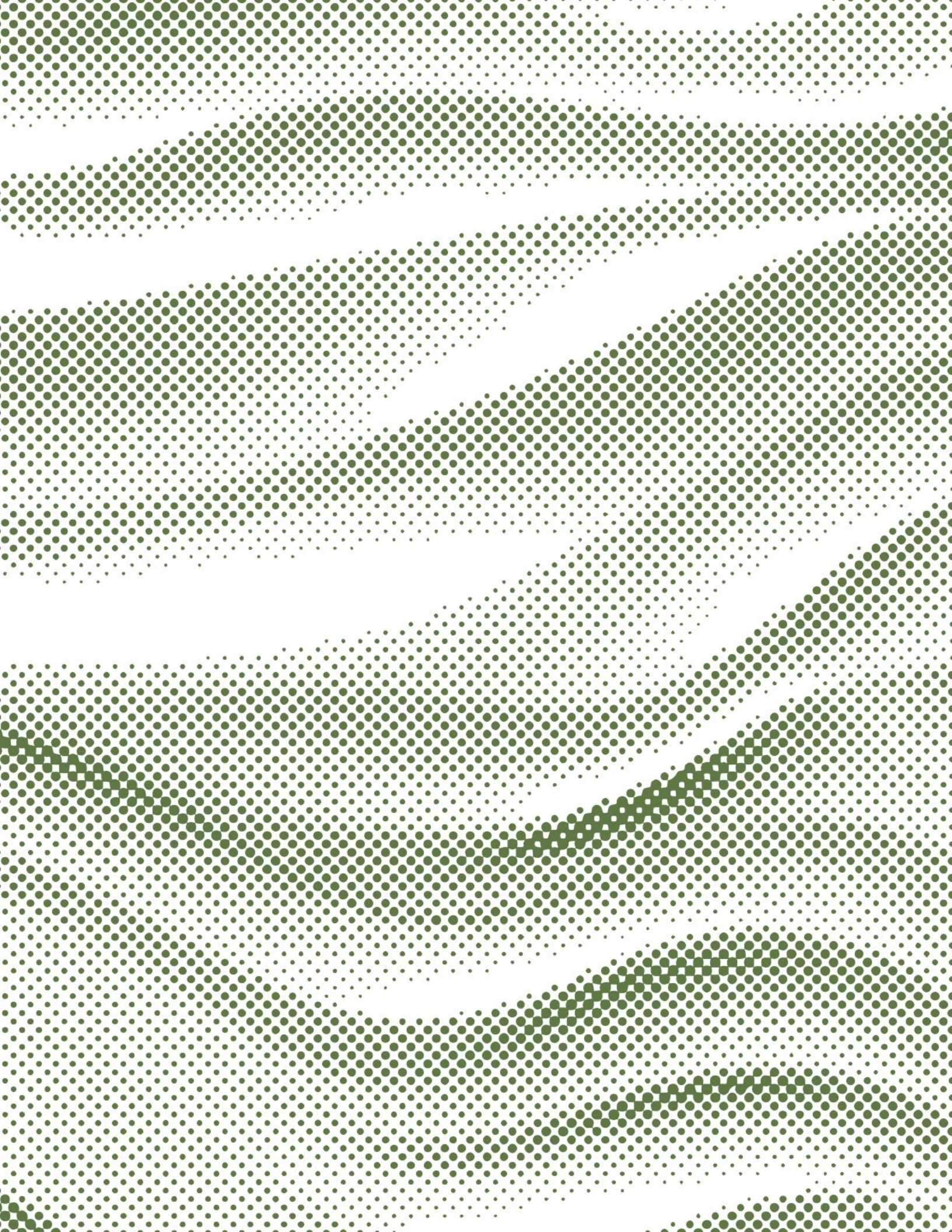




DESAFIOS DE INTELIGÊNCIA

EDIÇÃO 2026





REPÚBLICA FEDERATIVA DO BRASIL
Presidente Luiz Inácio Lula da Silva

CASA CIVIL
Ministro Rui Costa

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA
Diretor-Geral Luiz Fernando Corrêa

SECRETARIA DE PLANEJAMENTO E GESTÃO
Secretário Thiago Cunha Araújo

ESCOLA DE INTELIGÊNCIA
Diretora Anna Cruz

Coordenação
Coordenação-Geral de Pesquisa

Catálogo Bibliográfico Internacional e Normalização
Divisão de Conhecimento e Memória

Impressão
Divisão de Serviços Gráficos

SPO Área 5, Quadra 1
CEP: 70610-905 – Brasília/DF

1ª edição/impressão: dezembro de 2025

Projeto Gráfico
Luciano Mendes

Fotos
Agência Brasil

Fotos da capa
Fernando Frazão (Agência Brasil)
Rovena Rosa (Agência Brasil)

Foto da contracapa
Fabio Rodrigues-Pozzebom (Agência Brasil)

Dados Internacionais de Catalogação na Publicação (CIP)

Agência Brasileira de Inteligência (ABIN)
Desafios de Inteligência: edição 2026/ Agência Brasileira de
Inteligência.- Brasília: ABIN, 2025.

117 p.: il. color.

ISBN 978-65-86360-38-7

1. Atividade de Inteligência - Brasil. 2. Clima. 3. Demografia. 4. Cripto-
grafia pós-quântica. 5. Inteligência Artificial. 6. Segurança Cibernética.
7. Interferência Externa. Eleições - segurança.

I. Agência Brasileira de Inteligência. II. Título.

CDU 355.40(81) A268



Presidência da República | Casa Civil
Agência Brasileira de Inteligência



DESAFIOS DE INTELIGÊNCIA

EDIÇÃO 2026



Brasília
Dezembro de 2025

Índice

Apresentação	9
Agradecimentos	11
Sumário Executivo	13
Nota metodológica	21

01

Transições globais	25
Clima	26
Demografia	31
Tecnologia	37

02

Situação internacional	45
Competição	46
Conflitos	49

03

América do Sul	55
Segurança	56
Integração	63

04

Brasil: desafios para a inteligência	67
Segurança do processo eleitoral de 2026	68
Transição para a criptografia pós-quântica	72
Ataques cibernéticos autônomos com uso de agentes de inteligência artificial	78
Reconfiguração das cadeias de suprimento globais	83
Dependência tecnológica, atores não estatais e interferência externa	88
Conclusão	93
ABIN	97
Publicações	99
Notas	105



Apresentação

D*esafios de Inteligência – Edição 2026* é a nova versão do relatório público preparado pela Agência Brasileira de Inteligência (ABIN) com o objetivo de apresentar à sociedade e às autoridades sua visão sobre riscos diretos e indiretos à segurança do Brasil.

As orientações estratégicas para a atuação da ABIN são dadas pela Constituição, pelas leis, pela Política Nacional de Inteligência (PNI) e por normativos como o Decreto de reorganização do Sistema Brasileiro de Inteligência (Sisbin), de 2023. Na democracia, contudo, é imprescindível que, para além dessas balizas normativas, as ameaças, as percepções e as alternativas afetas à segurança das pessoas e das instituições sejam conhecidas

e debatidas pelo público. Um dos papéis da ABIN, órgão central do Sisbin, é criar as condições para esse debate e, assim, promover, em colaboração com as forças da sociedade, o aprimoramento das concepções e das práticas concernentes às áreas de Inteligência e de segurança.

Há um ano, a ABIN lançava o primeiro *Desafios de Inteligência*, no qual destacava as dinâmicas de agravamento da crise climática, alteração dos pa-

drões populacionais, aceleração da corrida tecnológica e acirramento da competição entre potências mundiais, com uma série de riscos iminentes para o Brasil e seu entorno estratégico.

Ao longo do último ano, vimos essas dinâmicas internacionais ganharem mais proeminência. Na esfera geopolítica, observamos o emprego de instrumentos econômicos como fatores de pressão política e uma escalada das ameaças militares a países latino-americanos, inclusive fronteiriços com o Brasil. Observamos, ainda, acirrada competição pela dianteira no desenvolvimento e uso da inteligência artificial, o que impactará de forma duradoura as relações entre países centrais e periféricos no Sistema Internacional.

Nesta edição, atualizamos a evolução das transições globais e das dinâmicas de competição internacional, destacando cinco desafios para a Inteligência em 2026: segurança do processo eleitoral, transição para a criptografia pós-quântica, ataques cibernéticos autônomos com agentes de inteligência artificial, reconfiguração das cadeias de suprimento globais e interferência externa por atores não estatais. Todos esses desafios são profundamente impactados pela intensificação da competição internacional em contexto de transição sistêmica de poder.

A atualização dos desafios, entretanto, não significa que aqueles apontados na edição passada foram superados. As análises desta nova edição mostram a transversalidade de ameaças persistentes, tais como o crime organizado e a interferência externa. Numa situação dinâmica, essas ameaças combinam-se e geram novos riscos, analisados no capítulo dedicado aos desafios para 2026.

A série *Desafios de Inteligência* tem-se caracterizado pela coprodução envolvendo especialistas de universidades, instituições de pesquisa e agências governamentais, aos quais somos extremamente gratos. Uma novidade da presente edição

foi a realização de consulta prévia estruturada, por meio da qual dezenas de especialistas foram ouvidos sobre clima, tecnologia, demografia, saúde e migrações, além da situação internacional e regional. Destacou-se a contribuição dos pesquisadores integrantes da Rede de Pesquisa em Inteligência Estratégica, estabelecida em maio de 2025 pela Escola de Inteligência da ABIN.

A criação da Rede de Pesquisa, assim como a consolidação da série *Desafios de Inteligência*, vem ao encontro dos múltiplos esforços empreendidos pela Agência desde 2023 no sentido de redirecionar, reorganizar e reposicionar seu trabalho, com ênfase na legitimidade e na eficácia de sua atuação, a serviço da sociedade brasileira.

É responsabilidade do Estado brasileiro prover condições de segurança para as brasileiras e os brasileiros, sem as quais não pode haver desenvolvimento. Para fazer isso, é preciso produzir conhecimento especializado sobre riscos, vulnerabilidades e ameaças — focos da atuação dos órgãos de Inteligência. Com este documento, a ABIN, mais uma vez, traz a público um importante resultado do exercício de suas atribuições legais, reafirmando a disposição de trabalhar para a construção de uma sociedade próspera, justa, democrática e soberana.

Boa leitura!



Luiz Fernando Corrêa
Diretor-Geral
Agência Brasileira de Inteligência

Agradecimentos

A ABIN agradece às instituições e aos especialistas consultados, os quais compartilharam com a Escola de Inteligência suas avaliações sobre clima, demografia, saúde, migrações, tecnologia e situação internacional e regional.

A consulta a órgãos integrantes do Sistema Brasileiro de Inteligência foi realizada por meio dos canais formais estabelecidos, e os órgãos não serão mencionados individualmente. Não obstante, agradecemos nominalmente aos especialistas que concordaram em ser identificados. A consulta foi realizada ao longo de 2025 e proporcionou insumos valiosos para a elaboração das análises desta edição. A responsabilidade pelos resultados, contudo, é exclusivamente da ABIN.

Especialistas consultados

Almir de Oliveira Junior (IPEA), Ana Flávia Granja e Barros (UnB), Antônio Carlos Lessa (UnB), Antonio Jorge Ramalho da Rocha (UnB), Antonio Lassance (IPEA), Carlos Eduardo Pellegrino Cerri (USP), Carlos Frederico de Souza Coelho (PUC-Rio), Cintiene Sandes Monfredo Mendes (ESD), Cláudio Secchin (MTE), David Santana e Silva Barreto (Anatel), Isabel Rocha de Siqueira (PUC-Rio), James Marlon Azevedo Görgen (MDIC), Juliano da Silva Cortinhas (UnB), Julio Cesar Cossio Rodriguez (UFSM), Lucas Pereira Rezende (UFMG), Maurício Santoro Rocha (CEPE/Marinha), Paulo Artaxo (USP), Peterson Silva (ESD), Rodrigo Otávio Ribeiro Hagstrom (Anatel), Sandro Teixeira Moita (Eceme/Exército), Sergio Tavares de Almeida Rego (Fiocruz), Tiago Molina Schnorr (Sedec/MIDR), Victor Muniz Estevam Dias (Anatel), Wagner Silva de Araújo (SGD/MGI), Wilson Fusco (Fundação Joaquim Nabuco).



Sumário Executivo

O presente sumário executivo apresenta de forma resumida a avaliação da Agência Brasileira de Inteligência (ABIN) sobre os desafios que moldarão a segurança das pessoas e das instituições no Brasil em 2026.

A análise parte da constatação de que o mundo atravessa um período de profunda reconfiguração, impulsionado pela confluência de três transições globais interdependentes — climática, demográfica e tecnológica. Esses processos ocorrem em um cenário de desestruturação da ordem internacional, marcada por uma multipolaridade desequilibrada e pelo acirramento da competição entre grandes potências.

O documento está estruturado para examinar, primeiramente, as implicações de cada uma dessas transições para a segurança nacional, demonstrando como as mudanças no clima, na estrutura populacional e na tecnologia geram riscos e oportunidades sistêmicas. Em seguida, avalia a nova dinâmica do sistema internacional e suas repercussões para o entorno estratégico sul-americano, um espaço cada vez mais permeável às disputas geopolíticas globais. Por fim, aprofunda a análise sobre desafios de Inteligência específicos e de alta criticidade que deverão concentrar atenções e recursos por parte da Inteligência brasileira em 2026,

como a segurança do processo eleitoral, a transição para a criptografia pós-quântica, o uso de inteligência artificial em ciberataques autônomos, a reconfiguração das cadeias globais de suprimentos e a relação entre dependência tecnológica e interferência externa. A análise desses desafios ilustra a natureza complexa das ameaças contemporâneas.

Para o Brasil, esse ambiente apresenta tanto vulnerabilidades e ameaças quanto oportunidades estratégicas. O êxito em mitigar riscos e capitalizar vantagens comparativas nessas condições, pelo emprego coordenado das capacidades estatais, dependerá de uma compreensão aprofundada das dinâmicas em curso. *Desafios de Inteligência – Edição 2026* visa a compartilhar com o governo e a sociedade a visão atualizada da ABIN sobre os principais desafios de segurança, contribuindo para o debate e a formulação de políticas de Estado resilientes e para a projeção dos interesses nacionais em um mundo em transformação.

Os dados mencionados neste Sumário Executivo estão referenciados nos respectivos capítulos.



1. Transições Globais

Transições globais são mudanças históricas significativas, disruptivas e interdependentes que afetam a sociedade, a economia e o meio ambiente. Embora suas origens sejam rastreáveis, a previsão de seu desenvolvimento futuro é altamente complexa. *Desafios de Inteligência – Edição 2026* propõe-se a acompanhar e atualizar, sob a ótica da Inteligência de Estado, o momento atual das transições nos domínios do clima, da demografia e da tecnologia. Essas transformações reconfiguram as relações internacionais, onde múltiplos atores (estatais, empresariais, sociais) agem constrangidos por estruturas históricas. O contexto atual é marcado pela alta densidade das interações e das interdependências (energia, informação, transportes) e por um impacto humano sem precedentes, caracterizando o Antropoceno ou a Era Digital. Acumulam-se evidências sobre mudanças climáticas, alterações demográficas profundas e inovações tecnológicas irreversíveis. Sob o prisma da segurança do Brasil, são avaliados os riscos e as oportunidades inerentes a essas três transições.

| Clima

A mudança do clima consolidou-se como um imperativo de segurança global não convencional, com particulares implicações para o Brasil, atuando como fator multiplicador de riscos. O aquecimento global está em ritmo acelerado: 2024 foi o ano mais quente registrado (ultrapassando 1,5°C acima do nível pré-industrial), e a Organização Meteorológica Mundial (OMM) projeta 86% de chance de ao menos mais um ano exceder 1,5°C entre 2025 e 2029. O Brasil enfrenta um aumento de catástrofes (incidentes anuais quase dobraram desde 2020), como a seca amazônica em 2024 (a pior estiagem desde 1954) e as inundações no Rio Grande do Sul em abril e maio de 2024 (478 municípios e 2,4 milhões de afetados), aprofundando desigualdades sociais preexistentes. Os impactos setoriais são severos, com perdas anuais de R\$ 13 bilhões. A segurança energética é vulnerável a essas mudanças: o desmatamento amazônico reduz os “rios voadores”, causando perdas anuais bilionárias (perda anual estimada de 3.780 GWh, ou R\$ 1,1 bilhão somente nas hidrelétricas de Itaipu e de Belo Monte). A segurança alimentar é ameaçada (46% das pragas agrícolas podem piorar até 2100). Infraestruturas críticas são expostas a novos ris-

cos e a elevação do nível do mar ameaça a densa população costeira do Brasil.

| Demografia

A atual fase da transição demográfica global, impulsionada pela queda da taxa de fecundidade (global: 2,2 filhos por mulher em 2022; Brasil: 1,55) e pelo aumento da longevidade, reconfigura as perspectivas de distribuição de poder entre os países. Ocorrem assimetrias regionais: o Norte Global envelhece (o exemplo extremo é o Japão: 38% de idosos até 2060), pressionando sistemas de assistência e arranjos laborais, e a população de partes do Sul Global cresce a ritmo acelerado (África: 1,2 bilhão de habitantes para 2,5 bilhões até 2050). A população brasileira envelhece rapidamente (número de pessoas com mais de 65 anos subiu de 7,4% da população em 2010 para 10,9% em 2022), enfrentando um paradoxo: o aumento de diplomados no ensino superior (18,4% da população em 2022) coexiste com a emigração de pessoas com qualificação profissional. Isso intensifica a competição por talentos e por fluxos de remessas (o Brasil recebeu US\$ 4 bilhões em 2022). Regionalmente, o Brasil é destino migratório (150 mil venezuelanos acolhidos entre 2018 e 2025; 130 mil



haitianos entre 2010 e 2018), o que impõe desafios à prestação de serviços essenciais e à segurança fronteiriça. No total, o Brasil recebeu 457 mil imigrantes entre 2017 e 2022. Nesse contexto, são ampliados os riscos advindos do crime transnacional, que explora rotas para tráfico humano.

| Tecnologia

A transição para a Era Digital reconfigura o poder global, centrada na disputa geopolítica (EUA-China) por tecnologias críticas como inteligência artificial (IA), computação quântica, 5G/6G e infraestrutura espacial. A aceleração dessa transição em um contexto crescentemente competitivo impõe riscos sérios à segurança do país: a computação quântica ameaça a criptografia tradicional e ataques ciberné-

uticos a infraestruturas críticas se tornam frequentes (o Brasil sofreu 61 ataques contra infraestruturas críticas em 2023). O desafio nevrálgico é a soberania digital, minada pela dependência estrutural de hardware estrangeiro (como unidades de processamento gráfico – GPUs) e pela concentração de poder em *big techs*. Essas empresas monopolizam dados e desafiam estruturas estatais (como o caso do bloqueio da plataforma X no Brasil em 2024), ameaçando a autonomia decisória nacional. Embora vulnerável, o Brasil demonstra avanços, ocupando o 2º lugar em cibersegurança nas Américas e desenvolvendo soluções soberanas, como o aplicativo msg gov, solução governamental de comunicação segura com criptografia pós-quântica, enquanto busca cooperação internacional.

2. Situação Internacional

A ordem internacional, constituída por atores estatais e não estatais, por instituições e pela distribuição de poder entre eles, atravessa uma redefinição sistêmica. O cenário atual denota uma multipolaridade desequilibrada e desinstitucionalizada, caracterizada pelo acelerado declínio da ordem liberal pós-1945, consolidada sob liderança dos EUA. A competição estratégica entre grandes potências, especialmente EUA e China, é o fator central dessa mudança, gerando crescentes incertezas. Evidencia-se o enfraquecimento de pilares da governança internacional pós-1945 (ONU, OMC, FMI), prejudicados por disputas internas, perda de legitimidade e paralisia decisória, ao passo que novos arranjos internacionais, como os BRICS, vêm ganhando proeminência. O resultado é a erosão de consensos, a fragmentação da normatividade internacional e a conversão da economia em instrumento de pressão (sanções, tarifas). Para o Brasil, eleva-se o risco de pressões por alinhamento explícito. A estabilidade e a capacidade de manter relações múltiplas tornam-se, assim, ativos estratégicos para atrair investimentos e promover o desenvolvimento pacífico.

| Competição

A competição entre grandes potências vem se acelerando no domínio militar. Um indicador chave é o recorde de gastos militares globais, que atingiram US\$ 2,7 trilhões em 2024, com EUA (37%) e China (12%) respondendo por quase metade do total. A crescente insegurança internacional é agravada pelo desmonte da arquitetura de acordos nucleares (ABM, INF, New START), que levou ao

colapso do equilíbrio, constituindo a principal fonte de instabilidade global atualmente. Em janeiro de 2025, as potências nucleares possuíam aproximadamente 12.241 ogivas. A rivalidade EUA-China evoluiu para um confronto mais complexo, que militariza e securitiza esferas como a tecnológica e a econômica, com estratégias de de-risking e com sanções exacerbando o desacoplamento de cadeias produtivas. Nesse cenário, o Brasil enfrenta



pressões para abandonar sua tradicional política externa de equilíbrio, com os EUA demonstrando reduzida tolerância à autonomia estratégica sul-americana e impondo condicionalidades em diversas esferas.

| Conflitos

O acirramento da disputa estratégica global gera conflitos de atrito (Ucrânia) e riscos de escalada regional (como a ocorrida no Oriente Médio), resultando em ameaças transversais para o Brasil. Destacam-se a guerra cognitiva com uso de IA, as

pressões financeiras e as assimetrias digitais. A dependência de tecnologias estrangeiras (telecomunicações, nuvem) expõe o país a sabotagem, espionagem e coerção, comprometendo a soberania dos setores de Segurança e Defesa. Ao mesmo tempo, em um mundo conflagrado, seu histórico de paz e sua tradição mediadora constituem, para o Brasil, uma oportunidade singular para atrair investimentos, reforçada por uma posição diplomática pragmática, como membro do BRICS e candidato à Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

3. Entorno Estratégico: América do Sul

O entorno estratégico do Brasil apresenta desafios securitários prementes. O Atlântico mantém relevância vital: mais da metade da população brasileira vive no litoral, 97,6% da extração de petróleo e 80% do comércio nacional dependem do mar. A costa africana possui peso demográfico e econômico crescente (a Nigéria será o 3º país mais populoso em 2050). Na América do Sul, o Brasil (detentor de 50% do PIB e população regionais) compartilha 16,9 mil km de fronteiras e 60% do bioma amazônico, dispondo de mecanismos de integração como Mercosul e Unasul. A região atrai crescente interesse no contexto da rivalidade geopolítica entre EUA e China, com presença de potências extrarregionais. Isolados, os países sul-americanos têm relações assimétricas com polos globais; portanto, avançar na integração regional é fundamental para sustentar posições conjuntas mais estáveis e mais vantajosas.

| Segurança

A América do Sul está inserida de maneira assimétrica na competição entre grandes potências, o que aumenta a pressão por alinhamentos explícitos, prejudica a autonomia estratégica e amplia a margem para a atuação de atores extrarregionais. As potências projetam seus interesses políticos e econômicos, disputando o controle de vastos recursos estratégicos — como lítio (Bolívia, Argentina, Chile), terras raras e petróleo (do qual o Brasil possui mais de 16 bilhões de barris de reservas provadas), além dos recursos da Bacia Amazônica. A China consolidou-se como principal parceiro comercial, tendo o intercâmbio com a região superado US\$ 500 bilhões em 2024, o que pode

gerar novas dependências econômicas. Os EUA, por sua vez, têm exercido crescentes pressões por alinhamento, incluindo ameaças militares. Além do limitado poderio dissuasório contra potências extrarregionais, outra vulnerabilidade crítica dos países da região reside na limitação das capacidades estatais frente ao avanço do crime organizado transnacional. Essa fragilidade pode ser instrumentalizada por potências externas, que utilizam pretextos como o combate ao “narcoterrorismo” ou a proteção de “bens comuns globais” para justificar interferências e minar a soberania dos países.



| Integração

O Brasil enfrenta um paradoxo em seu entorno estratégico: enquanto sua projeção internacional é retomada (BRICS, G20, COP30), sua influência na América do Sul não se recupera na mesma medida, o que limita sua autonomia estratégica. Esforços de reintegração política desde 2023 (retorno à Unasul e Celac) encontram obstáculos significativos devido à dissonância com projetos políticos de nações vizinhas, resultando no enfraquecimento de ini-

ciativas multilaterais. Nesse cenário, a integração da infraestrutura física e logística emerge como o vetor mais resiliente da cooperação, exemplificada por projetos como o Corredor Rodoviário Bioceânico. Essa agenda pragmática não apenas fomenta o comércio intrarregional, mas também oferece uma alternativa para a segurança econômica nacional, fornecendo rotas de escoamento resilientes diante de crises e pressões externas, como a imposição de tarifas unilaterais pelos EUA em 2025.

4. Brasil: Desafios para a Inteligência

A ABIN tem a missão de antecipar ameaças à segurança do Estado e da sociedade para assessorar o mais alto nível decisório, salvaguardando conhecimentos sensíveis. Este documento atualiza os desafios de Inteligência prioritários para 2026, considerando o contexto das transições globais e o cenário internacional e regional. As análises, elaboradas por equipes transversais da Agência, sintetizam aspectos não sigilosos para informar autoridades sobre riscos e alternativas de mitigação, convidando também a sociedade a refletir e dialogar sobre a Inteligência de Estado.

| Segurança do processo eleitoral de 2026

A segurança do processo eleitoral de 2026 enfrenta ameaças complexas e multifacetadas, tendo como vetor principal a deslegitimação sistêmica das instituições democráticas. Esse processo, observado desde 2018 e que culminou nos atos de 8 de janeiro de 2023, mina a confiança na Justiça Eleitoral e no sistema de votação. Tal desafio é potencializado por inovações tecnológicas, notadamente o uso de Inteligência Artificial e de *deepfakes* para manipulação em massa e para disseminação de desinformação em larga escala. O cenário de profunda polarização social agrava esse risco. Adicionalmente, a integridade do pleito é desafiada pela crescente influência do crime organizado em territórios sob sua influência e pelo risco de interferência externa voltada a desestabilizar o processo eleitoral e favorecer interesses geopolíticos estrangeiros, exigindo alta capacidade de antecipação e resposta do Estado.

| Transição para a criptografia pós-quântica

A criptografia, pilar da soberania digital e da segurança governamental (comunicações sigilosas e transações digitais), enfrenta um ponto de inflexão. O advento da computação quântica, estimado para ocorrer no prazo de 5 a 15 anos, tornará obsoleta a criptografia de chaves públicas atual. A urgência da transição para algoritmos pós-quânticos (PQC) baseia-se em dois fatores: a tática adversária de “coletar agora, decifrar depois” (ameaçando segredos de longo prazo, como os segredos militares, diplomáticos e de Inteligência) e o tempo de migração (superior a uma década). Eventual fracasso em administrar esse processo (cenário de “apocalipse quântico”) comprometeria gravemente a soberania. A resposta exige cripto-agilidade e o desenvolvimento de uma criptografia de Estado autônoma, reduzindo a dependência externa sem ignorar padrões tecnológicos e procurando manter, ao longo do processo, a confiança do público.

O processo de transição é um projeto nacional de quatro etapas: conscientização institucional, mapeamento de ativos criptográficos, planejamento priorizado e execução gradual.

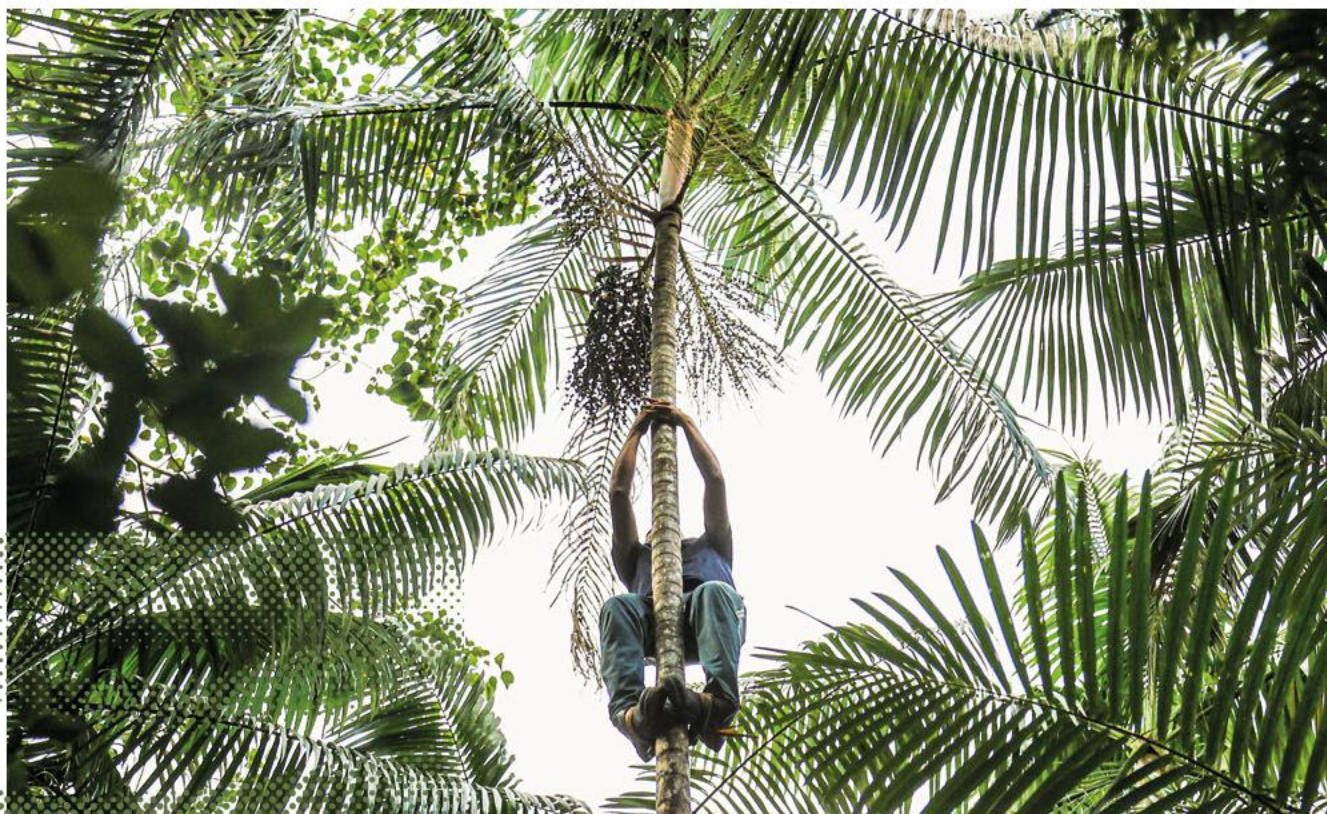
| Ataques cibernéticos autônomos com agentes de inteligência artificial

A transformação mais recente na segurança cibernética decorre da rápida evolução da inteligência artificial (IA), a qual era uma ferramenta e passa a ser um agente ofensivo autônomo, capaz de planejar, executar e adaptar ataques. A IA democratiza ameaças sofisticadas, permitindo a criação de *no-code malware* (RATs, ransomware) por atores pouco qualificados e escalando *spear-phishing* personalizado. O desafio central é geopolítico: a IA quebra a atribuição técnica (análise de TTPs, *fingerprinting*), gerando código variado e inserindo “bandeiras falsas” para negação plausí-

vel. Essa incerteza impede a dissuasão e eleva o risco de escalada horizontal de incidentes cibernéticos para conflitos militares. A velocidade da tecnologia cria um desequilíbrio (o ataque tem vantagem sobre a defesa), ameaçando infraestruturas críticas com ataques de dia zero (*zero-day attacks*) automatizados e potencializando a guerra de informação (com *deepfakes*, por exemplo) e a ciberespionagem. A resposta, um desafio de governança global, deve ser estratégica, combinando agentes de defesa autônomos com cooperação internacional (normatização e *watermarking*).

| Reconfiguração das cadeias de suprimento globais

A reconfiguração das cadeias globais de suprimentos é impulsionada pela ascensão da China, pela guerra econômica com os EUA e pelos choques da COVID-19, que expuseram vulnerabilida-





des sistêmicas. A conjuntura atual é marcada por uma desglobalização deliberada, que prevê tarifas agressivas e a desvalorização do dólar, acelerando a queda de sua participação nas transações globais (de 72% na virada do século para 59% atualmente). Nesse cenário, o Brasil se encontra em uma posição de dupla dependência: da China para seu superávit comercial (commodities) e do capital e de tecnologias ocidentais (EUA) para investimentos, sendo, ademais, afetado por tarifas norte-americanas (como no caso da imposição de tarifas de até 50%). O aproveitamento de oportunidades como aquelas abertas pelo *friendshoring* é limitado por fragilidades internas persistentes, a exemplo da desindustrialização.

| Dependência tecnológica, atores não estatais e interferência externa

O domínio digital consolidou-se como arena central da competição geopolítica, destacando-se o risco de atuação das *big techs* como vetores de influência de seus Estados-sede. Nesse contexto, a dependência de provedores externos em infraestruturas críticas (nuvem, dados, identidade digital) é uma vulnerabilidade estratégica severa para o Brasil. A dependência tecnológica habilita ações sofisticadas de interferência externa em múltiplos níveis: guerra cognitiva (por desinformação algorítmica), espionagem sistêmica (acesso a dados sensíveis) e coerção (ameaça latente de sabotagem de infraestruturas críticas). A eficácia da interferência reside na combinação híbrida desses métodos, permitindo a atores externos modular o debate público e influenciar processos decisórios, colocando em risco a soberania nacional.

A agenda de produção de conhecimentos de Inteligência é diversificada, refletindo a complexidade dos desafios presentes. Tanto os conteúdos produzidos quanto os métodos, fontes e recursos empregados para a atuação dos órgãos do Sisbin, incluindo a ABIN, podem e devem ser auditados e controlados por meio de diferentes instrumentos e instâncias, na forma da lei e de procedimentos administrativos que são públicos e cada vez mais aperfeiçoados conforme as exigências da sociedade. Não menos importante, embora o segredo seja parte indissociável do trabalho da Inteligência, a participação da sociedade na escolha desses assuntos e dos meios legítimos para abordá-los é essencial no regime democrático. A identificação prospectiva e fundamentada de prioridades, para a qual *Desafios de Inteligência – Edição 2026* pretende contribuir, é parte desse processo.

Nota Metodológica

A série *Desafios de Inteligência* analisa fenômenos globais e internacionais e seus vínculos com a agenda de produção de conhecimentos de Inteligência sobre riscos, ameaças e vulnerabilidades de segurança para o Brasil.

Seu objetivo não é produzir cenários, mas avaliar situações e eventos em diferentes escalas temporais e geográficas, os quais podem afetar a segurança das pessoas e das instituições no país.

Embora seja possível defini-la de diferentes maneiras, a segurança é compreendida aqui como a capacidade da sociedade e do Estado de antecipar, prevenir e responder, de forma crível, a riscos, ameaças e vulnerabilidades em múltiplos níveis (global, internacional, regional e nacional) contra o território, a população, o Estado Democrático de Direito, o desenvolvimento socioeconômico e a soberania nacional. Assim, mesmo quando são tratados assuntos de grande amplitude tais como as transições globais (climática, demográfica e tecnológica), o foco é ajustado conforme a definição de segurança adotada.

Os nexos causais entre as transições globais, a situação internacional, a situação na América

do Sul e os desafios nacionais de Inteligência são complexos. O que acontece no mundo afeta nosso país. Por sua vez, a maneira como as instituições e a sociedade lidam com tais desafios contribui para os resultados agregados a nível nacional, regional, internacional e global. Nesses distintos níveis, as dinâmicas se retroalimentam, afetando a segurança do país de diversas formas. A abordagem adotada aqui parte do nível mais amplo e, aplicando a definição de segurança acima, balizada pelos interesses nacionais do Brasil, estabelece recortes cada vez mais específicos para chegar à definição e à análise dos desafios para a Inteligência.

A série *Desafios de Inteligência* parte de duas premissas fundamentais: é necessário ampliar o público que discute os assuntos de Inteligência e, para fazê-lo de forma substantiva, é imprescindível lançar um olhar prospectivo para os seus principais desafios, produzindo análises relevantes. As duas

premissas possuem implicações do ponto de vista metodológico, as quais devem ser abordadas aqui para uma melhor compreensão do documento.

A primeira parte da análise, que compreende os capítulos 1, 2 e 3, é baseada em pesquisa em fontes públicas, para a qual contribuíram os esforços de pesquisadores do Núcleo de Pesquisa em Inteligência da Esint. Por um lado, o uso de fontes públicas permite aproveitar o conhecimento mais atual e acreditado sobre os temas abordados, ao mesmo tempo em que se aplica uma perspectiva própria da Inteligência, com ênfase em riscos, ameaças e vulnerabilidades. Por outro lado, a utilização de fontes públicas permite estabelecer diálogo com os centros de produção de conhecimento técnico e científico, mas sobretudo com o público, que pode consultar livremente as fontes utilizadas e verificar as análises e conclusões. Na pesquisa, foram privilegiados trabalhos científicos, documentos oficiais do governo brasileiro e de governos estrangeiros, documentos de organismos internacionais e de organizações da sociedade civil.

Além disso, seguindo a proposta da edição passada, foram novamente consultados especialistas externos. As atividades de ensino, pesquisa e extensão da Escola de Inteligência (Esint), tal como na edição anterior, proporcionaram contato contínuo com pesquisadores de diferentes áreas do conhecimento, em dezenas de eventos, alguns deles abertos, outros restritos e outros, ainda, com a participação de servidores de órgãos do Sistema Brasileiro de Inteligência.

Nesta *Edição 2026*, todavia, realizou-se também uma consulta sistemática com especialistas

externos, tanto pesquisadores quanto profissionais do Sisbin, de modo a coletar previamente suas avaliações e utilizá-las para guiar, desde o princípio, as análises aqui consolidadas. As contribuições, voluntárias, foram solicitadas por meio de formulários temáticos. Foram distribuídos cinco modelos de formulário, contendo perguntas abertas sobre clima, demografia e migrações, saúde pública, tecnologia e, por fim, situação internacional e regional. Alguns especialistas autorizaram a Esint a mencioná-los nos agradecimentos, enquanto outros preferiram contribuir de forma anônima. No âmbito do Sisbin, foram também enviadas contribuições de natureza institucional. Os especialistas consultados trabalham em instituições de ensino e pesquisa públicas e privadas, bem como em órgãos governamentais.

A segunda premissa fundamental dos *Desafios de Inteligência* é o reconhecimento de que um diálogo substantivo com a sociedade sobre a Atividade de Inteligência depende da disponibilização de análises prospectivas úteis. Isso exige partir do estudo de fontes públicas e da colaboração com especialistas externos, mas também priorizar e analisar problemas concretos mobilizando as capacidades e conhecimentos especializados dos profissionais de Inteligência, adquiridos ao longo dos anos em sua prática analítica e operacional. Essa é a perspectiva do capítulo 4 deste documento, no qual são analisados os desafios para a Inteligência em 2026.

Os temas dos desafios foram definidos pelos departamentos analíticos da ABIN, considerando as necessidades emergentes de assessoramen-

to especializado identificadas ao longo do último ano. Trata-se de uma seleção com olhar prospectivo que decorre da agenda regular de produção de conhecimentos de Inteligência, revisada periodicamente, e dos projetos especiais que organizam o acompanhamento de situações prioritárias.

As avaliações dos desafios foram realizadas por equipes multidisciplinares de analistas de Inteligência em duas etapas. Primeiro, sob a coordenação da Esint, foi conduzido um exercício de análise estruturada, com aplicação encadeada de diferentes técnicas, resultando em insumos organizados em cenários simples. Em seguida, a partir dos resultados do exercício, analistas especializados em cada um dos temas elaboraram avaliações mais aprofundadas, aportando o conhecimento acumulado pelo trabalho de Inteligência regular e as perspectivas específicas de riscos para 2026. Dessa forma, combinaram-se a aplicação de técnicas analíticas estruturadas com o conhecimento aprofundado dos especialistas temáticos.

Por fim, cabe ressaltar que a série *Desafios de Inteligência* não se sobrepõe ou compete com publicações, análises ou declarações de outras instituições governamentais. Seus recortes temporal (um ano), conceitual (questões securitárias), de dimensões de análise (global, internacional, regional e nacional) e temático (Inteligência) definem uma perspectiva única, típica dos serviços de Inteligência. Com sua publicação, a ABIN busca consolidar essa perspectiva e compartilhá-la amplamente, promovendo o debate e o aperfeiçoamento das concepções e práticas relacionadas à Inteligência em colaboração com a sociedade.



Exposição Sonhos: história, ciência e utopia, no Museu do Amanhã, na zona portuária do Rio de Janeiro | Foto: Tomaz Silva (Agência Brasil)



Transições Globais

01



Transições globais são um conjunto de mudanças significativas que ocorrem em escala mundial, com grande potencial disruptivo. As transições afetam a sociedade, a cultura, a economia, o meio ambiente e outras esferas da vida humana e incidem de forma simultânea e correlacionada, influenciando-se umas às outras. Compreender sua evolução ao longo dos processos históricos e prever seu desenvolvimento futuro são tarefas complexas. *Desafios de Inteligência – Edição 2026* busca acompanhar e atualizar, do ponto de vista da Inteligência de Estado, o momento atual dos processos de transição global nos domínios do clima, da demografia e da tecnologia.

As relações internacionais envolvem diversos tipos de atores (governos nacionais, burocracias especializadas, empresas, organizações internacionais, grupos e indivíduos). Tais atores fazem escolhas e agem constrangidos por estruturas construídas historicamente, de tipo político, econômico e social. Todavia, tanto os constrangimentos estruturais quanto as interações en-

tre atores ocorrem em contextos mais amplos, ambientais, humanos e tecnológicos. Desde o seu surgimento, a espécie humana aumentou continuamente a capacidade de alterar tais contextos. Atualmente, esse processo chegou a um ponto em que o aumento da densidade das interações (transportes, comunicações, energia, informação) levou especialistas a caracterizarem

o contexto das relações internacionais em função do impacto humano sobre o planeta, utilizando termos como Antropoceno ou Era Digital.

Nas últimas décadas, têm-se acumulado evidências sobre as causas e os efeitos das mudanças climáticas, o perfil demográfico das sociedades vem se alterando profundamente e inovações tecnológicas transformam de modo irreversível diversos aspectos da vida humana, com consequências importantes para o Brasil¹. Assim como essas mudanças abrem oportunidades, também trazem riscos para a segurança das pessoas e das instituições. Este capítulo tratará das transições climática, demográfica e tecnológica, sob o ponto de vista da segurança do Brasil.

Clima

O enfrentamento da mudança do clima — anteriormente percebida como uma ameaça distante — consolidou-se como imperativo para a segurança do Brasil. As alterações nos padrões climáticos planetários encontram-se em um ponto de inflexão e o clima será cada vez mais um multiplicador de riscos. Essas mudanças são impulsionadas principalmente por fatores antrópicos, que se manifestam de forma cada vez mais evidente, incluindo o desflorestamento, a poluição, a degradação de ecossistemas e o aquecimento global.

O cenário climático global, em 2024 e em 2025, demonstra uma acentuação na elevação da temperatura do planeta. O ano de 2024 foi confirmado pelo Serviço de Mudanças Climáticas da União Europeia como o ano mais quente já registrado, marcando o primeiro ano-calendário em que a



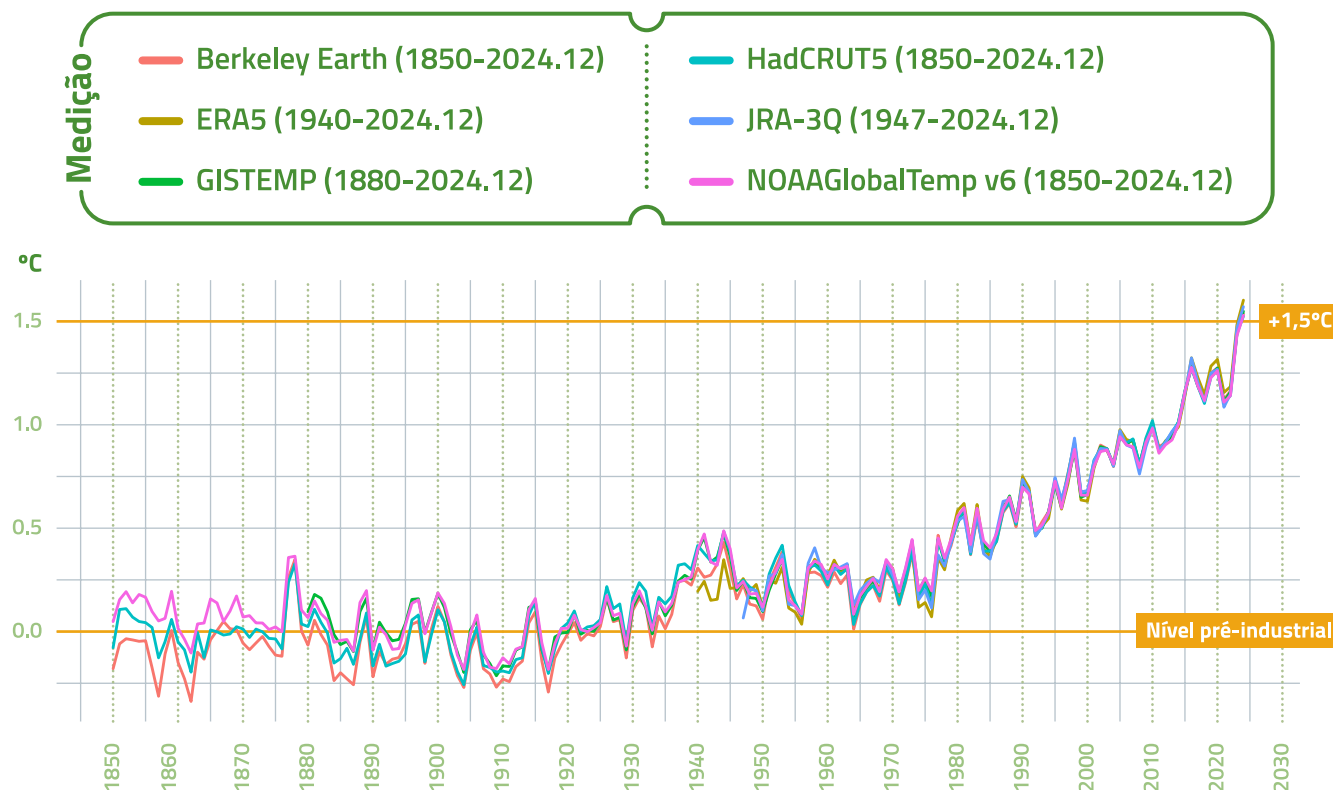
Forte chuva na capital paulista | Foto: Paulo Pinto (Agência Brasil)

temperatura média global excedeu 1,5°C acima do nível pré-industrial (Gráfico 1)². Além disso, a Organização Meteorológica Mundial (OMM) afirma que os últimos dez anos (2015-2024) foram os dez mais quentes já registrados³. As projeções da OMM para os próximos cinco anos (2025-2029) são alarmantes: há uma probabilidade de 86% de que pelo menos um desses anos exceda 1,5°C acima do nível pré-industrial e uma chance de 70% de que a média de cinco anos para o período seja superior a 1,5°C⁴.

O ano de 2024 confirmou a quebra da barreira de 1,5°C. A OMM projeta 86% de chance de um novo recorde ser batido até 2029, consolidando a crise climática como um multiplicador de riscos.

Gráfico 1 Temperatura média global (1850-2024)

Diferença em relação ao nível pré-industrial
(média 1850-1900)



Fonte: Adaptado de Organização Meteorológica Mundial (WMO), "Global mean temperature 1850-2024", <https://wmo.int/resources/dashboards/global-mean-temperature-1850-2024>.

A mudança do clima possui caráter dinâmico, tendo a ação humana papel central, e as relações entre variáveis podem gerar consequências de difícil previsão. A coexistência de múltiplos sistemas com potenciais “pontos de não retorno” (*tipping points*), como a degradação de biomas, o enfraquecimento da Corrente do Golfo, a diminuição do nível de oxigênio nos oceanos e o degelo de solos polares (*permafrost*), pode levar à retroalimentação dos fatores de mudança climática⁵. Dos subsistemas com pontos de não retorno, aqueles com limites mais baixos em relação ao aquecimento global são os mantos de gelo ártico e antártico, entidades críticas para a segurança hídrica, climática e energética do Brasil, uma vez que o derretimento de gelo nos polos influencia as regiões atlântica e amazônica⁶. Mitigar tais efeitos exige ampla cooperação internacional e um vasto esforço de modificação de padrões de vida.

A mudança climática é, assim, um dos processos de transição global capazes de afetar negativamente a segurança do Brasil. Ela pode ser caracterizada como uma ameaça securitária não convencional, cujos riscos não são facilmente mitigados por recursos de poder tradicionais⁷. Além disso, ela não opera isoladamente: a crise climática intensifica desafios securitários transnacionais já existentes, atuando como multiplicadora de riscos tais como crises migratórias, conflitos armados, insegurança alimentar e crises de saúde pública⁸.

O Brasil está enfrentando aumento acentuado de catástrofes relacionadas ao clima, com o número anual de incidentes quase dobrando desde 2020 em comparação com as duas décadas anteriores⁹. A região amazônica, por exemplo, enfrentou condições de seca severa em 2023/2024, considerada a mais intensa desde 1954. Nesse mesmo período, estima-se que 59% do território brasileiro foi afetado por secas, causando escassez de água e perda de meios de subsistência e

colheitas¹⁰. Enquanto isso, a região Sul tem experimentado eventos de chuva mais frequentes e intensos, elevando os riscos de inundações e deslizamentos de terra, particularmente em áreas urbanas. A tragédia das enchentes no Rio Grande do Sul, entre abril e maio de 2024, é um exemplo contundente: 478 municípios (96% do estado) e 2,4 milhões de pessoas (20% da população) foram afetados¹¹.



Tuiuiú, ave símbolo do Pantanal, protege seu ninho em meio aos incêndios florestais no Pantanal | Foto: Marcelo Camargo (Agência Brasil)



A crise climática já se manifesta em eventos extremos no Brasil: a seca amazônica de 2023/2024 foi a pior desde 1954, enquanto as enchentes de 2024 no RS afetaram 478 municípios (96% do estado).

A crescente intensidade e a imprevisibilidade desses eventos ameaçam a segurança energética, a segurança alimentar, a segurança de infraestruturas críticas e a segurança humana em geral. Diante disso, o trabalho governamental transversal para identificar vulnerabilidades e planejar investimentos públicos de mitigação e adaptação é imprescindível para a segurança da sociedade e do Estado. Destaca-se que a mudança do clima não é uma força neutra: ela aprofunda as desigualdades sociais preexistentes, particularmente no acesso a bens e serviços fundamentais. Populações já marginalizadas tendem a arcar com uma parcela maior do peso dos impactos¹², o que pode levar a um aumento da instabilidade social, crises de saúde e pressões migratórias internas.

A dependência do Brasil de fontes hídricas em sua matriz de energia, embora o coloque em posição de destaque na transição para fontes renováveis¹³, pode redundar em vulnerabilidades para a segurança energética nacional quando conjugada aos efeitos da crise climática, com reflexos na economia e na estabilidade social. A crise hídrica de 2021, por exemplo, forçou a ativação de termelétricas, mais caras e poluentes, resultando em aumento dos custos de energia¹⁴.

A Floresta Amazônica desempenha um papel fundamental na regulação dos padrões de chuva por meio dos chamados “rios voadores”, que se

originam na região e irrigam o Brasil central e o Sudeste. O desmatamento na Amazônia reduz a umidade nessas correntes de ar, diminuindo a precipitação e, por consequência, a geração hidrelétrica. Estudos recentes quantificam essa ameaça: as usinas de Itaipu e Belo Monte, que respondem por 23% da eletricidade do Brasil, deixam de gerar anualmente 3.780 GWh devido ao desmatamento, resultando em uma perda de receita superior a R\$ 1,1 bilhão¹⁵.

A segurança energética e alimentar do país está em risco. O desmatamento amazônico, ao reduzir os “rios voadores”, já causa perdas anuais de R\$ 1,1 bilhão na geração de energia em usinas hidrelétricas estratégicas como Itaipu e Belo Monte.

Encarado pelo prisma securitário, portanto, o desmatamento na Amazônia atenta contra a estabilidade econômica do país. A destruição contínua da floresta mina a confiabilidade e a acessibilidade da matriz elétrica, aumentando o risco de crises energéticas, de elevação de custos para os consumidores e de redução da produtividade industrial.

A crescente pressão das mudanças climáticas também afeta a produção e a distribuição de alimentos, com implicações diretas para a segurança alimentar e a estabilidade econômica. Em 2024, a agricultura brasileira enfrentou desafios significativos, incluindo secas e inundações relacionadas ao *El Niño*. A já mencionada tragédia no Rio Grande do Sul afetou mais de 206.000 propriedades rurais¹⁶; inversa e simultaneamente,



Colheita de açaí plantado em sistema de agrofloresta | Foto: Marcelo Camargo (Agência Brasil)



Plantação de soja no município de Alto Paraíso mostra o avanço da fronteira agrícola na região da Chapada dos Veadeiros | Marcelo Camargo (Agência Brasil)

a seca assolou 69% dos municípios da Amazônia Legal¹⁷. Financeiramente, o Banco Mundial estima que os eventos climáticos extremos no Brasil causem perdas de R\$ 13 bilhões ao ano em média¹⁸.

A crise climática também se manifesta na proliferação de pragas agrícolas. Projeta-se que 46% das doenças agrícolas no Brasil piorarão até 2100¹⁹, com impacto direto sobre culturas estratégicas, a exemplo do milho e da soja. Temperaturas crescentes e mudanças nos padrões de chuva promovem a disseminação de fungos, vírus e

vetores. As mudanças climáticas também podem reduzir a eficácia dos pesticidas, aumentando custos e riscos ambientais²⁰. Essa amplificação de doenças representa uma ameaça à posição do Brasil como potência agrícola global e à sua segurança alimentar interna, demandando estratégias para a adoção de práticas agrícolas resilientes ao clima.

As infraestruturas críticas nacionais, vitais para a economia e para a circulação de bens, serviços e pessoas, estão crescentemente expostas a danos por eventos climáticos extremos.



As inundações no Rio Grande do Sul, em maio de 2024, levaram ao fechamento do Aeroporto Internacional de Porto Alegre por quase cinco meses²¹. Paralelamente, as secas ameaçam o transporte aquaviário, como evidenciado pela estiagem na Bacia Amazônica no segundo semestre de 2023, que afetou o transporte fluvial e as importações para o estado do Amazonas²².

A elevação do nível do mar, fenômeno vinculado às mudanças climáticas, representa uma ameaça de longo prazo com impactos já visíveis e crescentes. O nível do mar global aumentou mais rápido do que o esperado em 2024, a uma taxa de 0,59 cm/ano, totalizando um aumento de 10 cm desde 1993²³. Isso representa uma ameaça fundamental, visto que mais da metade dos brasileiros reside em setores censitários localizados a até 150 km da costa²⁴. Parte desse espaço localiza-se em baixa altitude e concentra grandes metrópoles, centros industriais e infraestruturas estratégicas²⁵.

Os impactos climáticos também afetam a segurança pública e a coesão social, especialmente em um contexto de crescente frequência de desastres. No longo prazo, a recorrência de secas severas na região amazônica tende a impulsionar o deslocamento para centros urbanos e outras regiões do Brasil²⁶. Globalmente, estima-se que entre 200 milhões e 1 bilhão de pessoas podem se tornar migrantes climáticos até 2050²⁷.

No cenário internacional, a crise climática altera a distribuição relativa de poder. Países mais ricos podem investir mais em mitigação e adaptação, preservando seus recursos, enquanto Estados menos afluentes não têm a mesma capacidade²⁸. Ao problema de mitigar as consequências soma-se, portanto, o de planejar uma transição ecológica justa para as pessoas e para os países. Como potencial mecanismo de equilíbrio pode-se mencionar o desenvolvimento do mercado de créditos de carbono, instrumento que não apenas

possui alta relevância para a preservação das florestas tropicais e para o controle das emissões de gases de efeito estufa (GEE), como também se alinha ao imperativo estratégico do Brasil de promoção do desenvolvimento socioeconômico sustentável, em especial na região amazônica. Outra inovação nesse sentido foi a recente proposta brasileira para financiar a preservação das florestas tropicais, o Fundo Florestas Tropicais para Sempre (*Tropical Forests Forever Facility – TFFF*)²⁹.

Para a segurança do Brasil, são cruciais a preservação de biomas, a mitigação das vulnerabilidades da população a eventos extremos, o planejamento para enfrentar o aumento do nível dos oceanos em áreas costeiras densamente povoadas e o gerenciamento dos efeitos das mudanças climáticas para a segurança alimentar e a segurança energética.

A Inteligência de Estado oferece contribuições relevantes nessas frentes. Atua pela preservação ambiental ao produzir conhecimentos estratégicos sobre ilícitos e redes criminosas e ao apoiar a desintrusão de Terras Indígenas, regularizando o controle sobre o território e os recursos naturais. Além disso, age na proteção de conhecimentos tradicionais e biodiversidade. Auxilia o Governo Federal e os entes subnacionais com informações e articulação institucional em situações de crise. E, em eventos como a COP30, realizada em Belém em novembro de 2025, provê assessoramento em diversas áreas, tais como apoio à agenda de negociações, avaliação de riscos de segurança e logísticos e proteção de ativos informacionais sensíveis.

Demografia

Ao longo do século XXI, o mundo atravessará uma transição demográfica acelerada, impulsionada pela redução generalizada da fecundidade e pelo

envelhecimento populacional, com marcadas assimetrias regionais. Esses fenômenos, ocorrendo em uma escala inédita na história, mas em etapas e ritmos distintos nos diferentes países, prometem redefinir a divisão internacional do trabalho, os movimentos migratórios e questões críticas de saúde, segurança e geopolítica.

Essa reconfiguração demográfica global influenciará de maneira significativa a distribuição de poder econômico e político (Gráfico 2). Nesse cenário, países que conseguirem articular políticas migratórias coerentes, integrar populações diversas e investir em inovação obterão vantagens competitivas duradouras. Em contrapartida, aqueles que falharem em se adaptar enfrentarão severas pressões fiscais, declínio relativo de sua influência internacional e aumento das tensões sociais internas.

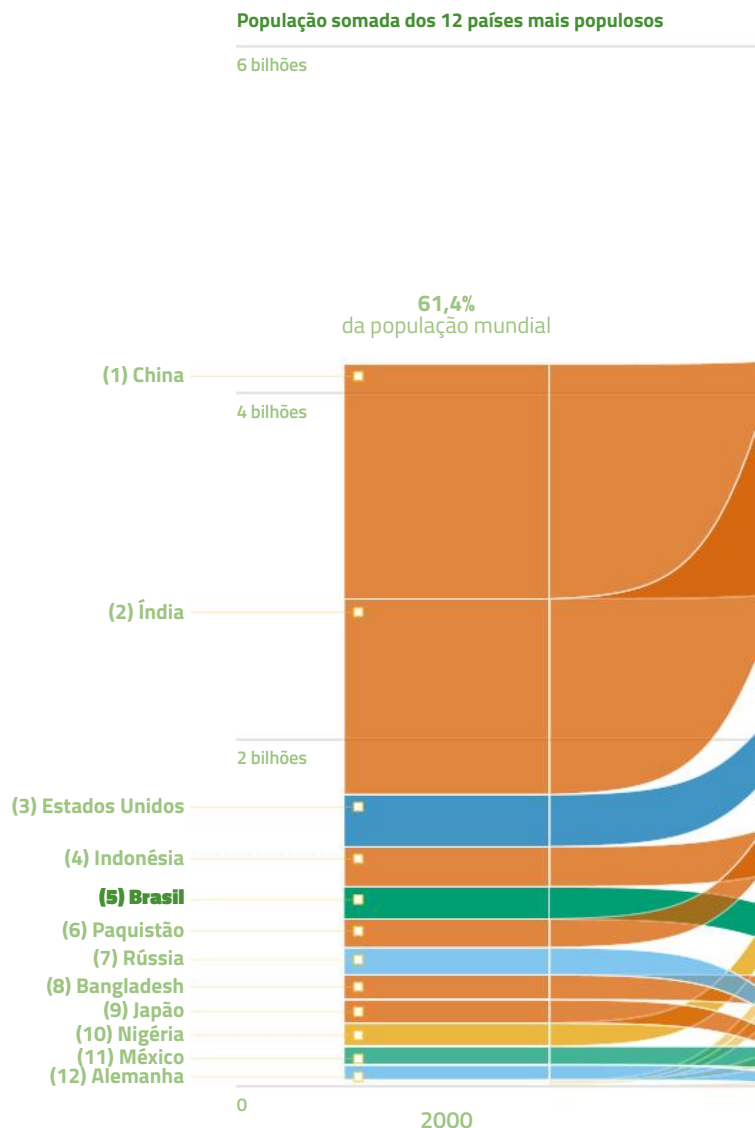
Para o Brasil, esse panorama constitui tanto um desafio complexo quanto uma oportunidade estratégica, que dependerá da capacidade do país de alinhar políticas de formação, retenção e atração de talentos às novas demandas da economia global, além de incorporar uma agenda consistente de acolhimento de migrantes, integração e combate à discriminação.

O fundamento da transição demográfica global reside na drástica e contínua redução da taxa média de fecundidade. De acordo com a Organização das Nações Unidas (ONU)³⁰, essa taxa era de 3,3 filhos por mulher em 1990 e caiu para 2,2 em 2024. Esse valor fica pouco acima da taxa de reposição populacional, nível necessário para manter a população global estável (2,1 filhos por mulher).

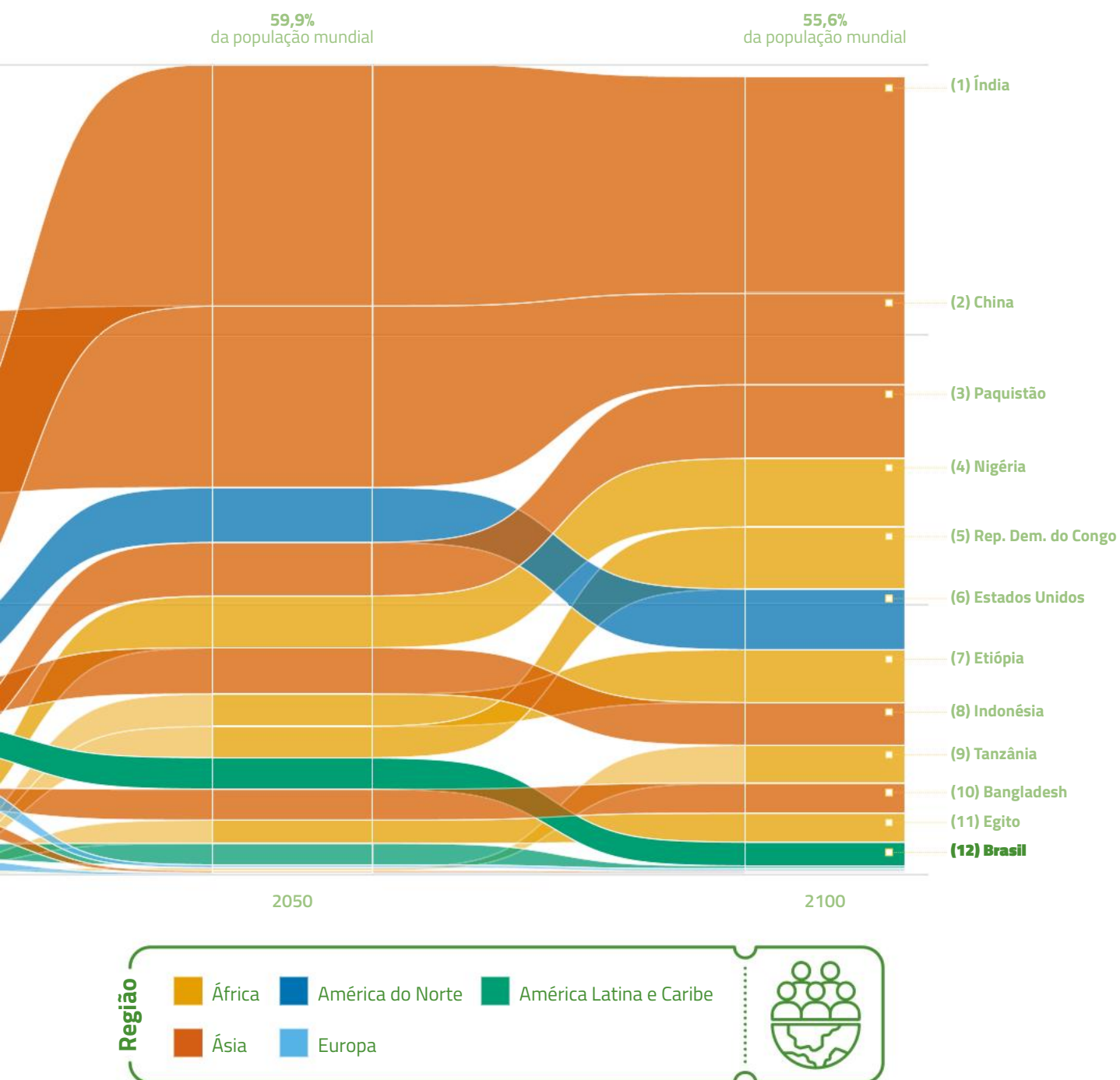
Para o Brasil, essa tendência é ainda mais acentuada e consolidada. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE)³¹, a taxa de fecundidade no país, que era de 2,39 filhos por mulher no ano 2000, despencou para 1,55 em 2022, valor significativamente abaixo da taxa de

Gráfico 2 Evolução da população 2000-2100

Os 12 países mais populosos em 2000 e os 12 mais populosos em 2100 (projeção)



Fonte: Organização das Nações Unidas, "World Population Prospects 2024," <https://population.un.org/wpp>.





reposição. Estudos indicam que essa queda continuará, com a taxa podendo chegar a 1,45 filhos por mulher até 2050³².

A transição demográfica brasileira é acelerada: a taxa de fecundidade caiu para 1,55 (2022), muito abaixo da reposição (2,1), e a população idosa (65+) saltou de 7,4% (2010) para 10,9% (2022), pressionando o sistema de seguridade social.

Embora a queda da fecundidade seja um fenômeno global, seu ritmo varia enormemente entre as regiões. Na Europa e na América do Norte, o declínio começou de forma gradual em meados do século XIX, com o avanço da Revolução Industrial. Já na América Latina e no Leste Asiático, o processo iniciou-se apenas na segunda metade do século XX, porém ocorreu de maneira mais abrupta e acelerada. Em contraste, certas regiões mantêm taxas de fertilidade relativamente altas, como em países populosos da África (Nigéria, Angola e Congo)³³ e em nações de maioria muçulmana. Essa disparidade pode afetar sensivelmente a balança de poder mundial, considerando, por exemplo, a expansão religiosa frequentemente associada ao crescimento populacional³⁴.

Conectado à queda da fecundidade, o aumento da expectativa de vida impulsiona o envelhecimento da população mundial. Dados da Organização Mundial de Saúde³⁵ mostram que, entre 2000 e 2019, a expectativa de vida global elevou-se em mais de seis anos, passando de 66,8 para 73,1 anos. Apesar de um recuo para 71,4 anos em 2021 devido à pandemia de Covid-19, a tendência

de alta deve ser retomada, com uma projeção de aumento de mais 4,4 anos até 2050³⁶.

Como reflexo direto, a estrutura etária global está mudando radicalmente. Em 1950, apenas 5% da população mundial (uma em cada 20 pessoas) tinha 65 anos ou mais. Em 2021, essa proporção dobrou para 10% (uma em cada dez). A projeção da ONU para 2050 é que 17% da população do planeta (uma em cada seis pessoas) esteja nessa faixa etária. No Brasil, o envelhecimento também é visível: o percentual de pessoas com 65 anos ou mais saltou de 7,4% em 2010 para 10,9% em 2022³⁷.

Enquanto as sociedades desenvolvidas envelhecem de forma acelerada, várias regiões do Sul Global vivenciam um crescimento populacional robusto. Na União Europeia³⁸, projeta-se que a população em idade ativa continue a declinar, com uma perda estimada de 35 milhões de pessoas com menos de 65 anos entre 2022 e 2050, o que pressiona fortemente os sistemas previdenciários, a saúde pública e a produtividade econômica. No Japão³⁹, paradigma do envelhecimento extremo, projeta-se que 38% de sua população terá 65 anos ou mais até 2060. Essa realidade compromete a renovação da força de trabalho e obriga a revisão de políticas migratórias historicamente restritivas.

O mundo enfrenta uma profunda divisão demográfica: o Norte Global envelhece (Japão terá 38% de idosos até 2060), enquanto a população de partes do Sul cresce (população da África Subsaariana dobrará para 2,5 bilhões até 2050), redefinindo o poder global.

Em contraste, a África Subsaariana desponta como o principal polo de crescimento populacional, com estimativas da ONU apontando que a região deverá dobrar sua população até 2050, passando de 1,2 bilhão para 2,5 bilhões de habitantes. A Ásia Meridional⁴⁰ também manterá um ritmo de expansão significativo. Entretanto, apesar do potencial de uma força de trabalho abundante, países como Paquistão e Bangladesh enfrentam limitações estruturais, como desigualdades acentuadas e investimento limitado em educação e saúde, fatores que podem restringir a conversão dessa vantagem demográfica em liderança econômica efetiva.

O desequilíbrio demográfico entre países do Norte Global - cuja população apresenta média de idade mais elevada - e países do Sul Global - de perfil mais jovem - está redefinindo os fluxos migratórios e intensificando a competição por talentos. Países desenvolvidos necessitarão cada vez mais importar mão de obra jovem e qualificada para sustentar suas economias. Em balanço de 2024, a OCDE observou em diversos de seus países-membros a flexibilização seletiva da imigração, combinando políticas de atração de trabalhadores qualificados com a diminuição dos índices gerais de migração⁴¹.



Instalações de acolhimento de venezuelanos não apresentam mais grandes filas | Foto: Marcelo Camargo (Agência Brasil)

As regiões com saldo demográfico positivo, por sua vez, podem se tornar não apenas fornecedoras de trabalhadores, mas também mercados consumidores estratégicos. Contudo, se por um lado elas se beneficiam das remessas de recursos enviadas por seus emigrantes, por outro, elas também perdem trabalhadores qualificados. O Banco Mundial⁴² calculou que as remessas globais ultrapassaram US\$ 800 bilhões em 2022, sendo uma fonte vital de receita para países menos desenvolvidos. No Brasil, as remessas somaram mais de US\$ 4 bilhões em 2022.

A intensificação dos fluxos migratórios gera desafios complexos de integração nos países receptores, especialmente quando existem diferenças culturais marcantes, podendo estimular tensões internas e discursos nacionalistas que ameaçam a coesão social. Experiências internacionais oferecem modelos de sucesso: o Canadá, com seu sistema de imigração por pontos⁴³, e a Austrália, com vistos por qualificação profissional⁴⁴, conseguiram construir narrativas positivas sobre a imigração, conquanto enfrentem resistências políticas internas.

Com efeito, a crescente restrição de políticas migratórias nos países desenvolvidos abre oportunidades para o Brasil atrair talentos e incentivar o retorno de profissionais qualificados. O Censo de 2022 registrou que 457 mil pessoas imigraram para o Brasil entre 2017 e 2022⁴⁵. Mais recentemente, pode-se mencionar políticas públicas de incentivo à fixação de profissionais qualificados no país, a exemplo do programa Conhecimento Brasil⁴⁶, e a expansão do mercado de trabalho formal observada nos últimos anos⁴⁷.

Regionalmente, o Brasil tem sido um destino central para fluxos migratórios. A Operação Acolhida, criada em 2018, exemplifica a resposta estatal a esses fluxos. De um total de mais de sete milhões de venezuelanos que migraram para pa-



íses vizinhos entre 2015 e 2022⁴⁸, cerca de 200 mil vieram para o Brasil⁴⁹; desses, 150 mil foram acolhidos e se instalaram em mais de 1.100 municípios até meados de 2025⁵⁰. A imigração haitiana, impulsionada pelo terremoto de 2010, também foi expressiva, com cerca de 130 mil ingressos até 2018⁵¹. Haitianos foram responsáveis por 40% das carteiras de trabalho emitidas a imigrantes em 2015⁵², concentrando-se em atividades industriais no Sul e Sudeste. Tais fluxos são exemplos de como o país pode compensar a tendência de estagnação da população economicamente ativa nos anos vindouros, embora também gerem desafios, especialmente em municípios fronteiriços, onde podem sobrecarregar serviços básicos e agravar problemas sociais.

O Brasil é um destino central de fluxos mistos (Operação Acolhida interiorizou 150 mil migrantes venezuelanos), mas essa dinâmica gera riscos de segurança em fronteiras exploradas pelo crime transnacional para tráfico humano e garimpo.

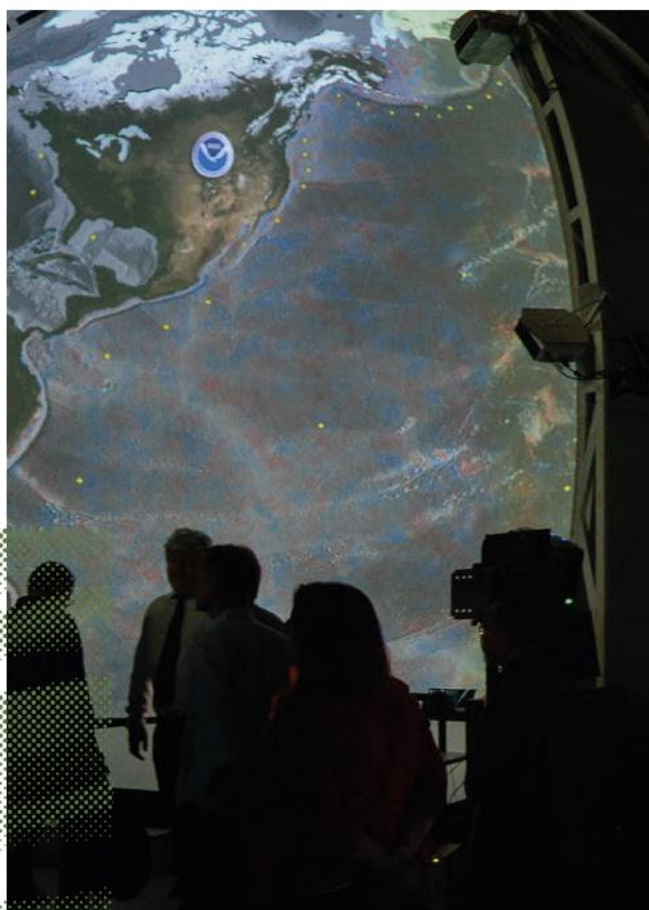
As transformações demográficas e os deslocamentos populacionais também trazem consigo importantes implicações para a saúde pública. Migrantes, especialmente refugiados, frequentemente enfrentam falhas no acesso à vacinação, diagnóstico e tratamento de doenças⁵³. Além disso, o aumento da densidade demográfica próximo a áreas de vegetação nativa, muitas vezes impulsionado por desmatamento e mudanças climáticas, aproxima humanos e animais silvestres, favorecendo o surgimento de doenças zoonóticas e novas epidemias⁵⁴. O envelhecimento populacional, por sua vez, acarreta uma demanda crescente por serviços médicos, sobrecarregando os sistemas de saúde e aumentando sua vulnerabilidade a outras crises.

Para mitigar esses riscos, é essencial que o Brasil invista em preparação, resiliência e resposta integrada. Estratégias-chave incluem a manutenção de Planos de Contingência para Emergências de Saúde Pública⁵⁵, o fortalecimento de sistemas de vigilância como os Centros de Informações Estratégicas em Vigilância em Saúde (CIEVS)⁵⁶, a ampliação da capacidade hospitalar e o investimento em pesquisa.

É importante, também, construir resiliência econômica e social, garantindo cadeias de suprimentos estratégicas. Durante a pandemia de Covid-19, por exemplo, países como Canadá, China, EUA, França e Israel usaram seus Serviços de Inteligência para garantir o acesso a suprimentos médicos essenciais⁵⁷.

No campo da segurança humana, os impactos são igualmente profundos e multifacetados. A ambivalência do papel do Brasil como país de trânsito e destino migratório, por exemplo, exigirá uma articulação complexa entre políticas de acolhimento e estratégias de segurança de fronteira para combater o tráfico de pessoas. A restrição de ingresso em países desenvolvidos tende a forta-

lecer a atuação de organizações criminosas transnacionais, que exploram rotas clandestinas na Amazônia e nas fronteiras com Guiana, Bolívia e Paraguai. Esse quadro eleva os riscos à soberania territorial e à segurança dos migrantes. As maiores facções criminosas do país já estão instaladas nessas fronteiras, diversificando suas atividades para além do tráfico de drogas e armas, incluindo garimpo, prostituição e extorsão⁵⁸. A intensificação dos fluxos migratórios pode favorecer a expansão dessas atividades ilegais, desafiando as instituições do Estado e aumentando o risco de corrupção de agentes públicos. Somente uma abordagem intersetorial e permanente permitirá transformar a complexa dinâmica demográfica em um ativo para a segurança e para a projeção regional do Brasil.

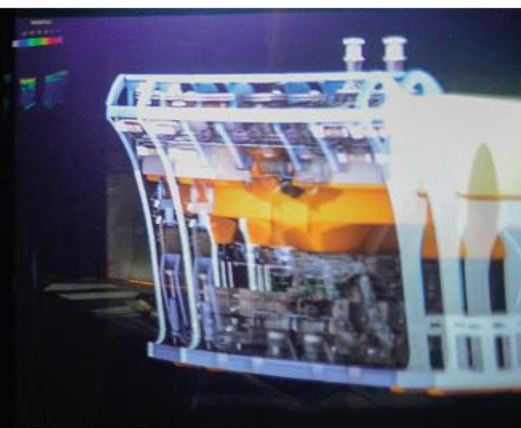


Tecnologia

A reconfiguração do poder global nas próximas décadas será impulsionada por um conjunto de tecnologias críticas que ultrapassa a digitalização convencional. Infraestrutura espacial, telecomunicações 5G e 6G, cibersegurança de ponta, computação quântica e inteligência artificial (IA) não apenas reordenam a economia, a Defesa e a Segurança em escala global, como exigem novos patamares de qualificação técnica e científica.

O espaço, ambiente antes dominado por governos, está sendo transformado pela economia emergente do New Space, marcada por inovação e investimentos privados nas áreas de lançamentos espaciais, veículos e comunicações⁵⁹. No setor de telecomunicações, as redes baseadas em satélites de órbitas baixa, média e geoestacionária (LEO, MEO, GEO) ampliaram, de forma significativa, a capacidade de cobertura global, em especial em regiões remotas e zonas pouco atendidas pelas infraestruturas tradicionais. O desenvolvimento dessas tecnologias também favoreceu a expansão das redes 5G e o avanço da tecnologia 6G, fundamentais para viabilizar, entre outros recursos, aplicações de inteligência artificial, Internet das Coisas (IoT), automação e cidades inteligentes.

UFRJ inaugura o supercomputador Lobo Carneiro, o mais potente instalado em uma universidade federal do país (2016)
| Foto: Tomaz Silva (Agência Brasil)



A crescente adoção de soluções tecnológicas baseadas em nuvem, juntamente com os avanços em computação quântica, tem incrementado o poder computacional das redes e ampliado a capacidade de processamento e análise de grandes volumes de dados, incluindo dados sensíveis. Essas tecnologias disruptivas trazem consigo desafios significativos para a cibersegurança. O desenvolvimento dos computadores quânticos tem potencial para quebrar métodos tradicionais de criptografia, como os algoritmos de chave pública atualmente utilizados para proteger comunicações e transações digitais. Países que não acompanharem os avanços em computação quântica tornar-se-ão vulneráveis a ataques cibernéticos

sofisticados, já que a capacidade desses sistemas de processar informações e de quebrar algoritmos de criptografia tradicionais representa uma ameaça significativa à segurança de dados sensíveis e à proteção de infraestruturas críticas⁶⁰.

A computação quântica ameaça a criptografia tradicional. A urgência da transição reside na tática adversária de “coletar agora, decifrar depois”, ameaçando a confidencialidade de longo prazo de segredos diplomáticos, militares e de Inteligência.

A Rodoviária de Brasília é o encontro dos Eixos Monumental e Rodoviário | Fabio Rodrigues-Pozzebom (Agência Brasil)





A tecnologia é um elemento crucial das dinâmicas interestatais contemporâneas, e a disputa pela supremacia tecnológica tem sido observada, sobretudo, na esfera da inteligência artificial. Com o avanço de modelos generativos e aplicações de aprendizagem de máquina, a IA está transformando cadeias de valor, impactando políticas de segurança, processos industriais, o controle de informações e a defesa cibernética. A acirrada competição pela liderança e inovação em tecnologias de ponta tende a intensificar pressões regulatórias e a fragmentar a governança global, sendo mais difícil chegar a consensos sobre ética, transparência e uso responsável e sustentável envolvendo as tecnologias emergentes e disruptivas.

Para os próprios serviços de Inteligência, a adoção de tecnologias disruptivas em seus processos, em especial a IA, é um desafio prioritário. Agências dos EUA, da Rússia e da China têm enviado esforços nesse sentido. A efetiva integração da IA com diferentes etapas da produção de Inteligência tem potencial para alterar significativamente processos de coleta, tratamento e análise de informações, com impactos relevantes para as decisões governamentais em áreas estratégicas. As barreiras, porém, são consideráveis, sobretudo tendo em vista o necessário processamento de dados sigilosos⁶¹.

No atual embate entre EUA e China pela liderança em IA, Washington tem explorado seu controle sobre o desenvolvimento de semicondutores e chips de alta tecnologia para tentar frear o avanço da IA chinesa⁶². Embora isso tenha gerado obstáculos, não impediu o progresso de empresas chinesas em desenvolver seus próprios grandes modelos de linguagem (LLMs)⁶³. Observa-se, portanto, que a competição tecnológica é uma arena central na geopolítica contemporânea, na qual o domínio de tecnologias críticas tende a se traduzir em poder e influência globais.

A criação de ecossistema local e nacional de inovação tecnológica exige a atuação estatal para assumir, financiar e coordenar os riscos inerentes ao desenvolvimento tecnológico, bem como para formar e atrair mão de obra especializada. No Brasil, existem setores avançados que conjugam inovação e produção, como a cadeia aeroespacial. A ampliação do uso de satélites para monitoramento territorial, previsão climática e segurança ambiental abre oportunidades de desenvolver tecnologias autônomas e de integrar cadeias globais de valor. O Brasil possui ativos relevantes que podem impulsionar a transformação digital de sua economia⁶⁴, contando com um ecossistema de inovação que interliga centros de pesquisa e de formação de capital humano. O país detém um dos poucos centros de inovação localizados no Sul Global (excetuando-se a China), com crescimento destacado. Em comparação internacional entre centros de inovação, São Paulo avançou da 86ª posição em 2023 para a 63ª em 2024⁶⁵.

A transformação digital oferece ganhos de eficiência para os Estados e conveniência para as pessoas. No entanto, para que esses benefícios sejam sustentáveis, os processos de transformação digital devem basear-se em decisões estratégicas que considerem os riscos e ameaças securitárias para a soberania nacional e a segurança da população. Nesse sentido, o desenvolvimento de estratégias de soberania digital por parte dos Estados é um imperativo para conquistar e preservar sua autonomia frente às empresas de serviços digitais, que monopolizam a extração de valor na forma de dados coletados das populações e mantidos sob sua custódia⁶⁶.

A soberania digital refere-se à capacidade de um país ou sociedade ter controle sobre seu próprio destino digital – os dados, *hardware* e *software* dos quais depende ou que são criados no país⁶⁷. Baseando-se nesse conceito e em seus correla-



tos – *cyber*soberania, soberania tecnológica e soberania de dados –, cresce a preocupação entre autoridades e formuladores de políticas públicas⁶⁸ quanto ao controle excessivo cedido a um pequeno número de empresas de tecnologia, que detêm vastas quantidades de dados sobre seus usuários e que concentram poder no mercado digital. Nota-se, além disso, que as empresas não buscam apenas lucrar com os dados coletados, mas também exercer poder, confrontando estruturas estatais e visando influenciar condutas governamentais, como exemplificado pelo comportamento da plataforma X no Brasil em 2024, que desrespeitou decisões do Poder Judiciário brasileiro, levando ao seu bloqueio⁶⁹.

A dependência estrutural em relação a corporações privadas, muitas vezes sob jurisdição estrangeira, representa um desafio significativo para a governança internacional e para a soberania digital, sobretudo do ponto de vista de países do Sul Global. A concentração de tecnologias e dados, especialmente com o estágio de desenvolvimento atual e a perspectiva de incremento da IA, redundam em enorme influência de empresas e governos estrangeiros sobre a opinião pública e na possibilidade de interferência em processos decisórios nacionais. Afinal, a opacidade das operações digitais torna pouco claros os limites entre os interesses das *big techs* e os interesses dos Estados onde estão sediadas.

A disputa tecnológica EUA-China define a Era Digital. A dependência estrutural do Brasil de hardware e software estrangeiros representa um risco severo à soberania digital, afetando a autonomia decisória, a Defesa e a Segurança do país.

O Brasil ainda enfrenta desafios significativos para garantir sua soberania digital, dependendo maciçamente de hardware estrangeiro, como unidades de processamento gráfico (*graphics processing units* – GPUs) e servidores⁷⁰. Ainda assim, o Brasil ocupa a 10ª posição no ranking global de distribuição de data centers, ficando atrás apenas da China entre os países do Sul Global⁷¹. A competição tecnológica entre grandes potências e entre entidades privadas com alcance global afeta a governança digital e impõe desafios à histórica neutralidade brasileira, a exemplo de restrições a fornecedores e de volatilidade nas cadeias de suprimento. Perante esse cenário, o Brasil pode adotar estratégias que combinem neutralidade ativa com autonomia tecnológica, gerenciando as dependências externas por meio da diversificação de fornecedores e de salvaguardas contratuais⁷².

A segurança cibernética é um pilar fundamental da segurança nacional na Era Digital. Os ataques cibernéticos contra infraestruturas críticas tornam-se cada vez mais sofisticados e frequentes, representando sérias ameaças a redes de telecomunicações, *data centers*, redes elétricas, sistemas satelitais e componentes essenciais do sistema financeiro nacional, como o sistema



A IA facilita a realização de ciberataques sofisticados contra infraestruturas críticas (Brasil sofreu 61 ataques em 2023). Apesar do risco, o país avançou, alcançando a 2ª posição em cibersegurança nas Américas, atingindo o estágio de modelo para os países da região (ITU 2024).

Pix. Tais ações têm potencial de comprometer a segurança do Brasil, desestabilizar a economia e prejudicar o funcionamento de serviços públicos essenciais, evidenciando a urgência de fortalecer mecanismos de proteção e resiliência digital nesses setores estratégicos.

O avanço de tecnologias conectadas (como IoT e 5G) aumenta a exposição a riscos, facilitando a ação de grupos criminosos. Em 2023, o Brasil sofreu 61 ciberataques que impactaram infraestruturas críticas, afetando distintos setores, como saúde, agricultura e tecnologia⁷³. A despeito desses problemas, nos últimos anos, o Brasil tem demonstrado uma evolução notável em cibersegurança. De acordo com a mais recente edição do Índice Global de Segurança Cibernética, divulgado pela União Internacional de Telecomunicações em 2024, o Brasil é o segundo país das Américas com a maior pontuação, ficando atrás apenas dos EUA,⁷⁴ e o primeiro da América do Sul (Gráfico 3).

Para que o Brasil siga ampliando sua resiliência digital, é imprescindível promover não apenas o aprimoramento da legislação nacional de cibersegurança, mas também aprofundar iniciativas de cooperação em múltiplos níveis. Isso envolve a integração de esforços entre diferentes órgãos

governamentais, setor privado e sociedade civil no âmbito nacional, criando políticas coordenadas, mecanismos de resposta rápida e compartilhamento de informações sobre ameaças cibernéticas.

No plano internacional, destaca-se a importância de participação ativa em fóruns multilaterais, desenvolvimento de acordos técnicos e legais com outros países e a adoção de padrões globais para proteção de redes. Esse enfoque colaborativo permite tanto a troca de boas práticas quanto a criação de estratégias conjuntas para enfrentar ameaças transnacionais, promovendo um ambiente digital mais seguro, inovador e confiável para todos os atores envolvidos.

O governo brasileiro tem se dedicado a ampliar a cooperação em âmbito multilateral na temática de cibersegurança. Os países do BRICS estão fortalecendo a cooperação em segurança cibernética, buscando uma resposta conjunta aos desafios digitais, aumentando a proteção contra ameaças cibernéticas e diminuindo a desigualdade tecnológica entre as nações parceiras⁷⁵.

As ameaças e as oportunidades da atual transição tecnológica relacionam-se intimamente com a distribuição de poder no sistema internacional. Nesse contexto, a dependência de infraestruturas e de serviços digitais estrangeiros expõe o Brasil a riscos significativos de interferência externa, controle de fluxos de informação e até mesmo sanções que podem paralisar serviços essenciais. Com o progressivo desenvolvimento da IA, as implicações da concentração das tecnologias e do controle sobre os dados são variadas e incluem influência de empresas e governos sobre a opinião pública, interferência sobre processos decisórios e utilização dessa tecnologia para fins militares e contrários à autodeterminação e soberania nacional.



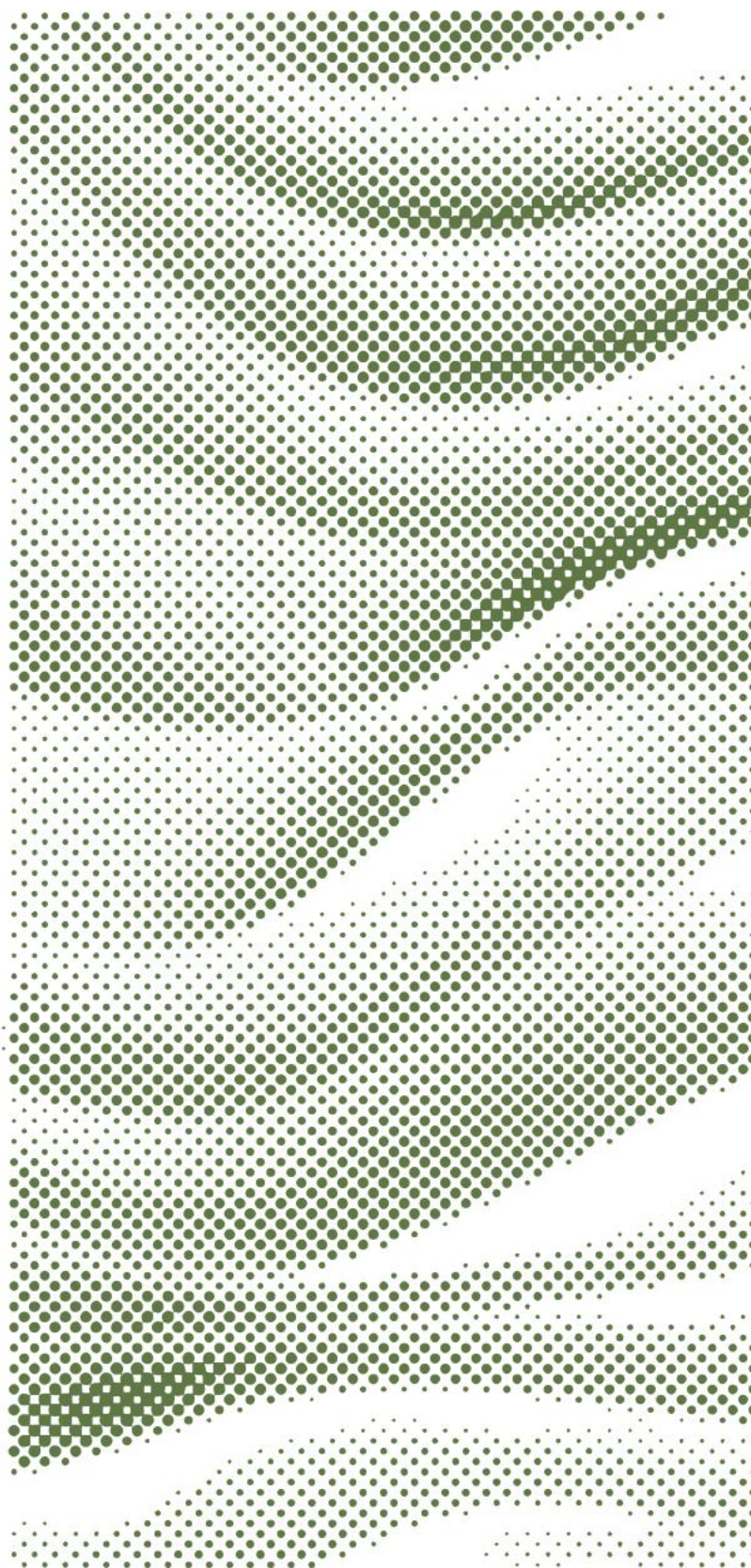
Gráfico 3 Cibersegurança na América do Sul, 2014-2024

Pontuação e posição dos países da América do Sul no Índice Global de Cibersegurança (GCI), índice normalizado



* A posição no ranking referente a 2024 foi inferida a partir da pontuação de cada país, devido a mudança na metodologia do relatório de 2024.

Fonte: International Telecommunication Union (ITU), "Global Cybersecurity Index (2014-2024)", <https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>; Banco Mundial, "Global Cybersecurity Index - Overall Score (ITU GCI)", https://data360.worldbank.org/en/indicator/ITU_GCI_GCI_OVRL_SCORE.





Situação Internacional

02

Centro espacial de Alcântara (CEA) no Maranhão | Foto:
Joédson Alves (Agência Brasil)



A ordem internacional é constituída por uma diversidade de atores que interagem entre si, pela forma como as capacidades e o poder estão distribuídos entre eles, e pelo conjunto de instituições formais e informais que estruturam tais interações. Os atores de maior peso são os Estados nacionais que detêm maiores capacidades combinadas, embora as dinâmicas próprias da Era Digital venham permitindo novas formas de concentração de riqueza e de poder por parte de corporações, de organizações não estatais e de indivíduos. As decisões estratégicas dos atores são condicionadas por essa ordem relacional, mas também pelo desenvolvimento dos processos globais de transição e pelas lógicas sociais, políticas e institucionais internas dos atores coletivos.

O sistema internacional atual pode ser descrito como uma multipolaridade desequilibrada e desinstitucionalizada. Embora múltiplos polos de poder tenham emergido nas últimas décadas, a distribuição de capacidades entre eles não é equilibrada, e as instituições formais e informais que deveriam induzir a cooperação encontram-se fra-

gilizadas⁷⁶. Esse cenário é marcado, fundamentalmente, pelo declínio da ordem liberal multilateral — consolidada após 1945 sob a liderança dos EUA —, que atravessa um acelerado processo de desestruturação. A competição estratégica entre as grandes potências, com destaque para os EUA e a China, está provocando redefinição sistêmi-



ca dessa ordem e das instituições de governança global, resultando em um cenário de crescentes incertezas e instabilidades.

O enfraquecimento de pilares da governança global como a Organização das Nações Unidas (ONU), a Organização Mundial do Comércio (OMC) e o Fundo Monetário Internacional (FMI) é uma evidência dessa transição. Tais organismos estão sendo progressivamente esvaziados por disputas internas, pela paralisia decisória imposta por potências que bloqueiam reformas institucionais e pela perda de legitimidade junto ao Sul Global. A recente expansão dos BRICs, com a adesão de cinco novos países em 2024 e 2025, evidencia esse processo. Além disso, governos de países do Norte Global têm reduzido suas contribuições a essas instituições⁷⁷, além de desacreditá-las⁷⁸. O resultado é uma erosão das normas e dos consensos que sustentaram a ordem internacional do pós-guerra, dando lugar à fragmentação da normatividade internacional, que se torna volátil e assimétrica⁷⁹. Presenciamos novas disputas entre grandes potências por zonas de influência política, militar, econômica e comercial⁸⁰, com a conversão da economia em ferramenta para subjugar países por meio de sanções, tarifas e pacotes financeiros⁸¹.

Para o Brasil, eleva-se o risco de pressões por alinhamento mais explícito na competição entre potências, ao mesmo tempo em que a crescente conflituosidade da situação internacional coloca em questão a relativa segurança e a estabilidade do país. A capacidade de manter boas relações com uma multiplicidade de atores e de assegurar longos períodos sem participar de conflitos armados internacionais promovem imagem pacifista do Brasil, o que potencializa a atratividade para investimentos e parcerias de longo prazo. Neste capítulo, serão analisados desdobramentos recentes do processo de transição de poder em nível

internacional sob os enfoques da competição entre potências e dos crescentes riscos de conflitos.

Competição

A intensificação do confronto entre grandes potências tem conduzido à militarização e à securitização progressivas de diferentes esferas de atividade, incluindo a tecnológica e a econômica. Setores como semicondutores, inteligência artificial, minerais críticos e energias de transição tornaram-se arenas de disputa, com o uso de sanções e controle de exportações exacerbando o desacoplamento de cadeias produtivas⁸².

No atual contexto internacional de multipolaridade desequilibrada, o Brasil deve estar preparado para cenários nos quais será pressionado a escolher posições mais firmes na disputa geoestratégica entre EUA e China. O principal risco pode vir da pressão de ambos os lados por uma aliança definida, o que colocaria em xeque a tradicional política externa brasileira de equilíbrio pragmático.

Mais especificamente, o aprofundamento das alianças Sul-Sul⁸³, a exemplo da recente expansão dos BRICS (em 2024, adesão de Egito, Etiópia, Irã e Emirados Árabes Unidos e, em 2025, adesão da Indonésia) pode impactar na deterioração das relações com os EUA, em domínios como cooperação tecnológica, canais diplomáticos e fluxos de investimento. Em particular, a atual administração estadunidense tem demonstrado reduzida tolerância à autonomia estratégica sul-americana, com condicionalidades políticas e constrangimentos indiretos em temas como governança digital⁸⁴. Recentemente, esses constrangimentos apresentam-se de forma mais direta, ameaçando os princípios do direito internacional⁸⁵, da soberania territorial e da autodeterminação política⁸⁶.

Uma das principais facetas do recrudescimento da disputa estratégica é o aumento dos gastos militares. Segundo dados do Instituto Internacio-

nal de Pesquisa para a Paz de Estocolmo (SIPRI)⁸⁷, em 2024 os gastos militares globais atingiram um recorde de US\$ 2,7 trilhões, um aumento de 9,4% em relação ao ano anterior e o maior valor já registrado desde 1988. Esse aumento ocorre em meio a sinais de novas corridas armamentistas nos domínios nuclear, balístico e espacial⁸⁸, além de discussões sobre os limites do emprego de inteligência artificial para fins militares⁸⁹. Estados

Unidos (37% do total mundial) e China (12%) responderam, somados, por cerca de metade de todo o gasto global em 2024.

Outro indicador da crescente insegurança internacional é o desmonte dos pilares da arquitetura de acordos que regulavam as relações entre as potências nucleares. Desde que os EUA se retiraram do Tratado sobre Mísseis Antibalísticos (ABM) em 2001, essa estrutura entrou em

Os gastos militares globais atingiram um recorde de US\$ 2,7 trilhões em 2024 (SIPRI). Quase metade desse valor (49%) foi concentrada por EUA e China, sinalizando a intensidade da nova competição estratégica.



Sala de controle de distribuição de energia elétrica da hidrelétrica de Itaipu Binacional em Foz do Iguaçu (PR) | Foto: Joédson Alves (Agência Brasil)



Reunião da Força-Tarefa para a Aliança Global contra a Fome e a Pobreza no Rio de Janeiro (RJ) | Foto: Tomaz Silva (Agência Brasil)

colapso. Em 2019, EUA e Rússia abandonaram o Tratado de Forças Nucleares de Alcance Intermediário (INF) e, em 2023, a Rússia suspendeu sua participação no tratado New START, que limitava os arsenais estratégicos dos dois países. O equilíbrio nuclear pactuado, crucial para manter a paz entre as grandes potências desde a década de 1970, ruiu, tornando-se o indicador mais claro de instabilidade global atualmente. Segundo dados do SIPRI⁹⁰, em janeiro de 2025, os nove países nucleares possuíam um total aproximado de 12.241 ogivas nucleares, com quase todas as potências modernizando ou expandindo seus arsenais.

O crescente antagonismo entre EUA e China aprofunda as consequências da instabilidade no cenário internacional e tem evoluído de uma competição por influência para um confronto estratégico mais amplo. Ambas as nações buscam alinhar os demais Estados aos seus interesses, mas

a lógica da rivalidade foi redefinida pela intensa securitização de temas econômicos, financeiros e, sobretudo, tecnológicos.

O equilíbrio nuclear pactuado, pilar da paz desde os anos 1970, ruiu. O desmonte de tratados cruciais (ABM, INF, New START), a manutenção de 12.241 ogivas pelos nove países nucleares e a modernização desses arsenais criam a fonte mais clara de instabilidade global.



Ano Novo chinês comemorado no bairro da Liberdade em São Paulo (SP) | Foto: Paulo Pinto (Agência Brasil)

Do ponto de vista estadunidense, essa nova fase se manifesta por meio de uma política de poder direto, em que o objetivo não é apenas competir, mas conter ativamente o avanço do adversário. A disputa por acesso a recursos e a mercados agora se dá no contexto de uma “guerra tecnológica” e de estratégias de *de-risking*⁹¹, que visam reorganizar as cadeias globais de valor e restringir o acesso chinês a tecnologias sensíveis.

Por outro lado, a resposta chinesa à contenção estratégica norte-americana tem-se materializado em esforços para exercer domínio sobre cadeias de suprimentos cruciais a setores de alta sensibilidade e relevância no cenário de competição entre as potências globais, como Defesa, energias renováveis, inteligência artificial e semicondutores. Destaca-se, nesse sentido, a recente imposição de controles sobre a exportação de terras raras e de tecnologias associadas à sua

extração e processamento⁹². Ao exigir licenças de exportação, atingindo o complexo industrial-militar estadunidense⁹³, o governo chinês não apenas responde às estratégias de *de-risking* ocidentais, mas também sinaliza sua capacidade e interesse político de mobilizar recursos de poder para obstruir ativamente o avanço tecnológico de nações adversárias.

Conflitos

O quadro de acirramento da disputa estratégica entre as potências globais tende a aumentar a chance e a gravidade de agressões militares e das guerras. De fato, no último ano, a ocorrência de conflitos armados seguiu em expansão, ampliando a tendência apontada pelo Instituto de Pesquisas de Paz de Oslo (*Peace Research Institute Oslo* – PRIO) desde 2021. No ano de 2024⁹⁴, o número de conflitos armados no mundo atingiu o maior



Aeronave KC-390 chega à Base Aérea de Brasília com brasileiros e estrangeiros provenientes da Ucrânia | Marcelo Camargo (Agência Brasil)

patamar desde 1946. Foram registrados 61 conflitos em 36 países, sendo a África o continente mais afetado.

Os efeitos da disputa estratégica entre as potências na reprodução e intensificação das dinâmicas conflitivas ao redor do globo podem ser mais bem observados no conflito russo-ucraniano e nas tensões no Oriente Médio. No primeiro caso, o teatro conflitivo da Ucrânia consolidou-se como uma exaustiva guerra de atrito para ambos os lados da disputa⁹⁵. A capacidade defensiva de Kiev tem dependido diretamente da continuidade do apoio militar de países da Organização do Tratado do Atlântico Norte (OTAN), cujo aporte principal em 2025 proveio não mais dos EUA, mas, sim, de seus parceiros europeus⁹⁶. No caso da Rússia, por outro lado, mostrou-se notável a capacidade de sustentar as operações militares contando com apoio mais limitado de seus parceiros e

aliados, a exemplo do Irã⁹⁷ e da Coreia do Norte⁹⁸ (apoio militar), bem como da China⁹⁹ (apoio econômico). A resiliência política e econômica da Rússia frente a pressões ocidentais também se manteve em 2025¹⁰⁰, apesar do emprego crescente de sanções¹⁰¹ e do avanço dos planos da União Europeia para alcançar independência energética em relação à Rússia¹⁰².

Paralelamente, a conjuntura securitária do Oriente Médio, agravada com a progressiva ampliação da escala de atuação militar israelense em territórios palestinos, tornou-se outro palco central da competição global. A grave crise humanitária e o risco de uma escalada regional — evidenciada por confrontos entre Israel e Líbano¹⁰³, Israel e Irã¹⁰⁴ e ataques israelenses a alvos do Hamas localizados em terceiros países¹⁰⁵ — causam impactos globais, com prejuízos à livre circulação de bens, serviços e pessoas.



Repatriados de Gaza chegam ao Brasil | Foto: Paulo Pinto (Agência Brasil)

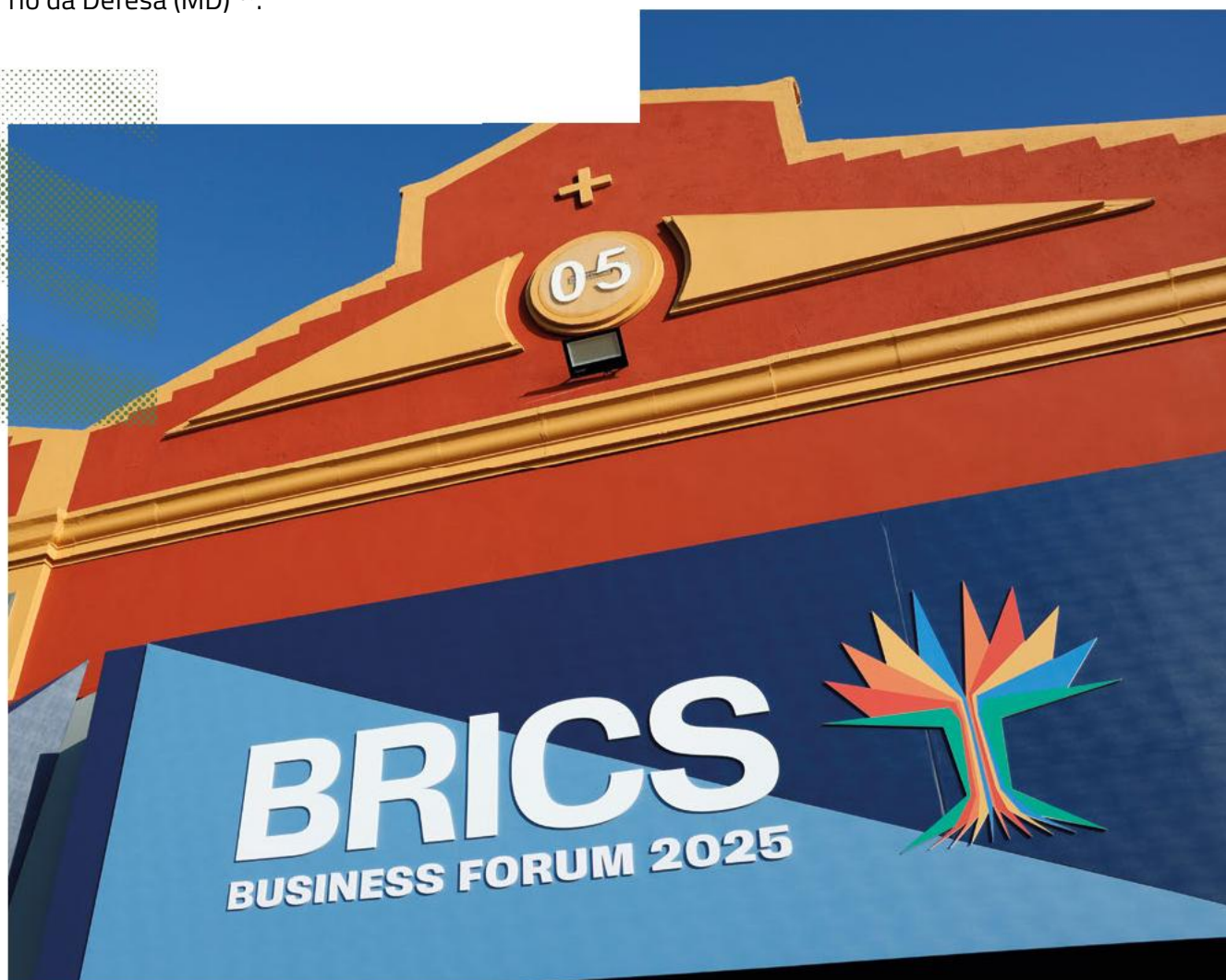
A dependência de tecnologias estrangeiras em telecomunicações, nuvem e sistemas de armamentos expõe a soberania brasileira a riscos de coerção e chantagem tecnológica, comprometendo a capacidade de comando e controle em cenários de crise.

Adicionalmente, surgem riscos transversais a serem monitorados pela Inteligência de Estado na atual conformação internacional, como a intensificação da guerra cognitiva com uso de inteligência artificial para desinformação, pressões financeiras extraterritoriais e a judicialização internacional de políticas públicas, especialmente nas áreas ambiental e de direitos humanos. Outro fator de risco reside nas assimetrias digitais: a digitalização crescente, combinada com a dependência tecnológica, expõe o Brasil a riscos de sabotagem, espionagem e coerção, além de ampliar vulnerabilidades diante de atores capazes de interromper serviços essenciais e manipular a opinião pública¹⁰⁶.

Para os setores de Defesa e Segurança, tais riscos e vulnerabilidades se manifestam de forma ainda mais crítica, comprometendo a soberania nacional. A dependência de sistemas estrangeiros

de comunicação, sensoriamento e armamentos expõe as Forças Armadas a riscos de interrupção e chantagem tecnológica, afetando a capacidade de comando e controle em cenários de crise. Ciente de tais desafios, o Governo do Brasil tem sinalizado um esforço renovado para reverter esse quadro. Observa-se uma articulação para adensar a Base Industrial de Defesa com investimentos estratégicos em ciência e tecnologia, por meio de iniciativas coordenadas entre a empresa Financiadora de Estudos e Projetos (Finep), o Ministério da Ciência, Tecnologia e Inovação (MCTI) e o Ministério da Defesa (MD)¹⁰⁷.

Em um mundo convulsionado por guerras (Ucrânia, Oriente Médio), a estabilidade geopolítica do Brasil emerge como um ativo singular para atrair investimentos, reforçado por sua posição pragmática como membro do BRICS e candidato à OCDE.



Rio de Janeiro (RJ), 05/07/2025 – Fórum Empresarial do Brics 2025, no Pier Mauá. Foto: Fernando Frazão (Agência Brasil)

Assim, apesar da conjuntura desfavorável, surgem oportunidades significativas para o Brasil. Em um mundo convulsionado por tensões e guerras, o país se destaca por seu histórico de paz e por sua tradição mediadora, que reduz o risco de confrontos armados diretos. Essa estabilidade é um fator favorável para atrair investimentos estrangeiros de empresas que buscam reduzir sua exposição a zonas de instabilidade. O país também tem conseguido manter boas relações diplomáticas com todos os atores globais relevantes, estando, juntamente com a Indonésia, entre os dois únicos membros dos BRICS que também são candidatos a ingressar na OCDE¹⁰⁸. Como membro do Mercosul, o Brasil encontra-se também em fase final de negociação de um acordo de livre comércio com a União Europeia¹⁰⁹.

Para melhor aproveitamento das oportunidades que despontam na atual conjuntura de incerteza sistêmica, o Brasil pode reforçar parcerias regionais autônomas com países amazônicos, atlânticos e africanos, com foco em segurança cooperativa e infraestrutura, e diversificar suas interlocuções no Sul Global, revalorizando mecanismos como o G20, BRICS+ e Fórum de Diálogo entre Índia, Brasil e África do Sul (IBAS). Outras oportunidades incluem a construção de capacidades nacionais em soberania digital, ciberdefesa e Inteligência para proteger dados estratégicos, e um redirecionamento das relações com países do Norte por meio da diplomacia científica, energética e climática, buscando acesso a tecnologias limpas, sem alinhamentos automáticos.

A complexidade do ambiente de segurança de 2026 demanda, portanto, um Estado com capacidade multidimensional, integrando Inteligência Estratégica, Defesa, Segurança, Política Externa e planejamento de longo prazo. As transformações em curso exigem um aparato de Inteligência estatal com alta capacidade de antecipação e de flexi-

bilidade adaptativa. Sem uma estratégia robusta para lidar com os riscos interdependentes no cenário internacional, o país pode se ver reduzido a espaço de disputa de influência entre as grandes potências, em vez de ser um ator com voz ativa na construção da nova ordem internacional.





América do Sul

03

Cataratas do Iguaçu, no Parque Nacional do Iguaçu em Foz do Iguaçu (PR) | Foto: Tânia Rêgo (Agência Brasil)



O entorno estratégico do Brasil é formado pela América do Sul, o Atlântico Sul, os países da costa ocidental africana e a Antártica. Nesta edição, foi mantido o foco no continente sul-americano, devido à premência das questões securitárias no entorno regional imediato que compreende as nações vizinhas.

É importante destacar algumas considerações introdutórias sobre a frente atlântica. Mais da metade da população brasileira vive a até 150 km do litoral¹¹⁰. Em termos econômicos, 97,6% da extração de petróleo e 85,3% da extração de gás natural¹¹¹, além de 80% do comércio internacional¹¹² do Brasil dependem do mar. Do outro lado do Oceano, os países do continente africano, inclusive os de língua portuguesa, oferecem oportunidades de cooperação e de comércio, além de cultivarem vínculos históricos e culturais com o Brasil. Os países africanos voltados para o Atlântico correspondem a 46% da população, 55% do PIB e 57% do comércio continental¹¹³. Além disso,

as atuais projeções populacionais estimam que, em 2050, mais de um quarto da população mundial residirá na África e que, em 2100, a Nigéria será o quarto país do mundo em população, atingindo mais de 470 milhões de habitantes¹¹⁴.

Na América do Sul, o Brasil tem 16,9 mil quilômetros de fronteiras terrestres, que abrangem 588 municípios e o conectam a 10 nações vizinhas. Cerca de metade da população, do PIB e do território da América do Sul pertencem ao Brasil¹¹⁵. Por volta de 60% do bioma amazônico localiza-se no Brasil, e esse bioma recobre 40% da área total da América do Sul. Nesse espaço compartilhado, relações econômicas, políticas, sociais e culturais de



caráter histórico constituem vínculos profundos, consagrados no objetivo constitucional do Brasil de buscar a integração da América Latina e em iniciativas concretas, tais como o Mercado Comum do Sul (Mercosul), a União de Nações Sul-Americanas (Unasul) e a Comunidade dos Estados Latino-Americanos e Caribenhos (Celac).

No entorno estratégico brasileiro, não há países que possam ser considerados hostis, mas a presença de grandes potências extrarregionais manifesta-se na forma de interesses políticos, militares, territoriais, comerciais e financeiros. Historicamente, a América do Sul goza de relativa estabilidade em relação a conflitos interestatais, e os riscos de confrontos entre Estados sul-americanos continuam sendo considerados pouco prováveis, embora a recente escalada de tensões entre a Venezuela e a Guiana no contencioso envolvendo a região de Essequibo continue merecendo atenção especial de autoridades sul-americanas.

A América do Sul, anteriormente uma área marginal nas disputas sistêmicas globais, está sendo progressivamente inserida como território de interesse geopolítico no contexto da crescente rivalidade entre os EUA e a China¹¹⁶. Na medida em que, isolados, os países sul-americanos mantêm relações profundamente assimétricas com os principais polos de poder globais, avanços na integração tendem a proporcionar posições conjuntas mais estáveis e vantajosas para o Brasil e para seus vizinhos. Neste capítulo, serão analisados riscos para a América do Sul considerando aspectos de segurança e o desafio da integração regional.

Segurança

A América do Sul está inserida na competição entre potências de maneira assimétrica e pouco coordenada, gerando impactos diretos sobre a soberania, a estabilidade regional e a autonomia estratégica dos Estados nacionais sul-americanos¹¹⁷. A intensificação da competição entre as grandes potências afeta a estabilidade regional, com disputas tecnológicas e comerciais se projetando sobre as políticas públicas domésticas, especialmente em áreas como transição energética e infraestrutura digital¹¹⁸.

Nesse cenário, aumenta a pressão por alinhamentos explícitos em detrimento de posturas autônomas ou equidistantes, e amplia-se a margem de ação de atores extrarregionais em zonas críticas como a região amazônica, a tríplice fronteira entre Argentina, Brasil e Paraguai, o Atlântico Sul e o Caribe. Especialmente preocupante tem sido o crescente emprego de instrumentos de poder convencionais e não convencionais para exercer pressão contra os países sul-americanos, caracterizando uma escalada no espectro conflitivo híbrido, em cujo extremo se encontra a agressão militar.

Com a competição estratégica avançando abertamente, observa-se uma luta crescente pela ampliação de alianças, em que vulnerabilidades econômicas e de segurança dos países sul-americanos podem ser exploradas por potências extrarregionais. Porém, as disputas também abrem oportunidades, como demonstrado pelos recentes investimentos externos no Brasil para a criação de polo de produção de veículos elétricos¹¹⁹.

Os interesses das grandes potências podem ser resumidos em dois conjuntos conectados: os políticos e os econômicos. Na dimensão política, os principais riscos decorrem de tentativas de projeção de poder, mediante ações que envolvam interferência nos assuntos internos e nas rela-



Cerimônia de geração de mídia e preparação das urnas eletrônicas para as eleições municipais de 2024 em São Paulo (SP) | Foto: Rovena Rosa (Agência Brasil)

ções intrarregionais; estabelecimento de presença militar; expansão extraterritorial da jurisdição legal, a exemplo do uso de *lawfare*; e securitização de temas sociais e políticos, como terrorismo, narcotráfico e imigração. Na dimensão econômica, por sua vez, os interesses envolvem o controle de recursos naturais, incluindo recursos energéticos e produção de alimentos, e o incremento de posições comerciais e financeiras, englobando influência sobre rotas comerciais e compra de ativos nacionais ou estatais estratégicos.

Com uma população superior a 430 milhões de habitantes e um PIB de mais de US\$ 4 trilhões, a

América do Sul tem peso relevante na demanda e na oferta de bens e serviços. A China consolidou-se como principal parceiro comercial do Mercosul em 2019, ultrapassando os EUA¹²⁰. Em 2024, o comércio entre a China e os países da América Latina e do Caribe ultrapassou, pela primeira vez, a marca de US\$ 500 bilhões¹²¹. Para além do comércio, os investimentos em infraestrutura logística, elétrica e em outras áreas estratégicas são vastos. A presença econômica dessas potências pode tanto estimular o desenvolvimento quanto criar dependências que impactam a soberania dos países sul-americanos e a integração econômica regional.

A região possui reservas estratégicas para as transições globais, incluindo algumas das maiores reservas de lítio (Bolívia, Argentina, Chile), petróleo (Venezuela, Brasil) e terras raras (Brasil). A competição por esses ativos eleva o risco de interferência.

A América do Sul é uma região produtora de commodities e possui reservas de recursos naturais cobiçados, como terras férteis, minérios estratégicos para o novo paradigma energético e a produção de armamentos, água, biodiversidade e a maior floresta tropical do mundo. Em 2024, as reservas provadas de petróleo no Brasil tiveram um aumento de 5,92%, atingindo mais de 16 bilhões de barris¹²², enquanto a Venezuela continua a ser o maior detentor global, com cerca de 19,3% do total de reservas¹²³.

A quantidade de recursos mundiais de lítio (Gráfico 4) é estimada em cerca de 105 milhões de toneladas, sendo a Bolívia o país com a maior quantidade conhecida (23 milhões de toneladas), seguida por Argentina (22 milhões) e Chile (11 milhões)¹²⁴. Além disso, o Brasil conta com a maior quantidade de terras raras da América do Sul e está entre os cinco maiores detentores do mundo, com aproximadamente 21 milhões de toneladas (Gráfico 5)¹²⁵. Contudo, a crescente concentração do refino e da separação de terras raras em poucos países aumenta a vulnerabilidade dos países da região a choques externos e práticas de dependência tecnológica.

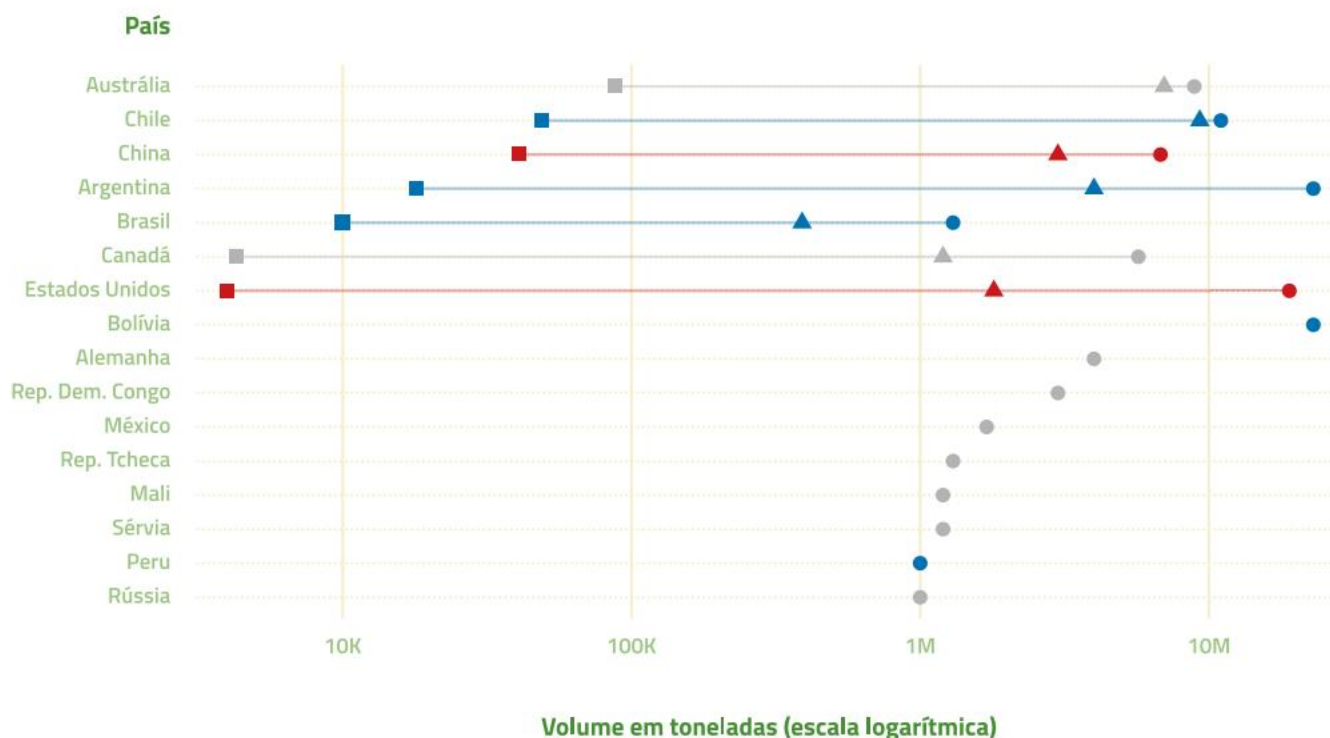
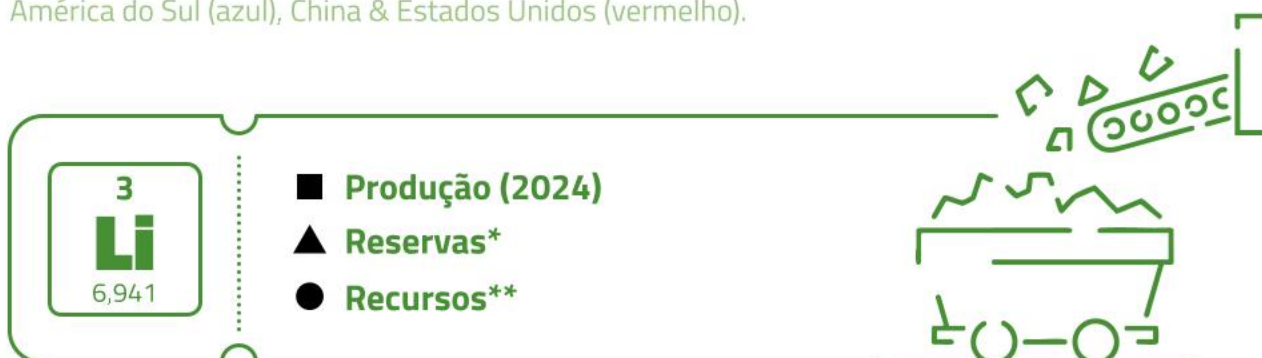


Passagem conhecida como Avenida Brasil no navio-plataforma P-71 no pré-sal da Bacia de Santos, a 200 km da costa do Rio de Janeiro (RJ) | Foto:Tânia Rêgo (Agência Brasil)



Gráfico 4 Produção, reservas e recursos de lítio

Países ordenados pela produção de 2024. Destaque para América do Sul (azul), China & Estados Unidos (vermelho).



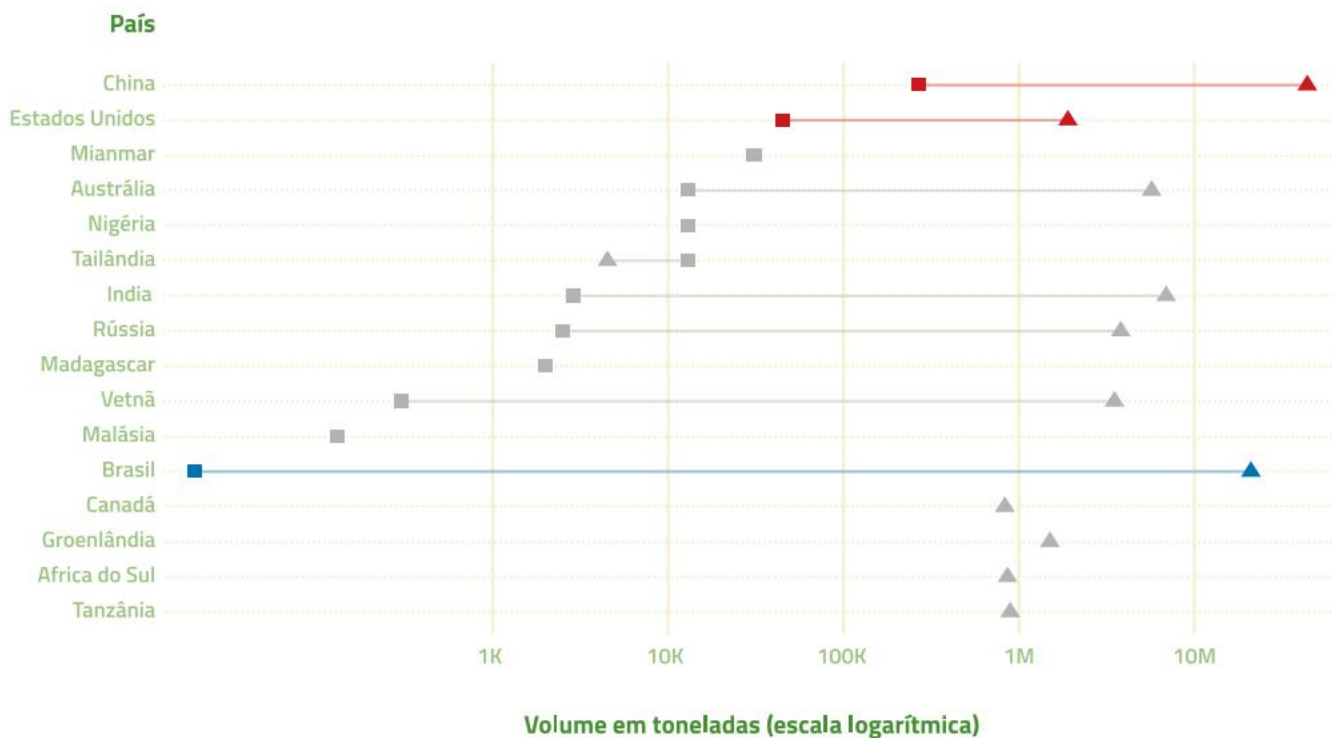
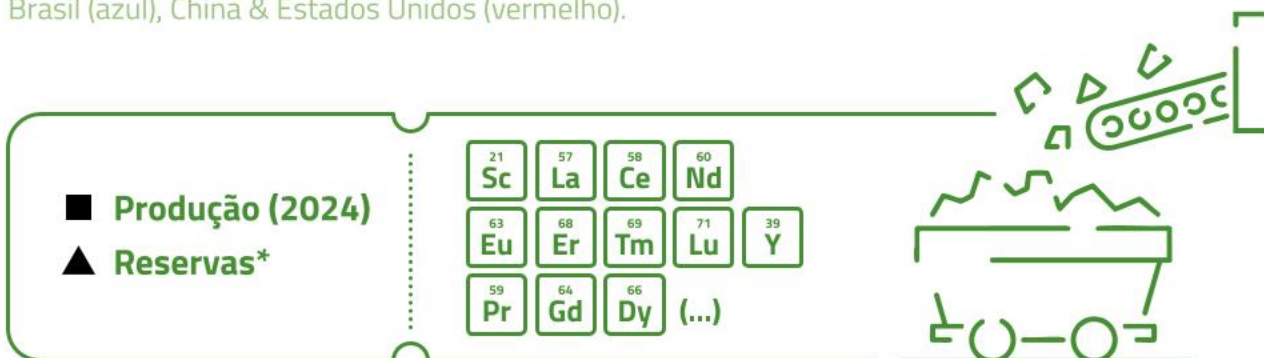
* Reservas: porção dos recursos minerais que é economicamente viável para extração no momento da avaliação, ainda que as minas ou instalações necessárias não estejam em funcionamento. ** Recursos: concentração de material natural (sólido, líquido ou gasoso) na crosta da Terra que é economicamente viável para extração, seja no presente ou potencialmente no futuro.

Fonte dos dados: United States Geological Survey (USGS), "Lithium," Mineral Commodity Summaries 2025; Michael Plante e Isabelle Tseng, "Rush for U.S. lithium production encounters tough economics," Federal Reserve Bank of Dallas, 14 de outubro de 2025, <https://www.dallasfed.org/research/economics/2025/1014-plant-tseng-lithium#:~:text=U.S.%20production%20set%20to%20increase,to%20start%20production%20in%202026>.



Gráfico 5 Produção e reservas de terras raras

Países ordenados pela produção de 2024. Destaque para Brasil (azul), China & Estados Unidos (vermelho).



* Reservas: porção dos recursos minerais que é economicamente viável para extração no momento da avaliação, ainda que as minas ou instalações necessárias não estejam em funcionamento.

Fonte dos dados: United States Geological Survey (USGS), "Rare earths," Mineral Commodity Summaries 2025.



Vista da aldeia Beira Rio, Terra Indígena Erikpatsa, do Povo Rikbaktsa em Brasnorte (MT). Foto: Fernando Frazão (Agência Brasil)

A região sul-americana também detém reservas compartilhadas de recursos estratégicos, porém a expansão da mineração nas novas fronteiras de exploração demanda atenção às dimensões socioambientais e de governança. O monitoramento de ilícitos ambientais, atividades garimpeiras irregulares e fluxos financeiros vinculados ao crime organizado constitui parte essencial da atuação da Inteligência estatal para assegurar a legitimidade das políticas minerais e a sustentabilidade territorial. O desafio consiste em articular segurança, desenvolvimento e inclusão, consolidando um modelo nacional que una soberania e responsabilidade ambiental.



1ª Conferência Nacional das Mulheres Indígenas em Brasília (DF) | Foto: Marcelo Camargo (Agência Brasil)



Nesse aspecto, cabe destacar a atuação de diversos órgãos de Inteligência¹²⁶ em recentes operações de desintrusão de Terras Indígenas (TIs) na Amazônia brasileira. As ações atenderam a determinações do Supremo Tribunal Federal (STF) exaradas no âmbito da Ação de Descumprimento de Preceito Fundamental (ADPF) nº 709, de 2020. Foram feitas desintrusões nas TIs Apyterewa, Trincheira Bacajá, Karipuna, Munduruku e Sai Cinza, Kayapó, Araribóia, Yanomami e Uru-Eu-Wau-Wau. Em setembro de 2025, o STF encerrou o julgamento da Ação, reconhecendo o cumprimento, por parte do governo brasileiro, das metas de proteção a TIs e de combate às atividades ilícitas¹²⁷.

Além da ocorrência de recursos minerais em seus solo e subsolo, a Região Amazônica também abarca a maior bacia hidrográfica do mundo, e o Aquífero Guarani, compartilhado por Brasil, Argentina, Paraguai e Uruguai, constitui uma das mais importantes reservas subterrâneas de água do planeta¹²⁸. A preservação da Amazônia brasileira, que representa cerca de 60% do território do Brasil, é vital não apenas para a biodiversidade global, mas também para a segurança nacional, devido a sua relevância geoestratégica.

Do ponto de vista securitário, a Inteligência de Estado deve estar atenta ao risco de militarização indireta de zonas sensíveis sob o pretexto da proteção de “bens comuns globais”, com o risco de instrumentalização da segurança ambiental para legitimar intervenções não solicitadas sobre zonas estratégicas.

A crescente inserção da região no cenário geoestratégico global potencializa a instrumentalização de desafios crônicos sul-americanos, a exemplo da expansão dos mercados ilícitos. Nesse sentido, alguns dos principais dilemas da região estão ligados à limitada capacidade de resposta das instituições diante de ameaças não estatais,

Potências extrarregionais exploram pretextos como o combate ao “narcoterrorismo” para justificar interferências, militarizar zonas sensíveis e minar a soberania e a autodeterminação política dos países sul-americanos.

como a ascensão do crime organizado e de grupos paraestatais armados, mantendo-se níveis elevados de violência interpessoal¹²⁹. O crime organizado transnacional é um dos maiores riscos, podendo abrir portas para a interferência de grandes potências sob pretextos de segurança, com base em narrativas como o “narcoterrorismo”¹³⁰.

Com efeito, o crime organizado transnacional deve ser tratado como grave problema de segurança pública regional, enraizado na capilaridade das economias ilícitas (drogas, armas, mineração ilegal, tráfico de pessoas, dentre outros ilícitos), cujos operadores exploram a porosidade territorial fronteiriça e as assimetrias institucionais existentes entre países vizinhos¹³¹.

No plano doméstico, a dinâmica interinstitucional e interagências adquire papel fundamental. O enfrentamento do crime transnacional com impacto direto em segurança pública não pode ser compreendido apenas sob a lógica da repressão policial, mas como uma estratégia integrada de governança da segurança, necessitando de canais formais de inteligência no âmbito do Sisin e do Subsistema de Inteligência de Segurança Pública (Sisp), e articulação entre os principais setores. Em termos de colaboração internacional, é imprescindível investir no aperfeiçoamento da



Ibama faz a soltura de araras e papagaios na Reserva ecológica Chapada Imperial em Brasília (DF) | Foto: Marcelo Camargo (Agência Brasil)

governança regional em matéria de segurança. O Brasil e seus vizinhos, que enfrentam os riscos associados à expansão e consolidação dos mercados ilícitos, devem se coordenar no combate a tais ameaças, evitando o protagonismo de potências extrarregionais e a instrumentalização da agenda de segurança pública nos espaços compartilhados da América do Sul.

Integração

O Brasil é uma potência regional com capacidades de nível médio e limitações à projeção de poder nos domínios convencional, espacial e nuclear. Assim como o Brasil, os demais países de seu entorno estratégico não dispõem de capacidades determinantes de dissuasão contra a atuação das grandes potências. Ademais, tanto na América do Sul quanto no Atlântico Sul e territórios adjacentes, o interesse nacional corresponde aos anseios de paz e de desenvolvimento sustentável, compartilhados pelos demais países. Na América do Sul, em especial, a existência de profundos vínculos históricos constitui o fundamento para iniciativas de integração que tendem a fortalecer a posição dos países da região frente às pressões externas no atual cenário de competição internacional.

A presente situação, no entanto, é paradoxal para o Brasil: enquanto sua política externa retomou projeção no cenário internacional, com destaque para a atuação junto aos BRICS e ao G20, bem como a organização da COP30, sua influência no entorno estratégico imediato não tem sido recuperada na mesma proporção. Na América do Sul, verifica-se o enfraquecimento dos projetos multilaterais, o que conduz a uma situação de mera convivência em vez de efetiva cooperação¹³². Nessas condições, a capacidade de influência brasileira, no sentido de promover o desenvolvimento sustentável, a cooperação e o multilateralismo, preservando a região como zona de paz, encontra-se limitada.

A estratégia de integração regional, essencial para a segurança e a proeminência das nações sul-americanas, foi retomada a partir de 2023, com uma série de iniciativas que visavam restaurar o diálogo e a cooperação no subcontinente. Quatro movimentos-chave ilustram essa mudança de rota: o retorno do Brasil à União de Nações Sul-Americanas (Unasul)¹³³ e à Comunidade de Estados Latino-Americanos e Caribenhos (Celac)¹³⁴; e as reuniões de líderes de países sul-americanos e amazônicos que resultaram no Consenso de Brasília¹³⁵ e na Declaração de Belém¹³⁶, respectivamente.



Entretanto, as iniciativas capitaneadas pelo governo brasileiro têm encontrado obstáculos significativos para avançar. Dentre as dificuldades, estão as prioridades distintas e a ascensão de forças políticas em países vizinhos com projetos divergentes daqueles que pautam a política externa brasileira. Essa realidade cria um cenário complexo para a consolidação de uma agenda sul-americana comum.

A agenda de integração de infraestruturas logísticas, todavia, tem-se mostrado a principal faceta positiva e o vetor mais resiliente da cooperação no subcontinente¹³⁷. Após o encontro que resultou no Consenso de Brasília e, posteriormente, em outubro de 2023, no Mapa do Caminho para a Integração da América do Sul¹³⁸, projetos de integração da infraestrutura e logística regionais ganharam corpo e mantiveram-se ativos mesmo durante momentos de relativa paralisia na coordenação política entre os países envolvidos. Destaca-se, nesse sentido, o Corredor Rodoviário Bioceânico que ligará portos brasileiros no Atlântico aos portos do norte do Chile, no Pacífico, adensando a interligação entre as duas frentes do entorno estratégico brasileiro¹³⁹.

A necessidade e os benefícios do desenvolvimento de infraestrutura integrada são compartilhados por todos os países sul-americanos, como aponta o fraco desempenho geral da região no Índice de Performance Logística do Banco Mundial. O desempenho médio do subcontinente (2,77) se encontra consideravelmente abaixo da média mundial (3), numa escala de 5 pontos (Gráficos 6 e 7)¹⁴⁰. A pontuação do Brasil em 2023 era um pouco superior à média, atingindo 3,2 pontos.

Para além do próprio mérito de impulsionar a integração no subcontinente e viabilizar a ampliação do comércio intrarregional sul-americano – cujos números encontram-se muito aquém do que se verifica em outras regiões do globo –, a

O Brasil enfrenta um paradoxo: enquanto retoma sua projeção global (BRICS, G20), sua influência regional imediata encontra sérias limitações. Dissonâncias políticas com vizinhos dificultam a retomada de projetos multilaterais como a Unasul.

Diante da paralisia na cooperação política, a integração de infraestrutura surge como o vetor mais resiliente, oferecendo segurança econômica e rotas alternativas frente a pressões externas, como as tarifas impostas pelos EUA.

promoção da integração da infraestrutura física e logística sul-americana também impulsiona alternativas à segurança econômica nacional. Com efeito, o fomento a rotas adicionais para o escoamento do comércio exterior brasileiro no subcontinente tem potencial para fornecer alternativas em situações nas quais empresas brasileiras se vejam instadas a buscar novos clientes e mercados por motivos de força maior, a exemplo da situação em que o Brasil se encontrou perante a imposição unilateral de tarifas comerciais pelo governo dos EUA (tarifa geral de 10% em abril, elevada para 50% em agosto de 2025)¹⁴¹.



Gráfico 6 Performance Logística Global (LPI 2023)

Cada país é colorido de acordo com sua pontuação no Logistics Performance Index.

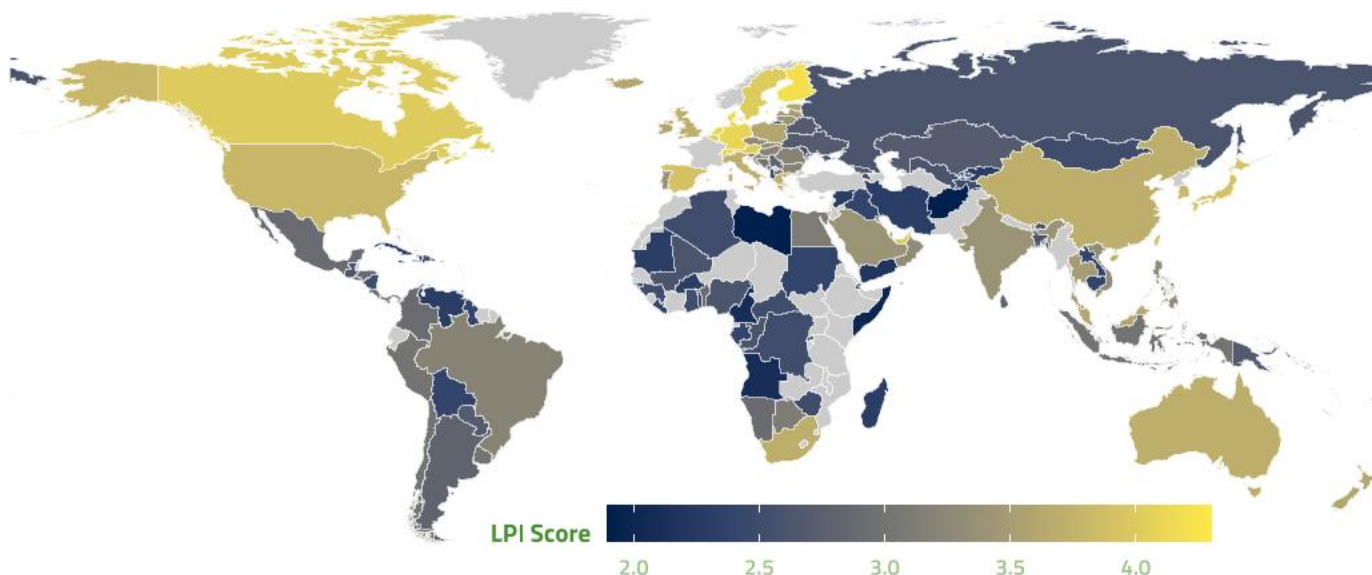
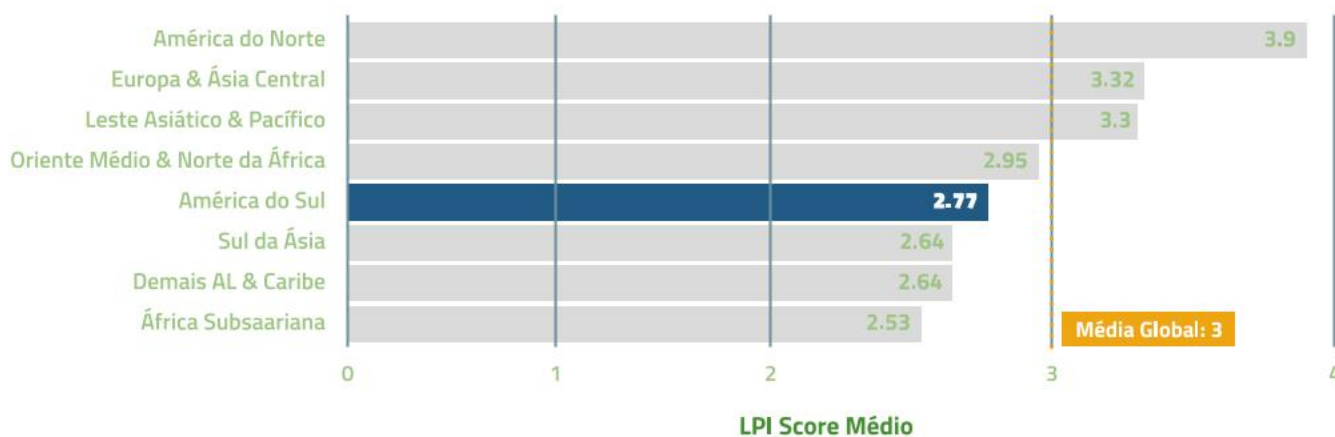
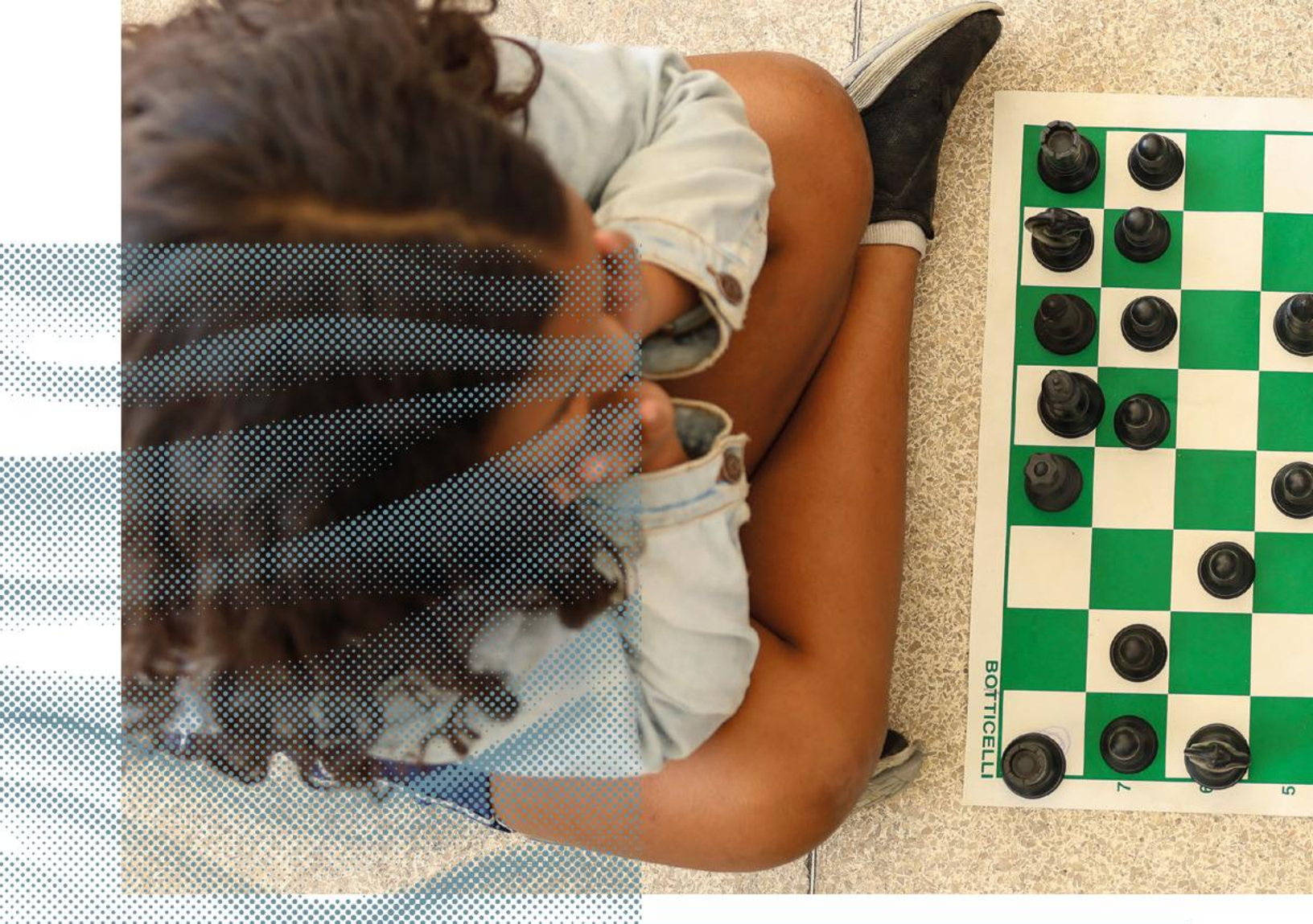


Gráfico 7 Média do LPI Score por Região

Comparação regional, com destaque para a América do Sul.



Fonte: Banco Mundial, Logistics Performance Index (LPI) 2023. Utiliza classificação regional da ONU, adaptada.



Brasil: desafios para a inteligência

04

Alunos jogam xadrez no Ginásio Experimental
Olímpico Reverendo Martin Luther King no Rio de
Janeiro (RJ) | Foto: Tomaz Silva (Agência Brasil)



A ABIN tem duas atribuições principais. Uma é coordenar e facilitar a integração entre os órgãos que compõem o Sistema Brasileiro de Inteligência (Sisbin). A outra é assessorar o Presidente da República e os ministérios sobre fatos e situações que possam impactar a segurança da sociedade e do Estado brasileiros.

Os fatos e as situações a serem acompanhados pela Agência são definidos por diretrizes legais. Para assessorar de forma assertiva, contando com o trabalho coordenado do Sisbin, é preciso definir enfoques e prioridades. Esta edição atualiza a avaliação sobre os desafios de Inteligência prioritários em 2026, para os quais será necessário informar as autoridades competentes sobre riscos e alternativas de mitigação.

A atualização, todavia, não implica que os desafios apontados no ano anterior deixaram de ter relevância. Pelo contrário, o aprofundamento das análises evidencia sua persistência e transversalidade, como é o caso do enfrentamento dos merca-

dos ilícitos e do crime organizado, tema destacado na edição passada. Os acontecimentos do fim de 2025 confirmam os riscos apontados na edição anterior e evidenciam o papel central da Inteligência para o enfrentamento do crime organizado.

As análises a seguir foram elaboradas por equipes de especialistas da ABIN, sob coordenação da Escola de Inteligência. Elas sintetizam aspectos não sigilosos dos desafios prioritários para 2026 e convidam diferentes públicos — pesquisadores, estudantes, servidores, trabalhadores, movimentos sociais, imprensa e cidadãos — a refletir e dialogar sobre a atuação, as capacidades e as perspectivas da Inteligência de Estado brasileira.



Segurança do processo eleitoral de 2026

O Brasil tem enfrentado desafios relacionados à manutenção da democracia e à estabilidade institucional. Desde 2018, observa-se a propagação recorrente, principalmente por meio de plataformas digitais, de desinformação acerca das eleições brasileiras. Tal processo resultou em mobilizações que questionavam o processo eleitoral nacional, as quais culminaram na invasão aos prédios dos Três Poderes, em Brasília, em 8 de janeiro de 2023.

Diante desse panorama, o processo eleitoral de 2026 ocorrerá em meio a desafios tanto para a sociedade quanto para a Atividade de Inteligência, demandando atuação integrada entre diferentes órgãos de Inteligência e capacidade de antecipação e resposta do Estado frente a ameaças multifacetadas. Essas ameaças incluem ações de deslegitimação do modelo eleitoral, campanhas de desinformação (com manipulação por meio de ferramentas tecnológicas), ações de interferência externa e aprofundamento da polarização social (com instrumentalização político-eleitoral de diversos segmentos da população), além da atuação do crime organizado e de potenciais ações de extremismo violento.

Deslegitimação do processo eleitoral

A deslegitimação sistêmica das instituições democráticas constitui um dos principais fatores de vulnerabilidade para as eleições de 2026. Trata-se de processo corrosivo, que mina a confiança e a percepção de legitimidade do eleitorado em relação às bases do regime republicano — o Poder Judiciário (com destaque para a Justiça Eleitoral), o Poder Legislativo e a capacidade de o Poder Executivo assegurar direitos e liberdades das pessoas nesse contexto.

As instituições passam, assim, a ser percebidas, por parte da população, como parciais e pou-



co confiáveis, o que compromete sua credibilidade. Campanhas orquestradas de desinformação atacam a segurança do sistema de votação e a lisura da apuração, contaminando a aceitação dos resultados e fomentando narrativas de vulnerabilidade das urnas e de fraude no resultado eleitoral. Frequentemente desenvolvidas com antecedência e ativadas em momentos oportunos, essas campanhas visam a influenciar a livre escolha do eleitor e desacreditar o voto como expressão da soberania popular.

A estabilidade institucional é condição essencial para a plena confiança pública no processo eleitoral. A segurança do escrutínio, dos sistemas de votação, sua inviolabilidade, a previsibilidade das normas e a percepção de sua aplicação isonômica são pressupostos fundamentais para que eleitores, sociedade e atores políticos aceitem os resultados da disputa eleitoral. A erosão dessa confiança abre espaço para narrativas de ruptura e de contestação, inclusive violenta, como as que emergiram após o pleito de 2022 e que permanecem latentes.

Desinformação e manipulação tecnológica

A desinformação constitui elemento central da deslegitimação do processo eleitoral, sobretudo em ambientes digitais, agravada pela manipulação tecnológica decorrente de recentes inovações informacionais.

A tecnologia tornou-se componente essencial da democracia contemporânea. O inegável potencial benéfico para o desenvolvimento econômico e social contrasta com sua conversão em ferramenta de manipulação e de desinformação. No contexto político-eleitoral, essa situação representa uma tendência de alto impacto para 2026.

As plataformas de redes sociais e de aplicativos de mensageria são hoje instrumentos fundamentais de produção e de difusão de informações.

Por suas características, porém, tornaram-se também meios privilegiados para disseminação de desinformação, discursos de ódio e teorias conspiratórias. A estrutura de seus algoritmos, desenhada para maximizar o engajamento, fomenta “bolhas informacionais” e câmaras de eco, nas quais os usuários são expostos predominantemente a conteúdos que reforçam seus vieses e suas crenças preexistentes, aprofundando a segmentação e a polarização.

Para o processo eleitoral de 2026, o desafio amplifica-se com o advento e o uso de novas tecnologias, notadamente a Inteligência Artificial (IA) generativa e os *deepfakes*. A capacidade de produzir, em larga escala, conteúdos audiovisuais sintéticos e hiper-realistas, com baixo custo e sem necessidade de habilidades técnicas avançadas, inaugura uma nova era de desinformação e de manipulação política.

A utilização de *deepfakes* tem potencial para forjar declarações de candidatos, descontextualizar falas ou simular discursos inexistentes de forma extremamente convincente. Trata-se de ferramenta de grande potencial disruptivo, capaz de desequilibrar a disputa eleitoral e destruir reputações em tempo quase imediato. A velocidade de criação e de disseminação de tais conteúdos supera a capacidade de verificação e de apresentação da verdade seja pelos candidatos, imprensa profissional ou autoridades, tornando inevitável a contaminação do debate público.

A eficácia de ações regulatórias destinadas a coibir o uso indevido dessas tecnologias disruptivas, antes ou durante o período eleitoral, permanece incerta. A natureza difusa da criação e da circulação desses conteúdos, somada à resistência de conglomerados tecnológicos à regulação estatal e à proteção oferecida por fronteiras jurisdicionais, dificulta a atuação das instituições e a aplicação de normas efetivas.



Criminalidade organizada e interferência externa

Dois fatores adicionais apresentam potencial de riscos relevantes à segurança da democracia e à integridade do processo eleitoral em 2026: a criminalidade organizada e a interferência externa.

A crescente simbiose entre a criminalização da política e a politização do crime evidencia a capacidade de milícias e de facções de influenciar o processo eleitoral. Em áreas periféricas e de baixa presença estatal, grupos criminosos exercem poder paralelo, controlando a vida de comunidades e, consequentemente, o voto. Essa influência manifesta-se tanto em ações de financiamento de campanhas quanto em ações de coação de eleitores e indicação de candidatos próprios, chegando, em casos extremos, a eliminação de adversários políticos. A penetração da criminalidade na política descaracteriza a representação democrática e ameaça as instituições, corrompendo-as por dentro.

Paralelamente, a possibilidade de interferência externa no processo eleitoral brasileiro é fator de risco que não pode ser subestimado. Atores estatais ou não estatais podem ter altos incentivos para promover ações de desestabilização do processo eleitoral, minando a confiança nas instituições, influenciando resultados e favorecendo interesses geopolíticos e econômicos próprios. Essa interferência pode ocorrer por meio de campanhas de desinformação sofisticadas, ataques cibernéticos à infraestrutura eleitoral ou via financiamento oculto de grupos políticos específicos e de movimentos de viés antidemocrático.

A articulação transnacional de movimentos extremistas, que compartilham táticas de manipulação e de propaganda em fóruns e comunidades próprias, eleva a sofisticação dessas ações e cria ameaças coordenadas e globalizadas contra

o processo democrático brasileiro, impactando diretamente a soberania nacional. Identificar e neutralizar essas ameaças constitui desafio para a Atividade de Inteligência.

Polarização social e a instrumentalização de crenças religiosas

A polarização ideológica tornou-se elemento de segmentação social, dividindo parte da sociedade em grupos antagônicos e prejudicando o diálogo democrático e a convivência pacífica com a pluralidade de ideias. Esse contexto de hostilidade contínua favorece a emergência do extremismo, que pressupõe retratar o adversário político como inimigo a ser eliminado, e não como competidor legítimo.

Esse quadro de radicalização contribui para o processo de deslegitimação e de enfraquecimento das instituições, alimenta o não reconhecimento de resultados eleitorais e mina a confiança pública nas estruturas do Estado Democrático de Direito. O fenômeno não se limita ao território nacional, inserindo-se em uma dinâmica transnacional, que acompanha o crescimento global de narrativas extremistas e fragmentárias.

Nesse contexto, tem sido observada a instrumentalização de crenças religiosas como elemento de mobilização e de polarização. A exploração das diferenças religiosas nesse sentido, em vez de promover o necessário diálogo entre religiões, contribui para traçar divisões, justificar posições intransigentes e mobilizar fiéis por agendas eleitorais com base em uma lógica de guerra religiosa. Essa dinâmica amplia a polarização e submete o debate político a dogmas que afrontam o princípio da laicidade do Estado.

No limite, a polarização exacerbada pode ainda catalisar ações de extremismo violento ideologicamente motivadas (EVIM), com riscos à integri-



dade física de eleitores, autoridades e infraestruturas críticas necessárias ao processo eleitoral. O extremismo, ao fornecer narrativas de deslegitimação do processo eleitoral, pode implicar ameaças concretas, como aquelas que culminaram nos eventos de 8 de janeiro de 2023 e que permanecem como risco para 2026.

Resiliência diante de múltiplas vulnerabilidades

O processo eleitoral de 2026 ocorrerá em contexto de múltiplas vulnerabilidades, com potencial para impactar a segurança e a integridade da democracia brasileira. A deslegitimação institucional, acelerada por campanhas de desinformação, constitui o alicerce sobre o qual outros riscos se estruturam.

O uso de inovações tecnológicas como inteligência artificial e *deepfakes* amplia, em escala sem precedentes, o poder de manipulação em massa e de instrumentalização política da desinformação. Por conseguinte, aprofundam-se a polarização ideológica e a exploração de crenças religiosas como ferramentas de disputa política, corrompendo a democracia e o tecido social. Essa fragmentação amplifica o poder de discursos radicalizados, os quais, em última instância, podem levar a ações de extremismo violento ideologicamente motivados. Somam-se a esse cenário a influência do crime organizado e o risco de interferência externa no processo eleitoral, resultando em quadro de alta complexidade para a segurança democrática em 2026.

As instituições e a democracia brasileiras, contudo, têm demonstrado resiliência. Apesar de sérias limitações de meios e recursos, a Inteligência de Estado foi capaz de monitorar o movimento de deslegitimação das eleições de 2022 e de antecipar o ataque às sedes dos Três Poderes em 8 de janeiro de 2023, contribuindo em seu escopo de

atuação para a defesa da democracia, como atestado pelo relatório final da CPMI do 8 de Janeiro. Nas eleições de 2024, a ABIN desenvolveu projeto específico voltado à proteção da democracia e integrou trabalho interagências de âmbito nacional coordenado pela Secretaria Nacional de Segurança Pública com foco em operações de segurança durante os períodos de votação. O processo eleitoral de 2026 será mais um teste à capacidade nacional de proteger suas instituições, mediar conflitos de modo pacífico e reafirmar os valores fundamentais do Estado Democrático de Direito.



Transição para a criptografia pós-quântica

A sociedade moderna utiliza criptografia diariamente, mesmo sem perceber. Ela está nas transações bancárias, nas criptomoedas, nos aplicativos de comunicação e em muitas outras atividades cotidianas. Responde por garantir confidencialidade, integridade e autenticidade de dados em trânsito e em repouso (armazenados). No contexto governamental, a criptografia tem papel direto na soberania digital: protege comunicações sigilosas e documentos sensíveis contra adversários, sustenta a cadeia de custódia de evidências, assegura a validade de atos administrativos e preserva a continuidade do Estado diante de crises. Ainda, é a base técnica para viabilizar autenticação entre órgãos e a interoperabilidade segura de serviços públicos em escala nacional.

Em linhas gerais, a criptografia se divide em dois grandes campos: criptografia simétrica e criptografia de chaves públicas. A primeira usa a mesma chave para cifrar e decifrar dados. Já a criptografia de chaves públicas (ou assimétrica) emprega duas chaves: uma privada, que deve permanecer em sigilo, e uma pública, que pode ser divulgada. Suas principais aplicações são a assinatura digital (autenticidade e não repúdio) e o acordo/troca de chaves para estabelecer canais seguros.

Vivemos um ponto de inflexão tecnológica, o início da Era Quântica, na qual a promessa do computador quântico pressiona a sociedade, em especial os Estados, a revisar, com urgência, suas defesas informacionais. Embora ainda em desenvolvimento, computadores quânticos têm potencial para resolver classes específicas de problemas muito mais rapidamente que máquinas clássicas (termo para as máquinas que usamos atualmente). Essa capacidade compromete, em particular, grande parte da criptografia de chaves públicas utilizada hoje, o que altera pressupostos de segurança em larga escala. Não é possível fi-





nar um cronograma preciso para um protótipo de um computador quântico com poder de processamento realmente disruptivo, mas estimativas variam de 5 a 15 anos.

Diante desse cenário, academia, indústria e governos têm trabalhado no desenvolvimento de algoritmos pós-quânticos — construídos sobre problemas matemáticos para os quais computadores quânticos não oferecem atalho conhecido em relação aos clássicos. O esforço de padronização internacional de algoritmos pós-quânticos, liderado pelo *National Institute of Standards and Technology* (NIST) desde 2016, já publicou um algoritmo de troca de chaves e dois de assinaturas digitais, além de outros em estágio avançado de padronização, compondo um portfólio inicial de algoritmos a serem incorporados por sistemas públicos e privados. Outros algoritmos candidatos seguem em avaliação, o que exige que órgãos do Estado adotem cripto-agilidade — capacidade de atualizar e alternar entre os algoritmos criptográficos de forma simples e ágil — para absorver atualizações sem reescrever sistemas do zero.

A urgência da transição pós-quântica tem dois fundamentos. Primeiro, a tática “coletar agora, decifrar depois” (*“harvest now, decrypt later”*): adversários podem armazenar hoje comunicações e dados protegidos pelos algoritmos atuais e decifrá-los no futuro, quando computadores quânticos possuírem capacidade computacional suficiente. Informações de longo prazo de sensibilidade — diplomacia, defesa, fontes e métodos de Inteligência, dados pessoais — permanecem valiosas por anos ou décadas. Segundo, o tempo de migração: transições criptográficas costumam levar mais de uma década, pela dificuldade de substituir componentes em produção e pela necessidade de compatibilidade entre sistemas que negociam protocolos e chaves. Por isso, reconhecer o problema e iniciar a transição o quanto antes

é parte da própria estratégia de mitigação de risco do Estado.

Transição pós-quântica na Inteligência de Estado

Para a Inteligência de Estado, a transição pós-quântica não é um tema apenas técnico, mas um problema de prioridade nacional que redefine o ciclo de vida da informação sigilosa. A Inteligência trabalha com horizontes de sigilo que atravessam governos, por isso, o risco do ataque “coletar agora, decifrar depois” é estrutural para fontes e métodos. Uma eventual quebra retroativa de dados sigilosos pode expor identidades, rotinas e técnicas.

Para a Inteligência, destacam-se dois cenários. No primeiro, o Estado provê resposta preventiva, em que a transição pós-quântica é executada antes de um computador quântico com alto poder computacional estar disponível. Essa resposta começa por uma triagem completa dos acervos e dos canais a serem protegidos, priorizando conteúdos pelo valor informacional e pela vida útil do sigilo. Adotam-se protocolos híbridos (os quais combinam algoritmos clássicos e pós-quânticos), define-se ritmo de rotação de chaves e estabelecem-se critérios de revalidação e re-assinatura com carimbo do tempo confiável, preservando a cadeia de custódia e a compatibilidade entre sistemas.

No segundo cenário, conhecido como “apocalipse quântico”, o adversário conquista capacidades quânticas antes de a transição pós-quântica ter sido finalizada. Nesse cenário, o atacante poderá ter acesso a dados sigilosos. O plano de continência deve prever corte rápido da comunicação, revogação e reemissão de materiais criptográficos, isolamento e compartimentalização de redes e acervos sensíveis, além de reestabelecimento das âncoras de confiança (*re-trust*) e re-assinatu-



ra priorizada de conteúdos de longa vida. Medidas específicas de proteção a fontes e de coordenação com aliados reduzem impacto e evitam janelas de *downgrade* (exploração de versões anteriores menos seguras que as atuais).

O apocalipse quântico, em um contexto de Inteligência de Estado, pode trazer consequências trágicas e duradouras, tendo em vista que segredos de longa data podem ser revelados, abalando relações internacionais, a segurança dos agentes e das fontes humanas, a segurança de infraestruturas críticas e podendo colocar em risco a soberania do país. Por isso, exercícios de mesa e testes conjuntos devem validar rotas de resposta antes da crise.

Confiança pública

A transição para algoritmos pós-quânticos não afeta apenas sistemas internos de governo ou setores sensíveis, ela tem reflexos diretos também sobre a sociedade. Serviços digitais amplamente utilizados, como identidade digital, declarações eletrônicas, assinaturas digitais e processos judiciais dependem de cadeias de confiança que precisam permanecer válidas e verificáveis por décadas. Qualquer falha nesse processo pode comprometer a percepção de segurança dos cida-

dãos, gerar disputas judiciais e abalar a legitimidade de ações públicas no ambiente digital.

Portanto, a confiança pública se torna um ativo estratégico. A população não precisa entender os detalhes técnicos dos novos algoritmos e protocolos, mas precisa confiar neles. Em parte, essa confiança pode ser obtida se a população souber que a transição está sendo conduzida com responsabilidade, transparência e foco na preservação de direitos. Para isso, é essencial que o processo seja bem comunicado, que as decisões técnicas sejam fundamentadas, e que a transição ocorra sem interromper ou invalidar serviços críticos já consolidados e estáveis. A continuidade dos serviços é um aspecto central para manter a confiança.

Além disso, o Estado tem o dever de garantir que os dados dos cidadãos, especialmente dados pessoais sensíveis, sejam mantidos cifrados e seguros durante toda a transição. Isso implica ajustar políticas de proteção de dados e assegurar que não haja enfraquecimento involuntário das garantias já estabelecidas. A confiança pública em um processo crítico como este não se conquista apenas com inovação tecnológica, mas com estabilidade institucional, coerência técnica e respeito aos princípios que regem a relação entre o Estado e o cidadão no ambiente digital.

Criptografia de Estado na Era Quântica

A criptografia de Estado engloba um conjunto de políticas, algoritmos e bibliotecas que sustentam o sigilo, autenticidade e continuidade segura de operações governamentais. Uma grande diferença entre a criptografia para uso civil e para uso governamental é que a última precisa assegurar a proteção de dados por décadas, necessitando assim de maiores garantias de segurança.

Na Era Quântica, a dependência de algoritmos criptográficos desenvolvidos por terceiros pode representar um risco estratégico para a soberania nacional. A criptografia de Estado, compreendida por um conjunto de políticas, algoritmos e bibliotecas desenvolvido por agentes públicos, torna-se ativo crítico para proteção de dados sensíveis, infraestruturas críticas e comunicações sigilosas. A possibilidade de que algoritmos amplamente adotados contenham fragilidades não divulgadas reforça a importância de abordagens autônomas por parte do Estado.

Nesse contexto, o desenvolvimento de algoritmos pós-quânticos de Estado, com rigorosa validação técnica, é um dos pilares para garantir a soberania digital. Não se trata de ignorar os

padrões internacionais, mas de reduzir a dependência, possivelmente realizando a combinação de ambos. Deve ser considerada a criação de um portfólio de algoritmos pós-quânticos, adaptados à realidade institucional, operacional e legal.

No entanto, a criação de algoritmos pós-quânticos de Estado enfrenta desafios. São fundamentais o investimento na pesquisa avançada, testes extensivos contra ataques provenientes de computadores clássicos e quânticos e validações formais de segurança. Além disso, é mandatório formar quadros especializados no tema com laboratórios governamentais e independentes. Falhas em quaisquer dessas etapas podem comprometer toda a infraestrutura que depende da segurança provida pelos algoritmos.

É essencial que a criptografia de Estado, principalmente na Era Quântica, seja tratada como projeto nacional de longo prazo, com continuidade entre governos e metas de maturidade bem definidas. A evolução desse processo fortalece a posição do Estado frente a ameaças futuras e reforça sua capacidade de proteger informações sensíveis em um cenário tecnológico incerto.





Etapas para uma transição pós-quântica

A transição pós-quântica em contexto governamental é um processo complexo que requer coordenação institucional, visão estratégica e execução técnica gradual e progressiva. Nesse contexto, em que o tempo de vida do sigilo pode atravessar décadas e em que a interoperabilidade entre sistemas é crítica, essa transição deve ser conduzida com estratégia e responsabilidade. Pode-se quebrar a transição em quatro grandes etapas fundamentais: conscientização e mobilização institucional, mapeamento de ativos criptográficos e avaliação de impactos, planejamento de migração por prioridade e execução da transição.

A conscientização e mobilização institucional é o primeiro passo da transição pós-quântica. Nessa etapa é fundamental reconhecer o impacto estratégico da ameaça quântica e tratá-la como uma ameaça à soberania nacional, e não somente um problema técnico. Essa etapa engloba a sensibilização da alta gestão dos órgãos e entidades, capacitação básica de equipes técnicas e a formação de estruturas coordenadoras, responsáveis pela transição. Também é um momento para emitir diretrizes e normativas oficiais, estabelecer metas temporais realísticas e definir princípios norteadores como cripto-agilidade e soberania tecnológica.

Na segunda etapa, com a governança estruturada, é preciso mapear ativos criptográficos e avaliar impactos. Nesse contexto, deve-se levantar quais sistemas usam criptografia, de que forma a usam e qual a sensibilidade dos dados protegidos. O mapeamento deve ser abrangente, cobrindo desde



aplicações críticas, como Infraestrutura de Chaves Públicas e comunicações sigilosas, até sistemas de uso indireto ou legados. Cada ativo identificado deve ser classificado, considerando o tipo de criptografia, sensibilidade da informação, grau de exposição e dificuldade de atualização. Tal mapeamento permite identificar riscos prioritários e áreas com maior impacto potencial caso a transição seja falha.

Com base no mapeamento de ativos, é possível iniciar a terceira etapa, o planejamento da migração. Essa etapa exige já uma definição dos algoritmos pós-quânticos a serem adotados, considerando tanto algoritmos padronizados, como também algoritmos de Estado para usos específicos. Sistemas que tratam de dados sensíveis de longa duração, como diplomacia e Inteligência, devem ser priorizados. Nesse estágio, também pode ser interessante o uso de protocolos híbridos como estratégia transitória.

Por fim, a etapa final é a execução da transição, com a substituição de algoritmos vulneráveis, implantação de novos protocolos e revalidação de sistemas críticos. Isso envolve atualização de software e de firmware, reemissão de certificados, ajuste de contrato com fornecedores e capacitação contínua. A transição deve ser monitorada com indicadores objetivos e preparada para contingências. A transição se considera concluída quando os sistemas deixam de operar com protocolos híbridos e passam a confiar exclusivamente em algoritmos pós-quânticos.



Ataques cibernéticos autônomos com uso de agentes de inteligência artificial

O excepcional desenvolvimento recente da inteligência artificial (IA) e dos grandes modelos de linguagem (*large language models* – LLMs) representa uma das mais significativas transformações tecnológicas do século XXI e repercute sobre todos os setores da sociedade moderna. Os inegáveis benefícios sobre produtividade e pesquisa oportunizados por essa tecnologia, entretanto, trazem consigo um cenário de risco crescente relacionado à segurança cibernética. Isso porque a autonomia e a capacidade de adaptação da IA não apenas facilitam os ataques cibernéticos, mas fundamentalmente alteram a dinâmica de defesa e a resposta do Estado.

A transição de ferramentas de IA de meras facilitadoras de atividades cotidianas e/ou repetitivas para agentes ofensivos autônomos capazes de operar — planejar, executar e adaptar ataques sem intervenção humana contínua — estabelece um novo e perigoso paradigma de ameaça para setores estratégicos e infraestruturas críticas. O uso dual de agentes de IA na condução de ataques cibernéticos autônomos envolve três fatores centrais. Em primeiro lugar, registra-se a escalabilidade e a sofisticação introduzidas pela IA no arsenal de condutas maliciosas no ambiente cibernético. Em segundo lugar, o agravamento do desafio da atribuição técnica dos ataques e suas complexas implicações para a geopolítica global. Por fim, os riscos concretos à segurança nacional que se materializam diante da velocidade incontável do avanço tecnológico e do desequilíbrio entre as capacidades ofensivas e defensivas.

A escala e a sofisticação do uso malicioso de agentes de IA

A principal ameaça representada pelos agentes autônomos de IA no contexto da segurança cibernética reside na sua capacidade de democratizar a sofisticação e permitir uma escalabilidade mas-





siva de operações maliciosas. Historicamente, a execução de um ataque cibernético complexo — envolvendo análise de vulnerabilidades, codificação de malware, desenvolvimento de infraestrutura de comando e controle (C2) e implementação de mecanismos de evasão — exigia equipes altamente especializadas e um investimento considerável de tempo e de recursos humanos. Agentes autônomos de IA eliminam essa barreira.

Como a análise de ameaças recentes evidencia, o uso de ambientes e agentes de programação baseados em IA tem permitido a proliferação do conceito de *no-code* malware. Indivíduos com pouca experiência em programação conseguem gerar *malwares* (trojans) de acesso remoto (RATs), personalizar *ransomwares* ou desenvolver complexos integradores de API com recursos de grau corporativo para os mais diversos tipos de operações maliciosas, a exemplo da fraude financeira e comércio de credenciais de acesso. A IA atua como um multiplicador de força, convertendo habilidades rudimentares em capacidade ofensiva avançada.

O potencial de escala é multifacetado. Agentes autônomos de IA podem processar vastas quantidades de dados roubados (*stealer logs*), perfis comportamentais e informações de vítimas, transformando dados brutos em Inteligência acionável para a priorização e personalização de ataques de engenharia social (*vibe hacking* e *spearphishing*). O aperfeiçoamento desse processo de análise e especificação de alvos (*targeting*) aumenta drasticamente a taxa de sucesso do ataque tendo em vista a precisão na seleção de potenciais alvos, assim como a capacidade de desenvolver códigos maliciosos específicos para atacar o alvo assinalado.

A IA possibilita, igualmente, a criação rápida e automatizada de plataformas criminosas robustas. Isso inclui desde a construção de *carding stores* (lojas de cartões de crédito roubados) alimentadas por IA para validação e antifraude, até

a implantação de serviços de identidade sintética, gerando perfis falsos com alta credibilidade e em grande volume. Essa capacidade de desenvolvimento de infraestrutura robustece a resiliência operacional dos atores maliciosos já que lhes permite monitorar continuamente as defesas de alvos potenciais e adaptar-se em tempo real. Ao enfrentar bloqueios ou mecanismos de detecção, o agente de IA pode efetuar *pivots* (mudanças de tática) e reconfigurações dinâmicas de forma imediata, garantindo a longevidade e a eficácia da campanha de ataque. Essa resiliência operacional torna as tentativas de desmantelamento mais onerosas e ineficazes.

O desafio da atribuição técnica e suas implicações geopolíticas

A atribuição de um ataque cibernético — o processo de identificar e nomear o responsável (indivíduo, grupo ou Estado) — sempre foi um dos desafios mais complexos na geopolítica do ciberespaço. Com a introdução de agentes de IA autônomos, esse desafio se aprofunda, criando uma nebulosidade estratégica que tem implicações diretas na estabilidade global.

Tradicionalmente, a atribuição técnica baseia-se na análise forense de Táticas, Técnicas e Procedimentos (TTPs), na reutilização de código ou infraestrutura e na observação de padrões linguísticos ou temporais associados a um determinado ator (o chamado *fingerprinting*).

Os agentes de IA, no entanto, introduzem elementos de ofuscação inéditos. Ao utilizar modelos de IA para criar *malware* ou planejar cadeias de ataque, o código gerado tende a ser homogêneo ou, ao contrário, excessivamente variado. A IA pode ser instruída a evitar a reutilização de trechos de código ou a gerar *exploits* que não reflitam os padrões heurísticos de um grupo específico. Isso



dilui as assinaturas digitais, tornando o *fingerprin-ting* uma técnica obsoleta para a identificação.

Agentes de IA podem, ainda, ser programados para integrar ativamente mecanismos de falsa atribuição, inserindo intencionalmente metadados, comentários em linguagens estrangeiras ou utilizando infraestrutura (servidores *proxy*, VPNs) tipicamente associada a um Estado rival, desviando a atenção dos investigadores. A consequente dificuldade na atribuição técnica confiável tem um impacto direto na geopolítica global.

A incerteza quanto à autoria impede a aplicação de mecanismos de dissuasão e resposta baseados em normas internacionais. Se um Estado não consegue determinar com certeza se o ataque à sua infraestrutura crítica foi perpetrado por um grupo cibercriminal comum, um ator patrocinado por um Estado ou se foi uma operação de bandeira falsa, a resposta apropriada torna-se extremamente arriscada.

Esse cenário alimenta uma perigosa assimetria e a escalada horizontal de conflitos. A falta de responsabilidade clara incentiva a agressão no ciberespaço, pois os Estados podem operar por meio de proxies de IA com alta negação plausível. A escalada pode levar a um ciclo de acusações não verificáveis, aumentando a tensão diplomática e o risco de que incidentes cibernéticos transbordem para conflitos militares tradicionais, na ausência de mecanismos claros de “lei de guerra” ou de resposta calibrada para o domínio cibernético.

Desenvolvimento tecnológico acelerado e riscos à segurança nacional

O rápido e muitas vezes desregulado desenvolvimento tecnológico no campo da IA impõe riscos existenciais à segurança nacional de qualquer Estado. A janela de tempo entre a descoberta de uma nova capacidade ofensiva por agentes de IA e

o desenvolvimento e implementação de uma defesa eficaz apresenta uma disparidade cujo resultado é a criação de um desequilíbrio estratégico em favor dos agressores.

O principal risco reside na capacidade dos agentes de IA, especialmente aqueles desenvolvidos ou utilizados por atores estatais ou patrocinados por Estados, de lançar ataques complexos e coordenados contra infraestruturas críticas nacionais. Sistemas de energia, telecomunicações, redes financeiras, saúde e transporte são alvos prioritários que, se comprometidos de forma autônoma e em larga escala, podem paralisar um país. O uso de IA para automatizar técnicas em praticamente todos os estágios do framework MITRE ATT&CK (diretriz de classificação e descrição de ataques cibernéticos), por exemplo, como já observado em grupos de ameaças persistentes avançadas (APTs), demonstra a maturidade das aplicações maliciosas da IA em contextos de conflito cibernético.

O fator temporal é crucial. A corrida tecnológica pela primazia em IA, impulsionada por disputa entre potências como EUA e China, leva ao rápido lançamento de modelos cada vez mais poderosos, sem que haja uma avaliação de risco ou um quadro regulatório global que garanta sua segurança. A natureza de uso dual da IA significa que qualquer avanço na capacidade de codificação ou de análise de *datasets* pode ser imediatamente apropriado pelo vetor ofensivo.

Os riscos à segurança nacional impostos pelo uso malicioso da IA apontam para ameaças emergentes relevantes, como vulnerabilidade massiva, aprimoramento da guerra da informação e escalada da ciberespionagem.

A vulnerabilidade massiva pode ser sintetizada em relação à capacidade da IA de identificar rapidamente vulnerabilidades de *zero-day* em sistemas amplamente utilizados e transformá-las



em *exploits* operacionais de forma automática, aumentando as chances de que um único ataque cause falhas sistêmicas e generalizadas.

No que diz respeito à guerra da informação, agentes de IA são ferramentas ideais para a disseminação autônoma e personalizada de desinformação e propaganda, visando a subversão da estabilidade política, eleitoral e social de um país. A capacidade de criar *deepfakes* e narrativas coesas em escala torna a guerra de informação uma ameaça à coesão social e à soberania dos Estados. O conflito russo-ucraniano é um notável exemplo de utilização de IA para disseminação de propaganda.

Com relação à escalada da ciberespionagem, a automação de tarefas de acesso, exfiltração de dados e manutenção de persistência em redes visadas torna a espionagem cibernética mais furtiva, abrangente e contínua, potencialmente comprometendo segredos de Estado, vantagens competitivas e propriedade intelectual em um ritmo sem precedentes.

O desafio da regulação dos agentes autônomos de IA

A criação de regulamentações internacionais para agentes autônomos de IA representa um grande desafio devido à natureza descentralizada e global da tecnologia. Em um cenário onde agentes autônomos podem ser programados para explorar vulnerabilidades e realizar ataques em tempo real, as normas precisam ser eficazes em diversas jurisdições e contextos legais, o que é extremamente difícil devido às disparidades nas legislações nacionais.

Enquanto alguns países podem adotar regulamentos rigorosos, outros podem ser mais permissivos, criando lacunas que podem ser exploradas por cibercriminosos de todo o mundo, tornando todo ambiente global de IA mais vulnerável. Além disso, muitos agentes autônomos operam de ma-

neira oculta, dificultando a detecção e responsabilização, o que aumenta a complexidade de se estabelecer uma regulamentação clara e aplicada de maneira uniforme em nível global.

Outro obstáculo significativo é a diversidade de motivações para o uso de IA em ataques cibernéticos, que vão desde ações de grupos criminosos até operações estatais com fins de espionagem ou guerra cibernética. Essa multiplicidade de atores e intenções complica a criação de normas que sejam eficazes em punir os responsáveis e prevenir o uso indevido da tecnologia.

A regulamentação internacional precisaria definir claramente não apenas o que constitui um ataque cibernético utilizando IA, mas também estabelecer critérios sobre a responsabilidade de desenvolvedores e governos, além de promover mecanismos de cooperação entre países para rastrear, mitigar e punir esses ataques. A falta de consenso sobre definições jurídicas, aliada ao risco de normas desatualizadas frente à velocidade da inovação tecnológica, torna a tarefa de regular o uso de IA em ciberataques uma questão de difícil resolução.

Para além de um desafio técnico

A ascensão de agentes de IA na condução de ataques cibernéticos autônomos marca um ponto de inflexão na segurança cibernética global. O poder da IA para escalar o uso malicioso, reduzir a barreira de entrada e aumentar dramaticamente a sofisticação técnica de operações encobertas impõe um desafio triplo à comunidade internacional: a mitigação da ameaça de ataques autônomos, o estabelecimento de um regime de responsabilidade no ciberespaço e a gestão da velocidade incontável do desenvolvimento tecnológico.

A dificuldade crescente na atribuição técnica mina os alicerces que sustentam o uso da dissua-



são enquanto ferramenta de política externa, elevando o risco de confrontos geopolíticos baseados em acusações não comprovadas e alimentando um ambiente de desconfiança e instabilidade no ciberespaço. Simultaneamente, a vulnerabilidade de infraestruturas críticas à automação ofensiva da IA representa uma ameaça direta e imediata à segurança nacional e à soberania dos Estados.

Diante desse cenário, a resposta não pode ser apenas tecnológica; ela deve ser estratégica, regulatória e diplomática. É imperativo o investimento maciço em pesquisa de IA para segurança e defesa cibernética, com foco no desenvolvimento de agentes de defesa autônomos capazes de combater ameaças em tempo de máquina.

Adicionalmente, a cooperação internacional é fundamental para o estabelecimento de normas globais para o uso responsável da IA, especialmente por parte de Estados, a implementação de mecanismos de rastreamento e *watermarking* em grandes modelos de linguagem e a criação de regimes de responsabilidade legal para a má utilização de aplicações de IA.

A segurança na era da IA não é um problema estritamente técnico, mas um desafio de governança global capaz de definir a paz e a estabilidade do século XXI, razão pela qual deve ser acompanhado atentamente pela Atividade de Inteligência.



Reconfiguração das cadeias de suprimento globais

As cadeias globais de suprimentos, ou também cadeias globais de valor (CGV), constituem um dos elementos centrais da organização econômica contemporânea. Elas se caracterizam pela fragmentação internacional da produção em etapas dispersas geograficamente, coordenadas por grandes corporações transnacionais, de acordo com vantagens comparativas em custos, acesso a insumos e capacidades tecnológicas. Esse processo de organização da economia internacional faz parte de uma trajetória de transformações estruturais em curso desde meados do século XX.

A expansão das CGV insere-se no arcabouço institucional de Bretton Woods. O sistema pós-guerra, centrado nos EUA, operava pela exportação de capitais (e, posteriormente, serviços) estadunidenses em contrapartida à importação líquida de bens primários e manufaturados dos países receptores, configurando um ciclo integrado de produção e pagamentos. Após 1971, mesmo com o fim do padrão dólar-ouro, a moeda norte-americana manteve-se como referência nas reservas internacionais e unidade de conta do comércio global. A lógica essencial do sistema — financiamento em dólares, a liberalização dos mercados e a continuidade das importações dos EUA — se manteve, e com ela os incentivos ao deslocamento produtivo, o que consolidou o *offshoring* industrial das economias ocidentais.

Nos anos 1990, a globalização ganhou impulso decisivo. Inicialmente, a lógica resultante das CGV consolidou-se em torno de uma divisão funcional da economia global: atividades de produção de bens padronizados, baseados em custos, localizadas na periferia; enquanto funções de maior complexidade, como design, propriedade intelectual, marcas, marketing e coordenação de cadeias, permaneceram nos países centrais. Dessa forma, a captura de lucros monopolísticos concentrou-se





em grandes conglomerados das economias avançadas, enquanto países periféricos tornaram-se fornecedores de trabalho barato, insumos primários ou manufaturas de menor sofisticação.

Ao mesmo tempo, o processo possibilitou a ascensão econômica de certos países da periferia. Taiwan e Coreia do Sul, inicialmente inseridos em setores de baixa e média complexidade, avançaram para indústrias de alta tecnologia por meio de políticas industriais seletivas, investimentos estratégicos e fortalecimento do capital humano, consolidando liderança em semicondutores com TSMC e Samsung. A China iniciou processo semelhante, abrindo-se ao capital ocidental em suas zonas especiais de comércio, entrando na OMC em 2001 e transformando-se em plataforma exportadora de escala inédita, especializada em montagem e manufatura intensiva em trabalho e de menor valor agregado.

Ascensão da China, Guerra Econômica e COVID-19

A partir da primeira década do século XXI, a China passou a ocupar segmentos de maior intensidade tecnológica e de capital nas CGVs. De economia complementar às desenvolvidas, transformou-se em competidora internacional em mercados de produtos industriais sofisticados e na exportação de capitais, sobretudo em infraestrutura logística, energética e de telecomunicações no âmbito da *Belt and Road Initiative* (BRI). Paralelamente, os EUA, em razão de transformações estruturais internas, de sua posição como emissor da moeda de reserva global e de políticas fiscais persistentemente deficitárias, seguiram trajetória correlacionada de desindustrialização e déficits comerciais crescentes. Essa dupla dinâmica redefiniu a distribuição de poder, ganhos e vulnerabilidades entre os países e impulsionou o debate sobre a reorganização do sistema econômico, financeiro

e monetário mundial, estabelecendo as bases da atual lógica geoeconômica e dos desafios da reestruturação das cadeias globais de valor.

Nos EUA, as últimas administrações adotaram medidas de contenção contra a China, impondo restrições à exportação de semicondutores, softwares e componentes críticos, bem como limitando investimentos chineses em setores estratégicos por meio do Comitê sobre Investimento Estrangeiro nos Estados Unidos (CFIUS, na sigla em inglês). Essas políticas, voltadas a proteger propriedade intelectual, manter a liderança tecnológica e reduzir riscos de dependência externa, consolidaram um consenso bipartidário e foram acompanhadas por aliados dos EUA, especialmente na União Europeia, que implementaram controles semelhantes em setores de defesa e telecomunicações, como o 5G.

A pandemia de COVID-19 (2019–2020), que provocou interrupções na produção e escassez de contêineres e semicondutores, expôs a vulnerabilidade das cadeias globais, revelando a fragilidade do modelo *just in time* e levando à adoção do modelo *just in case*, com estoques estratégicos e diversificação de fornecedores. A pandemia acelerou movimentos de *reshoring*, o retorno da produção ao próprio país, e *friendshoring*, o deslocamento das linhas de produção para países aliados ou mais próximos politicamente, reduzindo dependências críticas, enquanto conceitos como *decoupling*, uma separação total das economias, e *derisking*, a redução de riscos decorrentes de excessiva dependência de determinados países, passaram a orientar políticas públicas e investimentos em setores estratégicos como semicondutores e inteligência artificial. Esse período marcou a transição da desaceleração para a desglobalização, com a segurança nacional e a competição geoeconômica superando a ênfase na eficiência e no comércio.



Entre 2017 e 2025, observou-se uma estagnação no comércio global, evidenciada pela estabilização da relação entre comércio mundial e PIB após a recuperação pós-crise financeira de 2008, enquanto os fluxos de Investimento Direto Estrangeiro (IDE) também desaceleraram, caindo 12% em 2022 e totalizando US\$ 1,3 trilhão. Segundo a OCDE, entre o primeiro semestre de 2022 e o primeiro semestre de 2023, os fluxos globais de IDE diminuíram 30%, enquanto os fluxos para a área da OCDE caíram 42%. Para 2025, a organização destaca que, embora os fluxos globais de IDE tenham mostrado sinais de recuperação após a desaceleração observada em anos anteriores, ainda estão abaixo dos níveis registrados antes da pandemia de COVID-19. Esse cenário reflete tanto a desaceleração do crescimento do comércio internacional quanto o impacto de crises geopolíticas, maior aversão ao risco e políticas internas restritivas, indicando um enfraquecimento estrutural da globalização e com implicações diretas para as cadeias de suprimentos.

No entanto, mesmo com esses retrocessos, a interdependência econômica não desapareceu. Empresas seguiram buscando eficiência via *offshoring*, mas com novas configurações geográficas. A China manteve sua posição central na manufatura, enquanto a parte de menor valor agregado de sua produção se deslocou para o Sudeste Asiático. Índia e México, por sua vez, beneficiaram-se do *friendshoring*, que visava mitigar riscos geopolíticos e garantir fornecedores mais confiáveis.

Mudança de governo nos EUA

Embora a desglobalização já tivesse começado antes da Pandemia de COVID-19, a conjuntura sob a atual administração norte-americana marcou um ponto de inflexão. A guerra econômica com a China intensificou-se, com tarifas acima de 100%

e restrições a investimentos que chegaram a paralisar temporariamente o comércio direto entre os países. A lógica de *America First* tornou-se mais intensa e transacional, priorizando o *reshoring* de setores estratégicos para os EUA, mesmo em detrimento de aliados como Canadá, México e Índia, ao rejeitar o *friendshoring* e impor um protecionismo tarifário generalizado.

Essa lógica de desglobalização deliberada busca reestruturar o sistema comercial global para corrigir o que o governo norte-americano considera desequilíbrios estruturais: déficits comerciais persistentes e dependências críticas de cadeias de suprimentos. O governo norte-americano também procura vincular acordos comerciais à cooperação em segurança nacional, integrando objetivos econômicos e estratégicos dos EUA e enfraquecendo o sistema multilateral de comércio da OMC.

Por outro lado, em contradição com esses objetivos, o governo dos EUA aprovou um pacote fiscal com amplas reduções tributárias, a chamada *Big Beautiful Bill*, que, segundo estimativas do mercado, deve aumentar em cerca de US\$ 3 trilhões o já elevado déficit fiscal desse país, com o correlacionado aumento do déficit comercial. Em conjunto com a incerteza decorrente das tarifas, a política parece ter também enfraquecido a posição do dólar, refletindo-se em altas de mercado do ouro (cerca de 60% desde o início de 2025) e de criptoativos (bitcoin subiu cerca de 70% desde outubro de 2024), instrumentos alternativos de reserva de valor.

Embora a diversificação de reservas e a queda relativa do dólar já fossem observáveis desde os anos 2000, a política do atual governo dos EUA parece ter acelerado essa tendência. Em setembro de 2025, o valor das reservas de ouro dos bancos centrais superou o das reservas de títulos de longo prazo do Tesouro norte-americano pela



primeira vez desde 1996, enquanto a participação do dólar nas reservas internacionais caiu de 72% na virada do século para 59%. De janeiro de 2020 até 2025, a participação da propriedade de estrangeiros nos títulos públicos dos EUA caiu de cerca de 40% para menos de 31%. Esses dados não indicam o fim do status de moeda reserva, mas evidenciam uma tendência estrutural reforçada pela política atual dos EUA.

Um equilíbrio difícil

O Brasil, apesar de registrar déficit comercial com os EUA e desequilíbrio significativo em transações correntes, foi incluído entre os países fortemente afetados pela política tarifária norte-americana, enfrentando alíquotas de até 50%, patamar comparável apenas ao aplicado à Índia. A medida revelou caráter predominantemente político, associando-se a formas de pressão externa no contexto das disputas institucionais brasileiras e de seu posicionamento geopolítico. Apesar da possibilidade de redirecionamento parcial das exportações para outros mercados, a elevação das tarifas sobre produtos brasileiros causa prejuízos socioeconômicos expressivos nas cadeias afetadas, prevendo-se um impacto geral de redução de 0,2% do PIB e perda de cerca de 100.000 empregos, conforme estimativas de setembro de 2025.

Essa conjuntura agravou a posição do Brasil na reestruturação das cadeias de suprimentos globais, que, embora ofereçam oportunidades, continuam marcadas por ameaças e obstáculos, em grande parte decorrentes das fragilidades econômicas e geopolíticas. O período de maior intensidade da globalização, a partir dos anos 1990, coincidiu com crises e políticas de estabilização do país. De acordo com a Confederação Nacional das Indústrias (CNI), a desindustrialização observada nesse período, em decorrência de problemas de competitividade e Custo Brasil, reduziu a participação da indústria no PIB de cerca de 40% para 24,7% em 2024. O Custo Brasil sintetiza fatores internos que limitam a competitividade internacional do país, incluindo altos custos de capital, baixa qualificação de mão de obra especializada, insuficiente infraestrutura logística, energética e de telecomunicações, matriz logística distorcida, insegurança jurídica e elevada carga tributária.

A desindustrialização se reflete na tendência de reprimarização da pauta de exportações, fortemente concentrada em petróleo, soja e minério de ferro para a China. Ao mesmo tempo em que o Brasil foi perdendo posição relativa nas cadeias de suprimentos industriais e de maior valor agregado, tornando-se cada vez mais dependente das exportações para a China para manutenção de seu superávit comercial, suas taxas de poupança e investimentos estão entre as mais baixas do mundo, refletindo-se em um déficit crônico e crescente em transações correntes. Essa necessidade de capital externo para complementação da poupança interna brasileira é suprida principalmente pelos países ocidentais, com destaque para os EUA.

Assim, em conjunto, o Brasil é duplamente dependente dos dois rivais sistêmicos EUA e China, o que determina uma necessidade de manutenção de boas relações com ambos para viabilizar seus programas de desenvolvimento industrial e uma



melhor inserção internacional do país nas cadeias de suprimentos globais. Esse já difícil equilíbrio é ainda agravado pela conjuntura atual de transformação sistêmica da economia internacional e guerra econômica. Por fim, para além desses desafios externos, o aproveitamento das oportunidades da reestruturação das CGV, como o recebimento de investimentos na lógica do *friendshoring* e cooperação científico-tecnológica, depende da superação dos problemas e fragilidades internos seculares do país.

Inteligência para maximizar os interesses nacionais

Os conflitos travados em torno da atual reestruturação da economia internacional, e das cadeias de suprimentos em específico, apresentam uma faceta informacional decisiva e se desdobram no embate em curso entre os serviços de Inteligência das diversas potências. Do lado da Contraineligência, é vital proteger o segredo sobre conhecimentos e decisões estratégicas nacionais, além de se contrapor às diversas formas de ações adversas de competidores, como sabotagem, espionagem e interferências externas na esfera econômica.

A Política Nacional de Inteligência (PNI), por sua vez, prevê o acompanhamento da conjuntura internacional, implicando também atribuições de Inteligência de Estado para a produção de conhecimentos estratégicos especializados e integrados sobre Economia. Seu diferencial em relação aos trabalhos analíticos de outros órgãos governamentais está no monopólio legal de utilização de meios operacionais especializados para a obtenção de dados negados, bem como em seu olhar sistêmico específico de segurança econômica, geoeconomia e guerra econômica, com foco nas vulnerabilidades e nos interesses brasileiros.

No contexto dos atuais desafios da reestruturação das cadeias de suprimentos globais, cabe à Inteligência Econômica de Estado produzir apreciações e estimativas sobre problemas relacionados a temas como as cadeias globais de semicondutores, minerais críticos, criptoativos e inteligência artificial, de modo a maximizar a efetividade das políticas industriais e externa, mitigando-se contradições, desperdício de recursos e voluntarismos. Finalmente, cadeias produtivas em setores críticos para o Brasil, como o energético, inclusive petróleo, gás e biocombustíveis, ou o agronegócio, são objetos típicos da produção de Inteligência, devido à sua centralidade para a segurança econômica do País.

Dependência tecnológica, atores não estatais e interferência externa

O domínio digital consolidou-se como arena central da competição geopolítica e da projeção de poder no século XXI. A infraestrutura informacional, os fluxos de dados e as plataformas de interação social não são ambientes neutros; são territórios disputados, construídos e regulados por atores estatais e não estatais. Neste cenário, as *big techs* emergem como protagonistas cruciais, aprofundando relações desiguais e de dependência estrutural entre os atores do sistema internacional. Como atores não estatais, mas ligados a territórios e estruturas legais, burocráticas e repressivas de natureza estatal, as *big techs* atuam tanto com interesses próprios quanto, em arranjos complexos, como vetores de influência de seus países-sede.

O Brasil possui um mercado digital robusto, mas ainda busca maior autonomia no desenvolvimento, na produção e na implementação de tecnologias críticas para reduzir a dependência em relação a tecnologias, conhecimentos e inovações controlados por atores externos. Nesse contexto, a arquitetura de dependência tem nas *big techs* um de seus pilares, impondo-se ao Brasil um desafio multifacetado de soberania, no qual se destacam as vulnerabilidades do país a ações sofisticadas de interferência externa.

Big techs

A atuação das *big techs* é consequência de uma ordem internacional em que os Estados nacionais deixam de ser os únicos protagonistas. Os conglomerados de tecnologia atuam de forma cada vez mais transnacional, provendo bens e serviços diretamente aos cidadãos em escala mundial, além de se consolidarem como fornecedores de tecnologias essenciais ao próprio funcionamento dos governos. Nesse sentido, colocam-se na arena internacional como atores relevantes que perseguem interesses próprios. Contudo, nenhu-



ma corporação atua sem lastro em um território e em uma jurisdição. A capacidade de influência das *big techs* depende também do poder dos Estados que as abrigam e o alcance de suas decisões no espaço digital reflete, em última instância, a arquitetura de poder geopolítico construída por esses Estados.

As grandes empresas de tecnologia, com respaldo dos governos de seus países de origem, expandem contratos, instalam *datas centers*, firmam parcerias educacionais e financiam programas de inovação. Esses movimentos projetam poder, moldando a opinião pública e criando dependências para o provimento de serviços essenciais. As potências consolidadas controlam padrões, redes e cadeias produtivas, enquanto países periféricos operam em condição de dependência estrutural. Sistemas de identidade digital, armazenamento em nuvem, autenticação bancária, vigilância urbana e gestão de dados públicos dependem de provedores externos. Isso resulta em sérias vulnerabilidades, uma vez que leis estrangeiras podem impor o compartilhamento de dados com os governos dos países-sede dessas empresas.

Nesse sentido, deve-se compreender o investimento estrangeiro como oportunidade, mas também como instrumento de influência. As *big techs* têm o poder de condicionar o acesso às suas tecnologias a determinadas decisões políticas e comerciais dos países onde operam. A soberania no ciberespaço é enfraquecida por cláusulas contratuais que restringem ações de auditoria, impõem sigilo de código e limitam portabilidade de dados. Quando falhas de segurança ocorrem, o país depende da cooperação voluntária dos provedores para restabelecer serviços ou identificar responsáveis.

A conformação do espaço cibernético não é espontânea: resulta de políticas industriais, tra-

tados, regimes de vigilância e decisões militares definidos ao longo das últimas três décadas. Assim, a decisão de restringir o acesso, impor padrões locais ou desmembrar plataformas — com o objetivo de resguardar a soberania — deve estar baseada não apenas nos valores e bens jurídicos que a legislação nacional busca proteger, mas também na construção de capacidade estatal que possibilite o cumprimento de sua legislação.

Soberania digital: entre colaboração, dependência e controle

No caso brasileiro, a soberania digital é uma questão estratégica. Atualmente, o país depende de infraestruturas, serviços e tecnologias sujeitas a decisões tomadas em território estrangeiro. Porém, o Brasil ainda detém margem de manobra para definir seu grau de autonomia. O que está em disputa é a capacidade de decisão sobre fluxos de dados, cadeias produtivas e algoritmos que impactam diretamente a segurança nacional. Preservar soberania informacional significa manter o poder de escolha — decidir quando integrar, limitar e substituir.

As *big techs* e demais atores não estatais influenciam o sistema internacional, mas seu poder é balizado pela atuação dos Estados. A forma como o Brasil administra essa relação entre colaboração, dependência e controle determinará o espaço real de sua soberania digital nas próximas décadas. Em geral, as estratégias de soberania digital integram programas de incentivo à pesquisa aplicada e à autonomia em estágios críticos da cadeia de produção de semicondutores, ao desenvolvimento de *softwares* críticos e a inovações em inteligência artificial. A lógica predominante é de substituição seletiva de dependências: o que for crítico deve ser controlado, o que for dispensável pode ser terceirizado ou globalizado.



Não existe neutralidade tecnológica. Cada infraestrutura, de cabos submarinos a *data centers*, expressa e consolida relações de poder. Por isso, é imprescindível arbitrar as relações político-econômicas do ecossistema digital, priorizando investimentos em ciência, tecnologia, inovação e Inteligência com propósito estratégico.

Nesse ecossistema, reconhece-se que as redes sociais continuam a mediar parte substancial do debate político, inclusive por meio da facilitação ou inação diante de campanhas de desinformação. Nesse contexto, as dificuldades para desenhar e implementar uma estratégia integrada de comunicação, Inteligência e atuação junto às plataformas digitais no enfrentamento à desinformação faz com que o poder público, diante da população, apareça ora como censor, ora como espectador impotente. Como resultado, o espaço público digital permanece suscetível a campanhas de propaganda adversa e de desinformação.

Para mitigar esse risco, a alfabetização digital é prioritária, pois ajuda a prevenir a população contra a manipulação informacional em larga escala. Campanhas de esclarecimento e parcerias com universidades e veículos públicos formam a camada mais eficaz de resiliência social frente a narrativas fabricadas e disseminadas com interesses encobertos.

No campo internacional, a condução da política externa pela diplomacia brasileira tem papel fundamental na garantia da soberania digital. A soberania efetiva demanda negociações pragmáticas com polos concorrentes ou antagônicos, sem alinhamentos automáticos. A competição entre potências externas quanto ao controle de padrões técnicos, rotas de dados e cadeias produtivas de semicondutores oferece oportunidades para a negociação de vantagens assimétricas, como investimentos, crédito e transferência limitada de tecnologia, em troca de acesso a mercados.

Nesse sentido, o Brasil é um ator excepcional. Por um lado, oferece estabilidade e acesso a um mercado robusto e geograficamente estratégico. Por outro lado, tem um ecossistema produtivo que oferece capacidades tecnológicas relevantes para a integração desse mercado com cadeias globais de valor. É natural, portanto, que as negociações tecnológicas incluam contrapartidas reais dos atores que desejarem operar no mercado digital brasileiro: transferência de tecnologia, hospedagem local de dados sensíveis, auditoria de algoritmos e respeito às normas de segurança cibernética.

Interferência externa

A necessidade de promover a soberania digital torna-se clara quando se considera mais detidamente a ameaça de interferência externa. A interferência externa é a atividade deliberada, encoberta, empreendida por um ator externo (tipicamente um Estado, mas não somente) visando influenciar o comportamento de um Estado-alvo para atingir objetivos estratégicos específicos do patrocinador da ação. Esses objetivos são alcançados pela manipulação de processos decisórios, da opinião pública ou da estabilidade político-econômica. As ferramentas para tal incluem propaganda adversa, desinformação, fomento encoberto a grupos e entidades, apoio à manipulação jurídico-legal (*lawfare*) e sabotagem — frequentemente combinadas em estratégias híbridas.

O recrudescimento dessas ações ocorre em um cenário de redefinição sistêmica da ordem internacional. A transição para uma multipolaridade desequilibrada e desinstitucionalizada, marcada pelo declínio da ordem liberal e pela acentuada competição EUA-China, securitiza esferas como a tecnologia, a economia e a informação. Para o Brasil, situado em uma América do Sul cobiçada por seus recursos estratégicos, essa disputa glo-



bal eleva a pressão por alinhamentos e expõe vulnerabilidades crônicas, com graves consequências para a segurança.

Nesse contexto conflagrado, a dependência tecnológica é uma vulnerabilidade grave e imediata. A assimetria estabelecida pelo controle estrangeiro da infraestrutura digital, em sentido amplo, não constitui apenas um desequilíbrio comercial; ela representa um vetor estrutural de acesso e influência para os Estados-nação que sediam ou regulam essas corporações, transformando a tecnologia em ferramenta de projeção de poder estatal. Considerando a ameaça de interferência externa, a dependência tecnológica multiplica os riscos em vários níveis, permitindo a combinação de métodos de interferência em campanhas complexas, de difícil detecção, atribuição, obstrução e neutralização.

Num primeiro nível, a dependência facilita a interferência por intermédio das operações de informação. O controle estrangeiro sobre os algoritmos que filtram e distribuem conteúdo (redes sociais, mecanismos de busca) confere a capacidade de modular o debate público. Isso permite a atores externos conduzir guerra cognitiva em escala e em uma zona eminentemente cinzenta, amplificando artificialmente a desinformação, explorando clivagens sociais para aprofundar a polarização e minando a confiança pública em instituições (como o sistema eleitoral ou o judiciário). Trata-se do uso do ecossistema informacional de uma sociedade aberta para manipulá-la.

O segundo nível é a espionagem cibernética sistêmica. A dependência crítica de serviços de computação em nuvem estrangeiros para armazenar dados sensíveis — governamentais, financeiros, militares, diplomáticos, de Inteligência, de empresas estratégicas e da base industrial de defesa — cria um ponto único de falha (uma vulnerabilidade crítica centralizada) para a segurança da informa-

ção. O acesso facilitado a esses dados confere ao ator externo uma vantagem estratégica absoluta, permitindo antecipar decisões, mapear redes de poder e obter material para coerção futura.

O terceiro, e mais drástico, nível é o potencial de sabotagem (por ataque cibernético) e coerção. A dependência da infraestrutura crítica nacional (setor elétrico, financeiro, comunicações) de hardware e software de origem estrangeira concede ao ator externo a capacidade latente de degradar, interromper ou destruir serviços essenciais. A mera existência dessa capacidade funciona como um instrumento de coerção: a ameaça de um “apagão” digital ou energético pode ser utilizada para forçar o Brasil a adotar posições de política externa ou a aceitar condições comerciais desfavoráveis.

A verdadeira eficácia da interferência reside na combinação híbrida dessas ações, potencializada pela tecnologia. Um ator externo pode, por exemplo, utilizar seu acesso privilegiado às infraestruturas de nuvem e software de gestão para exfiltrar dados sigilosos sobre as vulnerabilidades operacionais de sistemas de gerenciamento de distribuição energética. Simultaneamente, esse ator pode lançar uma campanha utilizando as plataformas digitais para disseminar narrativas de pânico sobre um suposto “risco iminente de apagão”, minando a confiança pública na gestão estatal.

Com o país-alvo sob intensa pressão pública (pela guerra cognitiva) e com suas vulnerabilidades técnicas mapeadas (pela espionagem), o ator externo lança mão de ações de coerção. Não há necessidade de um ataque de sabotagem completo e ruidoso. Estas ações podem manifestar-se como demonstração de força — uma breve interrupção no fornecimento de energia em uma área industrial — servindo como ameaça crível e não atribuída, a qual força o país-alvo a ceder a demandas geopolíticas ou comerciais.

Essa vulnerabilidade tecnológica não substitui, mas agrava os riscos tradicionais. As pressões políticas e militares para o alinhamento regional, como as observadas na pressão econômica, política e militar sobre a Venezuela ou na securitização do debate sobre o crime organizado, tornam-se mais eficazes quando o país-alvo já está vulnerável em termos tecnológicos, dividido em termos cognitivos pelas operações de informação e comprometido em termos informacionais pela espionagem. As ações encobertas de interferência externa tornam o país mais suscetível à coerção geopolítica clássica.

Em suma, a dependência tecnológica transfere porções significativas da soberania cognitiva, informacional e infraestrutural para atores externos. Sem o controle sobre seus próprios dados e sobre os algoritmos que moldam o debate público, os países dependentes permanecem expostos a uma interferência constante, sutil e escalável no espectro híbrido, que pode ditar resultados políticos e econômicos sem a necessidade de uma única ação militar direta. A mitigação desse risco exige o adensamento da soberania digital e da capacidade cibernética nacional.



Conclusão

O cenário global atual é definido por uma confluência de transições — climática, demográfica e tecnológica — que ocorrem em meio a uma reconfiguração da ordem internacional. Essa reconfiguração se acelerou ao longo de 2025, confirmando e aprofundando as tendências apresentadas na edição anterior de *Desafios de Inteligência* (riscos globais, competição, multipolaridade). A América do Sul, por sua inserção assimétrica e pouco coordenada, ganhou mais relevância nessa disputa internacional, com consequências preocupantes para a segurança regional. O equilíbrio continua sendo característica do posicionamento brasileiro, porém a preservação de autonomia estratégica depende, entre outros fatores, do tratamento adequado dos desafios de Inteligência apontados para 2026.

No plano global, os riscos compartilhados pelas pessoas e os países não são compartimentados, embora suas consequências sejam distribuídas de forma desigual. Para o Brasil, a crise climática não é apenas um desafio ambiental, mas um multiplicador de riscos que impacta a segurança energética, alimentar, hídrica e a segurança humana, em

geral. A transição demográfica, com o envelhecimento da população e novos fluxos migratórios, pressiona a coesão social e a sustentabilidade fiscal. A revolução tecnológica, por sua vez, introduz fatores de ameaça, como a iminente quebra da criptografia pela computação quântica e a centralidade da inteligência artificial para os processos



de gestão, produção e inovação, desafiando a própria noção de soberania digital.

Essas dinâmicas interdependentes são amplificadas pela instabilidade geopolítica, que pressiona a tradicional política externa de equilíbrio do Brasil. O colapso da arquitetura de governança do pós-guerra deu lugar a uma multipolaridade desequilibrada e desinstitucionalizada, cujo eixo central é a competição estratégica entre EUA e China. Ao longo do último ano, aprofundou-se a securitização de domínios antes hegemônicos por uma superpotência, como a economia e a tecnologia, transformando cadeias de suprimentos, o ciberespaço e a corrida pela inovação em arenas mais competitivas. A estabilidade geopolítica do Brasil e sua posição internacional equilibrada emergem como ativos valiosos.

A instabilidade global se projeta diretamente sobre o entorno estratégico brasileiro. A América do Sul, detentora de recursos vitais no contexto das transições globais (lítio, petróleo, terras raras, biodiversidade), tornou-se um palco para esta competição assimétrica. A região enfrenta pressões por alinhamentos e está exposta à interferência de potências extrarregionais, que exploram fragilidades internas — como dissidências políticas e o avanço do crime organizado — sob pretextos securitários (como o “narcoterrorismo”) para minar a soberania e a autodeterminação política.

O Brasil enfrenta um paradoxo: enquanto sua projeção global é reativada (BRICS, G20), sua influência regional imediata, essencial para a autonomia, permanece limitada por dissonâncias políticas. Há dificuldades para retomar as iniciativas multilaterais sul-americanas, o que impede a construção de posições conjuntas estáveis. Nesse contexto, a integração da infraestrutura física, como o Corredor Bioceânico, que conecta as duas frentes principais do entorno estratégico brasileiro, emerge como vetor pragmático para a coope-

ração, oferecendo alternativas para a segurança econômica diante de choques externos, como a imposição de tarifas unilaterais.

Se o cenário atual impõe balizas e obstáculos para o exercício da autonomia estratégica do Brasil, os desafios de Inteligência avaliados no último capítulo sinalizam caminhos para preservar e potencializar tal autonomia. A Atividade de Inteligência, tal como regulamentada e praticada no Brasil, destina-se, primordialmente, a prover informações confiáveis necessárias ao processo decisório das autoridades do país e a proteger informações sensíveis, cuja revelação possa prejudicar o atingimento dos objetivos nacionais, consignados pela Constituição Federal. Nesse sentido, compartilhar a avaliação desses desafios com a sociedade contribui para o atingimento dos objetivos da Inteligência sob o mandato constitucional, legal e normativo da Atividade.

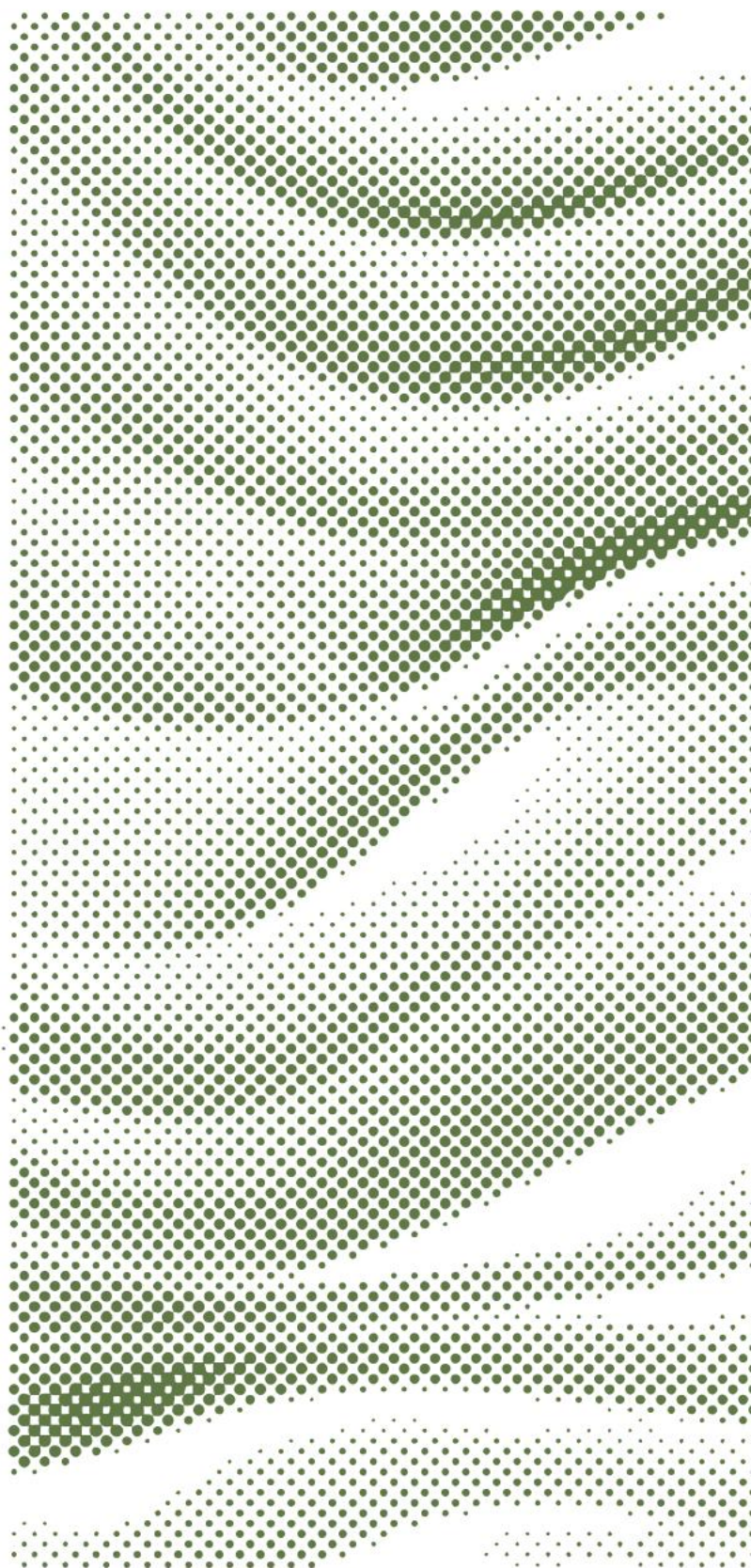
Para 2026, avalia-se que existem ameaças e vulnerabilidades significativas — mas também oportunidades — em relação à segurança do processo eleitoral, à transição para a criptografia pós-quântica, aos ataques cibernéticos autônomos com uso de IA, à reconfiguração das cadeias de suprimentos globais e à interferência externa por atores não estatais.

A natureza complexa dos desafios identificados impõe a cooperação efetiva entre os órgãos do Sistema Brasileiro de Inteligência. À ABIN, na sua função de órgão central e facilitador, compete articular iniciativas que fortaleçam as capacidades estatais e o controle democrático da Atividade. A magnitude espacial e temporal dos fenômenos exige, ademais, a interlocução permanente com especialistas externos ao Sistema e o aprimoramento contínuo das capacidades de análise prospectiva.

As transições globais e a situação internacional condicionarão as próximas décadas, mas o



futuro permanece dependente da ação humana — particularmente das dinâmicas de cooperação, conflito e securitização promovidas pelas grandes potências e pelos demais atores do sistema internacional. Para o Brasil, os compromissos com a paz, o multilateralismo e o respeito à soberania apresentam vantagens estratégicas superiores a qualquer alinhamento a um polo de poder. Em linha com seus preceitos constitucionais, o país atua pela integração regional e pela construção de uma sociedade sustentável, inovadora e justa.





ABIN

A Agência Brasileira de Inteligência (ABIN) é um órgão de Estado permanente, apartidário e apolítico, vinculado à Casa Civil da Presidência da República. Com atuação nacional e representações no exterior, a ABIN é responsável por fornecer ao Presidente da República e a seus ministros informações e análises estratégicas, oportunas e confiáveis, úteis para os processos de decisão do Governo Federal.

As atividades de Inteligência da ABIN são desenvolvidas com irrestrita observância aos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado brasileiro. Constituem fundamentos de sua ação a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana.

Na condição de órgão coordenador do Sistema Brasileiro de Inteligência (Sisbin), a ABIN tem por missão assegurar que o Poder Executivo Federal tenha acesso a conhecimentos relativos à segurança do Estado e da sociedade, como os que envolvem defesa nacional, relações exteriores, segurança interna, desenvolvimento socioeconômico e desenvolvimento científico-tecnológico.



Para cumprir essa missão institucional, os profissionais de Inteligência produzem conhecimentos estratégicos por meio da análise de fatos, eventos ou situações que permitam a identificação de oportunidades e ameaças relacionadas à proteção das fronteiras nacionais, à segurança de infraestruturas críticas, à contraespionagem, ao terrorismo, à proliferação de armas de destruição de massa, a políticas estabelecidas com outros países ou regiões, à segurança das informações e das comunicações, à defesa do meio ambiente, à proteção de conhecimentos sensíveis produzidos por entes públicos ou privados, entre outros assuntos atualizados periodicamente.

Além da produção de conhecimentos, a ABIN ainda fornece serviços ao Estado e à sociedade brasileiros, tais como criptografia de Estado, serviços de comunicação segura, capacitação em Inteligência para os profissionais e consultoria em segurança por intermédio do Programa Nacional de Proteção do Conhecimento Sensível (PNPC).

A ABIN seleciona seus profissionais por meio de concurso público e a aprovação em certame é requisito necessário para o ingresso nas carreiras de Inteligência. O processo de admissão compreende, entre outras etapas, avaliação de conhecimentos, investigação social e aprovação no Curso de Formação em Inteligência.

Publicações



Doutrina da Atividade de Inteligência

A atual Doutrina da Atividade de Inteligência foi publicada em novembro de 2023 e é a primeira que a ABIN disponibiliza amplamente ao público. A Doutrina define e explicita os entendimentos que a ABIN tem hoje sobre a atividade de Inteligência e como ela deve ser praticada pela Agência no Brasil, tendo por parâmetros a Constituição Federal e a legislação. Ela registra entendimentos conceituais que fornecem base prescritiva comum para o agir.

<https://www.gov.br/abin/pt-br/centrais-de-conteudo/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023>



Desafios de Inteligência

Desafios de Inteligência é um documento público anual preparado pela ABIN que mobiliza recursos de pesquisa e análise prospectiva para avaliar os principais riscos à segurança das pessoas e das instituições no Brasil no próximo ano, considerando quatro dimensões: global, internacional, regional e nacional.

<https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/desafios-de-inteligencia>



Revista Brasileira de Inteligência

A Revista Brasileira de Inteligência (RBI) é uma revista científica dedicada ao avanço do conhecimento sobre as concepções, processos, práticas, relações, estruturas e organizações relacionadas à Atividade de Inteligência. É publicada desde 2005 pela ABIN. De acesso aberto, a RBI é receptiva às contribuições de pesquisadores e pesquisadoras com diferentes origens e perspectivas, tendo como base comum o rigor científico e a honestidade intelectual.

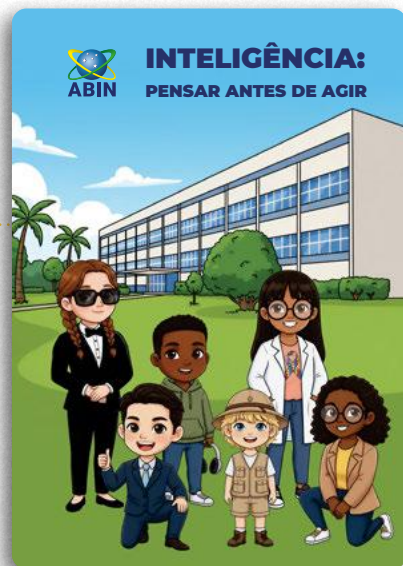
<https://rbi.abin.gov.br>



Série Inteligência e Memória

Em 2024, a Escola de Inteligência da ABIN iniciou a publicação de uma série editorial sobre Inteligência e memória institucional. O primeiro livro, "Inteligência na Democracia: desafios e perspectivas para a Agência Brasileira de Inteligência", é uma coletânea com capítulos escritos por profissionais de Inteligência e acadêmicos renomados. O segundo livro, "Memórias da Pandemia: a atuação da ABIN no enfrentamento à COVID-19 (2020-2021)", traz relatos de servidores e documentos desclassificados para contar como a ABIN se organizou e atuou para auxiliar os esforços da sociedade brasileira, de forma profissional íntegra, em um momento de grave crise global.

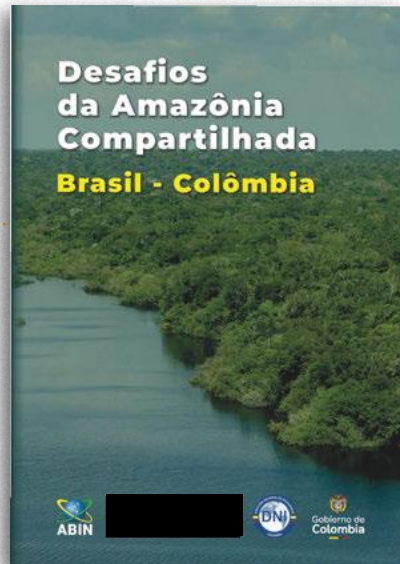
<https://repositorio.enap.gov.br/handle/1/8217>
<https://repositorio.enap.gov.br/handle/1/8544>



Inteligência: Pensar Antes de Agir

Voltada para o público infantil, a revistinha explica em linguagem palatável o que é Inteligência, Contrainteligência, quais profissionais atuam na ABIN e como é seu trabalho. Também dá exemplos concretos e diferencia a Atividade de Inteligência de outras, como a policial e a jornalística. A iniciativa busca consolidar o que se chama cultura de Inteligência, assumindo postura pública de transparência ativa por meio da promoção de abertura de espaços de interação com a sociedade. Os exemplares físicos são disponibilizados aos visitantes do Museu da Inteligência.

<https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/cartilha-institucional-1/inteligencia-pensar-antes-de-agir>



Desafios da Amazônia Compartilhada Brasil-Colômbia

Relatório público elaborado em colaboração com a *Dirección Nacional de Inteligencia* (DNI) da Colômbia. O relatório apresenta diagnóstico, análise dos impactos para a segurança humana e o meio ambiente e as tendências das principais ameaças transnacionais presentes na Amazônia Compartilhada Brasil-Colômbia: o narcotráfico, a mineração ilegal de ouro e o contrabando de migrantes. O trabalho é um esforço para enfrentar conjuntamente, desde uma perspectiva sul-americana, os desafios transnacionais de um território vasto e complexo, cada vez mais relevante, sobretudo em face da mudança climática, e inserido nas dinâmicas geopolíticas da atualidade.

<https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/desafios-da-amazonia-compartilhada/desafios-da-amazonia-compartilhada>



Mercúrio na Amazônia: redes criminosas transnacionais, vulnerabilidade socioambiental e desafios para a governança

Relatório público elaborado em colaboração com o Fórum Brasileiro de Segurança Pública (FBSP) e o Ministério do Meio Ambiente e Mudança do Clima. O estudo sistematiza e aprofunda o entendimento sobre as dinâmicas do contrabando de mercúrio e seu uso na mineração ilegal de ouro, a partir da integração de dados de campo, fontes abertas e análises institucionais. Trata-se do primeiro de uma série de estudos conjuntos ABIN-FBSP voltados à análise de temas estratégicos para a segurança pública e a soberania nacional.

<https://publicacoes.forumseguranca.org.br/handle/123456789/284>



PNPC

Programa Nacional de Proteção do Conhecimento Sensível

O Programa Nacional de Proteção do Conhecimento Sensível (PNPC) é uma consultoria de segurança com foco na prevenção de espionagem, sabotagem e vazamento de informações. Desde 1997, busca promover a proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas. O PNPC atua na sensibilização de pessoas, na identificação de ameaças e vulnerabilidades em sistemas de proteção e na apresentação de recomendações para redução de risco de incidentes. O PNPC publica uma série de guias de boas práticas, disponíveis na página do programa.

<https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC>



Se sua instituição é detentora de conhecimentos sensíveis e necessita aumentar o nível de proteção, entre em contato pelo e-mail pnpc@abin.gov.br.

Para reportar casos de suspeitas de espionagem ou sabotagem em sua instituição, envie um e-mail para reporte@abin.gov.br.





Notas

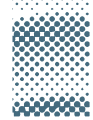
Para a elaboração de notas e referências, foi adotado o estilo do *Chicago Manual of Style* (notas e bibliografia), 17ª edição.

01 | Transições Globais

- ¹ Ministério do Planejamento e Orçamento, *Megatendências Mundiais e Incertezas para o Brasil 2050* (Brasília: MPO, 2025), <https://www.gov.br/planejamento/pt-br/assuntos/planejamento/estrategia-2050-conteudo/Arquivos/eb2050-megatendencias-mundiais-e-incertezas-para-o-brasil-2050-v-abr.pdf>; Elaine Marcial, Márcio Gimene e Marcello José Pio, *Cenários Brasil 2045* (Brasília: Assecor; ProcadDefesa, 2025), 67–73, https://socialport.com.br/wp-content/uploads/2025/07/Livro_Cenarios_Brasil_2045_web.pdf.
- ² União Europeia (UE), “Global Climate Highlights 2024,” 10 de janeiro de 2025, <https://climate.copernicus.eu/sites/default/files/custom-uploads/GCH-2024/GCH2024-PDF-1.pdf>.
- ³ Organização Meteorológica Mundial (WMO), “WMO Confirms 2024 as Warmest Year on Record at about 1.55°C above Pre-industrial Level,” 10 de janeiro de 2025, <https://wmo.int/news/media-centre/wmo-confirms-2024-warmest-year-record-about-155degc-above-pre-industrial-level>.
- ⁴ Organização Meteorológica Mundial (WMO), *Global Annual to Decadal Climate Update 2025* (maio de 2025), https://wmo.int/sites/default/files/2025-05/WMO_GADCU_2025-2029_Final.pdf.



- ⁵ Jakob Deutloff, Hermann Held e Timothy M. Lenton, "High Probability of Triggering Climate Tipping Points under Current Policies Modestly Amplified by Amazon Dieback and Permafrost Thaw," *Earth System Dynamics* 16 (2025): 565–583, <https://doi.org/10.5194/esd-16-565-2025>.
- ⁶ Nico Wunderling et al., "Climate Tipping Point Interactions and Cascades: A Review," *Earth System Dynamics* 15 (2024): 60, <https://doi.org/10.5194/esd-15-41-2024>.
- ⁷ Centro Soberania e Clima, "Defesa e Meio Ambiente: A Atuação das Forças Armadas em Meio à Crise Climática," 06 de dezembro de 2023, <https://soberaniaeclima.org.br/wp-content/uploads/2024/01/Relatorio-Defesa-e-Meio-Ambiente.pdf>.
- ⁸ E3G, "Trends in Climate and Geopolitics for 2025," 14 de janeiro de 2025, <https://www.e3g.org/news/trends-in-climate-and-geopolitics-for-2025/>.
- ⁹ Aliança Brasileira pela Cultura Oceânica, "2024: O Ano Mais Quente da História," dezembro de 2024, <https://maredeciencia.eco.br/wp-content/uploads/2024/12/Brasil-em-transformacao-1-2024-o-ano-mais-quente-da-historia.pdf>.
- ¹⁰ ACAPS, "Brazil: Impact of Drought in the Brazilian Amazon and 2025 Outlook," 28 de janeiro de 2025, [https://www.acaps.org/fileadmin/Data_Product/Main_media/20250128_ACAPS_BRAZIL - Impact of Drought in the Brazilian Amazon and 2025 Outlook .pdf](https://www.acaps.org/fileadmin/Data_Product/Main_media/20250128_ACAPS_BRAZIL_-_Impact_of_Drought_in_the_Brazilian_Amazon_and_2025_Outlook_.pdf).
- ¹¹ Governo do Estado do Rio Grande do Sul, "Defesa Civil Atualiza Balanço das Enchentes no RS," 20 de agosto de 2024, <https://www.estado.rs.gov.br/defesa-civil-atualiza-balanco-das-enchentes-no-rs-20-8>.
- ¹² Xinke Song et al., "A Systematic Review of the Inequality of Health Burdens Related to Climate Change," *Frontiers of Environmental Science & Engineering* 18, no. 63 (2024), <https://doi.org/10.1007/s11783-024-1823-4>.
- ¹³ Empresa de Pesquisa Energética (EPE), *Balanço Energético Nacional: Relatório Síntese 2025 (Ano base 2024)*, 28 de maio de 2025, https://www.epe.gov.br/sites-pt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-885/topico-767/BEN_S%C3%ADntese_2025_PT.pdf.
- ¹⁴ Empresa de Pesquisa Energética (EPE), *Balanço Energético Nacional: Relatório Síntese 2022 (Ano base 2021)*, maio de 2021, https://www.epe.gov.br/sites-pt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-675/topico-631/BEN_S%C3%ADntese_2022_PT.pdf.
- ¹⁵ Gustavo R. S. Pinto e João Pedro F. Arbach, *O Desmatamento Corta a Luz: Itaipu, Belo Monte e o Preço da Floresta Perdida* (Rio de Janeiro: Climate Policy Initiative/PUC-Rio, 2025), <https://www.climatepolicyinitiative.org/wp-content/uploads/2025/03/O-Desmatamento-Corta-a-Luz.pdf>.
- ¹⁶ Associação Rio-Grandense de Empreendimentos de Assistência Técnica e Extensão Rural (Emater/RS), "Impactos das Chuvas e Cheias Extremas no Rio Grande do Sul em Maio de 2024," maio de 2024, <https://www.estado.rs.gov.br/upload/arquivos/202406/relatorio-sisperdas-evento-enchentes-em-maio-2024.pdf>.
- ¹⁷ InfoAmazonia, "Seca Atinge 69% dos Municípios da Amazônia em 2024," 9 de agosto de 2024, <https://infoamazonia.org/2024/08/09/seca-atinge-69-dos-municipios-da-amazonia-em-2024/>.



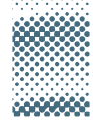
- ¹⁸ Banco Internacional para Reconstrução e Desenvolvimento (BIRD), "Brasil: Relatório sobre Clima e Desenvolvimento para o País (2023)," <https://openknowledge.worldbank.org/server/api/core/bitstreams/af026935-5f2d-4edd-b19e-d8fb66f6e9da/content>.
- ¹⁹ Francislene Angelotti, Emília Hamada e Wagner Bettiol, "A Comprehensive Review of Climate Change and Plant Diseases in Brazil," *Plants* 13, no. 17 (2024): 2447, <https://doi.org/10.3390/plants13172447>.
- ²⁰ Empresa Brasileira de Pesquisa Agropecuária (Embrapa), "Doenças em Lavouras Devem se Intensificar com as Mudanças Climáticas, Alerta Embrapa," 15 de abril de 2025, <https://www.embrapa.br/busca-de-noticias/-/noticia/99781504/doencas-em-lavouras-devem-se-intensificar-com-as-mudancas-climaticas-alerta-embrapa>.
- ²¹ CNN Brasil, "Após Cinco Meses Fechado, Aeroporto de Porto Alegre Retoma Operação Comercial Nesta Segunda-feira," 21 de outubro de 2024, <https://www.cnnbrasil.com.br/nacional/apos-cinco-meses-fechado-aeroporto-de-porto-alegre-retoma-operacao-comercial-nesta-segunda-feira/>.
- ²² Banco Central do Brasil (BCB), *Relatório de Riscos e Oportunidades Sociais, Ambientais e Climáticos*, Vol. 4 (agosto de 2024), https://www.bcb.gov.br/content/publicacoes/relatorio-risco-oportunidade/Relatorio-Riscos-Oportunidades-Sociais_2024.pdf.
- ²³ National Aeronautics and Space Administration (NASA), "NASA Analysis Shows Unexpected Amount of Sea Level Rise in 2024," 13 de março de 2025, <https://sealevel.nasa.gov/news/282/nasa-analysis-shows-unexpected-amount-of-sea-level-rise-in-2024>.
- ²⁴ Igor Vieira Ferreira e Caio Belandi, "Censo 2022: Informações de População e Domicílios por Setores Censitários Auxiliam Gestão Pública," *Agência IBGE*, 21 de março de 2024, <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/39525-censo-2022-informacoes-de-populacao-e-domicilios-por-setores-censitarios-auxiliam-gestao-publica>; Diana Meirelles da Motta, Ederson Nascimento e Fernando Luiz Araújo Sobrinho, "Urbanização e Cidades Médias da Fronteira Litorânea: Desafios e Recomendações para a Política Pública Urbana," in *Fronteiras do Brasil: O Litoral em Sua Dimensão Fronteiriça*, vol. 8, orgs. Bolívar Pêgo, Lília Nagamine, Carolina Krüger e Rosa Moura (Brasília: IPEA, 2023), 103.
- ²⁵ Instituto Brasileiro de Geografia e Estatística (IBGE), "Censo 2022: Informações de População e Domicílios por Setores Censitários Auxiliam Gestão Pública," *Agência IBGE*, 21 de março de 2024, <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/39525-censo-2022-informacoes-de-populacao-e-domicilios-por-setores-censitarios-auxiliam-gestao-publica>.
- ²⁶ ACAPS, "Brazil: Impact of Drought in the Brazilian Amazon and 2025 Outlook," 28 de janeiro de 2025, [https://www.acaps.org/fileadmin/Data_Product/Main_media/20250128_ACAPS_BRAZIL - Impact of Drought in the Brazilian Amazon and 2025 Outlook .pdf](https://www.acaps.org/fileadmin/Data_Product/Main_media/20250128_ACAPS_BRAZIL_-_Impact_of_Drought_in_the_Brazilian_Amazon_and_2025_Outlook_.pdf).
- ²⁷ Eliza Pan, "Reimagining the Climate Migration Paradigm: Bridging Conceptual Barriers to Climate Migration Responses," *Environmental Law* 50, no. 4 (2020): 1173–1225, <https://www.jstor.org/stable/27010196>.



- ²⁸ Michael Oppenheimer et al., "Sea Level Rise and Implications for Low-Lying Islands, Coasts and Communities," in *IPCC Special Report on the Ocean and Cryosphere in a Changing Climate*, eds. Hans-Otto Pörtner et al. (Cambridge: Cambridge University Press, 2019), 321–445, <https://doi.org/10.1017/9781009157964.006>.
- ²⁹ Ministério da Fazenda, "Fundo Florestas Tropicais para Sempre," <https://www.gov.br/fazenda/pt-br/aceso-a-informacao/acoes-e-programas/transformacao-ecologica/programas-em-destaque/fundo-florestas-tropicais>.
- ³⁰ Organização das Nações Unidas (ONU), *World Fertility 2024* (6 de maio de 2025), https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesapd_2025_wfr_2024_final.pdf.
- ³¹ Instituto Brasileiro de Geografia e Estatística (IBGE), "Brasil em Síntese," <https://brasilemsintese.ibge.gov.br/populacao/taxas-de-fecundidade-total.html>.
- ³² Ministério do Planejamento e Orçamento (MPO), *Megatendências Mundiais e Incertezas para o Brasil 2050* (Brasília: Governo Federal, abril de 2025), <https://www.gov.br/planejamento/pt-br/assuntos/planejamento/estrategia-2050-conteudo/noticias/eb2050-megatendencias-mundiais-e-incertezas-para-o-brasil-2050-v-abr.pdf>.
- ³³ Departamento de Assuntos Econômicos e Sociais, Organização das Nações Unidas (DESA-ONU), "World Population Prospects - Africa," <https://population.un.org/wpp/graphs?loc=903&type=Demographic%20Profiles&category=Line%20Charts>.
- ³⁴ Conrad Hackett et al., *How the Global Religious Landscape Changed From 2010 to 2020* (Washington, EUA: Pew Research Center, 2025), <https://doi.org/10.58094/fj71-ny11>.
- ³⁵ Organização Mundial de Saúde (WHO), *World Health Statistics 2025* (Genebra: WHO, 2025), <https://iris.who.int/bitstream/handle/10665/381418/9789240110496-eng.pdf?sequence=1>.
- ³⁶ Ministério do Planejamento e Orçamento (MPO), *Megatendências Mundiais e Incertezas para o Brasil 2050* (Brasília: Governo Federal, abril de 2025), <https://www.gov.br/planejamento/pt-br/assuntos/planejamento/estrategia-2050-conteudo/noticias/eb2050-megatendencias-mundiais-e-incertezas-para-o-brasil-2050-v-abr.pdf>.
- ³⁷ Instituto Brasileiro de Geografia e Estatística (IBGE), "Censo 2022: Número de Pessoas com 65 Anos ou Mais de Idade Cresceu 57,4% em 12 Anos," *Agência IBGE Notícias*, 27 de outubro de 2023, <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38186-censo-2022-numero-de-pessoas-com-65-anos-ou-mais-de-idade-cresceu-57-4-em-12-anos>.
- ³⁸ Parlamento Europeu (European Parliament 2019-2024), "Harnessing Talent in Europe's Regions," Resolução de 23 de novembro de 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0439_EN.pdf.
- ³⁹ Kohei Komamura e Shohei Okamoto, "Towards Universal Health Coverage in the Context of Population Ageing: A Narrative Review on the Implications from the Long-term Care System in Japan," *Archives of Public Health* 80, no. 210 (2022), <https://doi.org/10.1186/s13690-022-00970-8>.



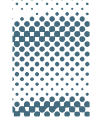
- ⁴⁰ Natasha Roya Matthews et al., "Health and Socioeconomic Resource Provision for Older People in South Asian Countries: Bangladesh, India, Nepal, Pakistan and Sri Lanka Evidence from NEESAMA," *Global Health Action* 16, no. 1 (2023), <https://www.tandfonline.com/doi/full/10.1080/16549716.2022.2110198#abstract>.
- ⁴¹ Organização para a Cooperação e Desenvolvimento Econômico (OCDE), *International Migration Outlook 2024* (Paris: OECD Publishing, 2024), 87–88, <https://doi.org/10.1787/50b0353e-en>.
- ⁴² Douglas Broom, "Migrant Workers Sent Home Almost \$800 Billion in 2022. Which Countries Are the Biggest Recipients?," *World Economic Forum*, 2 de fevereiro de 2023, <https://www.weforum.org/stories/2023/02/remittances-money-world-bank/>.
- ⁴³ Department of Citizenship and Immigration - Government of Canada, "Immigration and Refugee Protection Act, Canada Gazette," 01 de dezembro de 2014, <https://gazette.gc.ca/rp-pr/p1/2014/2014-12-01-x10/html/extra10-eng.html>.
- ⁴⁴ Department of Home Affairs – Australian Government, "Immigration and Citizenship – Skill Select," 04 de julho de 2025, <https://immi.homeaffairs.gov.au/visas/working-in-australia/skillselect>.
- ⁴⁵ Vinícius Britto, "Censo 2022: Número de Imigrantes Volta a Crescer Pela Primeira Vez Desde 1960," *Agência IBGE Notícias*, 27 de junho de 2025, <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/43816-censo-2022-numero-de-imigrantes-volta-a-crescer-pela-primeira-vez-desde-1960>.
- ⁴⁶ Ministério da Ciência, Tecnologia e Inovação (MCTI), "CNPq Divulga Resultado da Chamada Conhecimento Brasil Para Atração e Fixação de Talentos Científicos," 4 de junho de 2025, <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2025/06/cnpq-divulga-resultado-da-chamada-conhecimento-brasil-para-atracao-e-fixacao-de-talentos-cientificos-2>.
- ⁴⁷ Maria Andreia Parente Lameiras et al., *Carta de Conjuntura* 68, nota 19 (Instituto de Pesquisa Econômica Aplicada, 3º trimestre de 2025), https://www.ipea.gov.br/cartadeconjuntura/wp-content/uploads/2025/09/250924_cc_68_nota_19_mt_set_25.pdf.
- ⁴⁸ Marco Arena et al., "Os Migrantes da Venezuela Trazem Oportunidades Econômicas Para a América Latina," *International Monetary Fund*, 19 de dezembro de 2022, <https://www.imf.org/pt/News/Articles/2022/12/06/cf-venezuelas-migrants-bring-economic-opportunity-to-latin-america>.
- ⁴⁹ Vitor Abdala, "Venezuelanos São Maior Grupo de Imigrantes do Brasil," *Agência Brasil*, 27 de junho de 2025, <https://agenciabrasil.ebc.com.br/geral/noticia/2025-06/venezuelanos-sao-maior-grupo-de-imigrantes-do-brasil>.
- ⁵⁰ Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS), "Operação Acolhida Alcança Marco de 150 Mil Venezuelanos Interiorizados no Brasil," *Agência Gov*, 24 de junho de 2025, <https://www.gov.br/mds/pt-br/noticias-e-conteudos/desenvolvimento-social/noticias-desenvolvimento-social/operacao-acolhida-alcanca-marco-de-150-mil-venezuelanos-interiorizados-no-brasil>.



- ⁵¹ Mariana Sanches, "Haitianos Deixam Brasil em Meio à Crise Econômica e Fake News Sobre Fronteira Aberta nos EUA," *Folha de São Paulo*, 11 de março de 2021, <https://www1.folha.uol.com.br/mundo/2021/03/haitianos-deixam-brasil-em-meio-a-cri-se-economica-e-fake-news-sobre-fronteira-aberta-nos-eua.shtml>.
- ⁵² Danielle Annoni, *Direito Internacional dos Refugiados e o Brasil* (Curitiba: GEDAI/UFPR, 2018), https://gedai.ufpr.br/wp-content/uploads/2018/08/livro_Direito-Internacional-dos-Refugiados_FIINAL_compressed.pdf.
- ⁵³ Ministério da Saúde (MS), "Saúde Lança Nota Técnica com Orientações de Atendimento a Migrantes, Refugiados e Apátridas," 9 de setembro de 2024, <https://www.gov.br/saude/pt-br/assuntos/noticias/2024/abril/saude-lanca-nota-tecnica-com-orientacoes-de-atendimento-a-migrantes-refugiados-e-apatridas>.
- ⁵⁴ Gisele R. Winck et al., "Socioecological Vulnerability and the Risk of Zoonotic Disease Emergence in Brazil," *Science Advances* 8, no. 26 (29 de junho de 2022), <https://doi.org/10.1126/sciadv.abo5774>.
- ⁵⁵ Ministério da Saúde, "Planos de Contingência," <https://www.gov.br/saude/pt-br/composicao/svsa/resposta-a-emergencias/planos-de-contingencia>.
- ⁵⁶ Ministério da Saúde, "Centro de Informações Estratégicas em Vigilância em Saúde," <https://www.gov.br/saude/pt-br/composicao/svsa/cievs>.
- ⁵⁷ Agência Brasileira de Inteligência (ABIN), *Memórias da Pandemia: A Atuação da Agência Brasileira de Inteligência no Enfrentamento à COVID-19 (2020-2021)* (Brasília: ABIN, 2025), https://repositorio.enap.gov.br/bitstream/1/8544/1/ABIN_Memorias_da_pandemia_compressed.pdf.
- ⁵⁸ Fórum Brasileiro de Segurança Pública (FBSP), *Segurança Pública e Crime Organizado na Amazônia Legal: Informe Especial* (junho de 2023), <https://forumseguranca.org.br/wp-content/uploads/2023/06/informe-especial-seguranca-publica-e-crime-organizado-na-amazonia-legal.pdf>.
- ⁵⁹ Organização para a Cooperação e Desenvolvimento Econômico (OCDE), *Space Economy Investment Trends: OECD Insights for Attracting High-Quality Funding* (2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/space-economy-investment-trends_7eafcb97/9ae9a28d-en.pdf.
- ⁶⁰ Fórum Econômico Mundial, *Transitioning to a Quantum-Secure Economy* (2022), https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf.
- ⁶¹ Stephen Coulthart, "Disruptive Technologies and Intelligence Services: A Framework for Adoption in the Digital Age," *Intelligence and National Security* (2025): 4. <https://doi.org/10.1080/02684527.2025.2565953>.
- ⁶² John Villasenor, "The Tension Between AI Export Control and U.S. AI Innovation," *Brookings Tech Tank Commentary*, 24 de setembro de 2024, <https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation/>.
- ⁶³ Gregory C. Allen, *DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race* (Washington: Center for Strategic & International Studies, 2025), <https://www.csis.org/analysis/deepseek-huawei-export-controls-and-future-us-china-ai-race>.



- ⁶⁴ Raúl L Katz, *Oportunidades para la Transformación Digital Productiva: Evidencia Estadística sobre el Nivel de Digitalización Sectorial en América Latina y el Caribe* (Santiago: CEPAL/ONU, 2024), <https://repositorio.cepal.org/server/api/core/bitstreams/3f91f0ea-bd6f-493c-95b8-19306dad70e/content>.
- ⁶⁵ Center for Industrial Development and Environmental Governance (CIDE), *Global Innovation Hubs Index 2024* (CIDE, Tsinghua University; Nature Research Intelligence, 2024), <https://www.nature.com/articles/d42473-024-00457-w>.
- ⁶⁶ Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26, <https://doi.org/10.1177/0306396818823172>.
- ⁶⁷ Fórum Econômico Mundial, "What Is Digital Sovereignty and How Are Countries Approaching It?," 10 de janeiro de 2025, <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>; Germano Johansson e James Görgen, "O Sequestro da Soberania Digital," *JOTA Jornalismo*, 27 de junho de 2025, <https://www.jota.info/opiniao-e-analise/artigos/o-sequestro-da-soberania-digital>.
- ⁶⁸ Governo da República da Estônia, "The Heads of Government of Germany, Denmark, Estonia, and Finland: Europe's Digital Sovereignty Gives Us the Ability to Shape Our Own Future," 2 de março de 2021, <https://www.valitsus.ee/en/news/heads-government-germany-denmark-estonia-and-finland-europes-digital-sovereignty-gives-us>.
- ⁶⁹ Agência Brasil, "Turma do Supremo Vota para Manter X Suspenso no Brasil," 2 de setembro de 2024, <https://agenciabrasil.ebc.com.br/justica/noticia/2024-09/turma-do-supremo-vota-para-manter-x-suspenso-no-brasil>.
- ⁷⁰ Luís Osvaldo Rossmann, "Dependente de Big Techs, Brasil é 45º em Ranking Global de Soberania Digital," *Convergência Digital*, 11 de agosto de 2025, <https://convergenciadigital.com.br/governo/dependente-de-big-techs-brasil-e-45o-em-ranking-global-de-soberania-digital/>; Sergio Queiroz e Denise Direito, *Inteligência Artificial nos Países do BRICS: Soberania, Estágios de Desenvolvimento e Diferentes Perspectivas* (Rio de Janeiro: IPEA, 2025).
- ⁷¹ Alexandre Reis Siqueira Freire, coord., *White Paper Data Centers* (Brasília: Agência Nacional de Telecomunicações, 2025), 34, <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-lanca-white-paper-sobre-o-papel-estrategico-dos-data-centers-no-ecossistema-digital-brasileiro/white-paper.pdf/>.
- ⁷² Victor H. L. de Mello, "Soberania Digital Brasileira: Estratégias para o Futuro Autônomo," *Portal Migalhas*, 23 de junho de 2025, <https://www.migalhas.com.br/depeso/433038/soberania-digital-brasileira-estrategias-para-o-futuro-autonomo>.
- ⁷³ IT Forum, "Infraestrutura Crítica Brasileira Está Sob Ameaça de Ciberataques," 25 de abril de 2024, <https://itforum.com.br/noticias/infraestrutura-critica-br-ciberataques>.
- ⁷⁴ União Internacional de Telecomunicações (UIT), *Global Cybersecurity Index 2024* (2024), https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.



⁷⁵ BRICS, "BRICS Fortalece Cooperação em Segurança Cibernética," 11 de abril de 2025, <https://brics.br/pt-br/noticias/brics-fortalece-cooperacao-em-seguranca-cibernetica>.

02 | Situação internacional

⁷⁶ Escritório do Diretor de Inteligência Nacional (ODNI), *Global Trends 2040: A More Contested World* (2021), https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

⁷⁷ Gabriel Corrêa, "Com Corte do Financiamento, ONU Anuncia Redução na Ajuda Humanitária," *Agência Brasil*, 16 de junho de 2025, <https://agenciabrasil.ebc.com.br/radioagencia-nacional/internacional/audio/2025-06/com-corte-do-financiamento-onu-anuncia-reducao-na-ajuda-humanitaria>.

⁷⁸ Mariel Ferragamo e Diana Roy, "How Much Does the U.S. Fund the United Nations?," *Council on Foreign Relations*, 25 de setembro de 2025, <https://www.cfr.org/article/funding-united-nations-what-impact-do-us-contributions-have-un-agencies-and-programs>.

⁷⁹ Richard Haass, "The Dangerous Decade: A Foreign Policy for a World in Crisis," *Foreign Affairs* 102, no. 5 (2022), <https://www.foreignaffairs.com/united-states/dangerous-decade-foreign-policy-world-crisis-richard-haass>.

⁸⁰ Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), *Trade and Development Report 2024: Rethinking Development in the Age of Discontent* (2024), https://unctad.org/system/files/official-document/tdr2024_en.pdf.

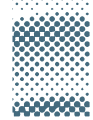
⁸¹ Edward Fishman, *Chokepoints: American Power in the Age of Economic Warfare* (Nova York: Portfolio/Penguin, 2025).

⁸² Gregory C. Allen, *DeepSeek, Huawei, Export Controls, and the Future of the U.S.-China AI Race* (Washington: Center for Strategic & International Studies, 2025), <https://www.csis.org/analysis/deepseek-huawei-export-controls-and-future-us-china-ai-race>.

⁸³ Ministério das Relações Exteriores, "Declaração de Líderes do BRICS," Rio de Janeiro, 6 de julho de 2025, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/declaracao-de-lideres-do-brics-2014-rio-de-janeiro-06-de-julho-de-2025.

⁸⁴ Lucas Pordeus León, "Big Techs dos EUA Influenciaram Sanção de Trump Contra o Brasil," *Agência Brasil*, 10 de julho de 2025, <https://agenciabrasil.ebc.com.br/internacional/noticia/2025-07/big-techs-dos-eua-influenciaram-sancao-de-trump-contr-o-brasil>; Pedro Rafael Vilela, "Em Carta a Lula, Trump Anuncia Tarifa de 50% a Produtos Brasileiros," *Agência Brasil*, 9 de julho de 2025, <https://agenciabrasil.ebc.com.br/internacional/noticia/2025-07/em-carta-lula-trump-anuncia-tarifa-de-50-produtos-brasileiros>.

⁸⁵ Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos (UN OHCHR), "US Attacks in Caribbean and Pacific Violate International Human Rights Law — UN Human Rights Chief," 31 de outubro de 2025, <https://www.ohchr.org/en/press-releases/2025/10/us-attacks-caribbean-and-pacific-violate-international-human-rights-law-un>.



- ⁸⁶ Julian Barnes e Tyler Pager, "Trump Administration Authorizes Covert C.I.A. Action in Venezuela," *The New York Times*, 15 de outubro de 2025, <https://www.nytimes.com/2025/10/15/us/politics/trump-covert-cia-action-venezuela.html>.
- ⁸⁷ Instituto Internacional de Pesquisa para a Paz de Estocolmo (SIPRI), *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (2025), https://www.sipri.org/sites/default/files/2025-08/yb25_summary_en_v2.pdf.
- ⁸⁸ Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2025: Armaments, Disarmament and International Security*, Summary (Solna, Suécia: SIPRI, 2025), 1, 10, 19.
- ⁸⁹ Laura Bruun e Marta Bo, *Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law* (Solna, Suécia: SIPRI, 2025).
- ⁹⁰ Instituto Internacional de Pesquisa para a Paz de Estocolmo (SIPRI), *SIPRI Yearbook 2025: Armaments, Disarmament and International Security* (2025), https://www.sipri.org/sites/default/files/2025-08/yb25_summary_en_v2.pdf.
- ⁹¹ Amrita Jash, "De-risking from China and Its Implications," *RSIS Commentary* 122, 30 de agosto de 2023, <https://rsis.edu.sg/wp-content/uploads/2023/08/C023122.pdf>.
- ⁹² Ministério do Comércio da República Popular da China, "MOFCOM Spokesperson's Remarks on China's Recent Economic and Trade Policies and Measures," 11 de outubro de 2025, https://english.mofcom.gov.cn/News/SpokesmansRemarks/art/2025/art_c202dcc0433d476db52b1e7f7fe53926.html.
- ⁹³ Gracelin Baskaran, "China's New Rare Earth and Magnet Restrictions Threaten U.S. Defense Supply Chains," *CSIS Critical Questions*, 9 de outubro de 2025, <https://www.csis.org/analysis/chinas-new-rare-earth-and-magnet-restrictions-threaten-us-defense-supply-chains>.
- ⁹⁴ Siri Aas Rustad, "Conflict Trends: A Global Overview, 1946–2024," *Prio Paper* (2025), <https://www.prio.org/publications/14453>.
- ⁹⁵ Max Bergmann e Maria Snegovaya, "Russia's War in Ukraine: The Next Chapter," *CSIS Briefs*, setembro de 2025, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-09/250930_Bergmann_Russia_Ukraine.pdf?VersionId=_S7BqEncSIshWtCuGzzrhK0FKLNpLMTb.
- ⁹⁶ Instituto Kiel para a Economia Mundial, "Ukraine Support Tracker: Europe Now Leading Spender on Weapons Production for Ukraine," 12 de agosto de 2025, <https://www.kielinstitut.de/publications/news/ukraine-support-tracker-europe-now-leading-spender-on-weapons-production-for-ukraine/>.
- ⁹⁷ Euro News, "Drone Debris Found in Ukraine Indicates Russia Is Using New Technology from Iran," 25 de junho de 2025, <https://www.euronews.com/next/2025/06/25/drone-debris-found-in-ukraine-indicates-russia-is-using-new-technology-from-iran>.
- ⁹⁸ Choi Yonghwan, "The Meaning and Significance of North Korean Troops' Deployment to Russia," *RUSI Commentary*, 4 de dezembro de 2024, <https://www.rusi.org/explore-our-research/publications/commentary/meaning-and-significance-north-korean-troops-deployment-russia>.

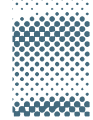


- ⁹⁹ Michal Bogusz e Witold Rodkiewicz, "Three Years of War in Ukraine: The Chinese-Russian Alliance Passes the Test," *OSW Commentary* 639, 20 de fevereiro de 2025, https://www.osw.waw.pl/sites/default/files/OSW_Commentary_639.pdf.
- ¹⁰⁰ Timothy Ash, "The 'Fortress Russia' Economy Has Adapted Well to Pressure. But Stagflation Presents an Opportunity for the West," *Chatham House*, 5 de setembro de 2025, <https://www.chathamhouse.org/2025/09/fortress-russia-economy-has-adapted-well-pressure-stagflation-presents-opportunity-west>.
- ¹⁰¹ Claire Mills, *Sanctions against Russia: What Has Changed in 2025?* (Londres: House of Commons Library, 2025), 6, <https://researchbriefings.files.parliament.uk/documents/CBP-10342/CBP-10342.pdf>.
- ¹⁰² Stephen Quillen, "EU Moves to Ban Russian Energy Imports by 2028," *Al Jazeera*, 20 de outubro de 2025, <https://www.aljazeera.com/news/2025/10/20/eu-moves-to-ban-russian-energy-imports-by-2028>.
- ¹⁰³ France 24, "Israel Targets Hezbollah HQ in Beirut as Border Clashes Continue," 3 de outubro de 2024, <https://www.france24.com/en/middle-east/20241002-%F0%9F%94%B4-live-at-least-six-killed-in-israeli-strike-on-central-beirut>.
- ¹⁰⁴ Ministério das Relações Exteriores, "Ataques Aéreos de Israel Contra o Irã," Nota à imprensa nº 259, 13 de junho de 2025, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/ataques-aereos-de-israel-contra-o-ira; Ministério das Relações Exteriores, "Ataques a Instalações Nucleares do Irã," Nota à imprensa nº 276, 22 de junho de 2025, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/ataques-a-instalacoes-nucleares-do-ira.
- ¹⁰⁵ CNN World, "Israel Targets Hamas Leadership in Qatar Strike," 10 de setembro de 2025, <https://edition.cnn.com/world/live-news/israel-qatar-attack-09-09-25>.
- ¹⁰⁶ Serviço Europeu para a Ação Externa (EEAS), *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (março de 2025), <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>.
- ¹⁰⁷ Financiadora de Estudos e Projetos, "Finep, MCTI e MD Celebram Investimento de R\$ 238 Milhões em 22 Projetos de Empresas na Área de Defesa," 22 de setembro de 2023, <http://www.finep.gov.br/noticias/todas-noticias/6661-finep-mcti-e-md-celebram-investimento-de-r-238-milhoes-em-22-projetos-de-empresas-na-area-de-defesa>.
- ¹⁰⁸ Casa Civil da Presidência da República, "O Processo de Acesso do Brasil à OCDE," 2 de agosto de 2022, <https://www.gov.br/casacivil/pt-br/assuntos/colegiados/ocde/processo-de-acessao-brasil-ocde/o-processo-de-acessao-do-brasil-a-ocde>.
- ¹⁰⁹ Palácio do Planalto, "Governo Federal Divulga Íntegra do Acordo de Parceria Entre Mercosul e União Europeia," 10 de dezembro de 2024, <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2024/12/governo-federal-divulga-integra-do-acordo-de-parceria-entre-mercosul-e-uniao-europeia>.



03 | América do Sul

- ¹¹⁰ Igor Vieira Ferreira e Caio Belandi, "Censo 2022: Informações de População e Domicílios por Setores Censitários Auxiliam Gestão Pública," *Agência IBGE*, 21 de março de 2024, <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/39525-censo-2022-informacoes-de-populacao-e-domicilios-por-setores-censitarios-auxiliam-gestao-publica>.
- ¹¹¹ Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP), *Boletim da Produção de Petróleo e Gás Natural* (Brasília: ANP, 2025), <https://www.gov.br/anp/pt-br/centrais-de-conteudo/publicacoes/boletins-anp/arquivos-bmppgn/2025/agosto.pdf>.
- ¹¹² Ministério do Desenvolvimento, Indústria e Comércio (MDIC), "ComexStat: Dados Gerais," <https://comexstat.mdic.gov.br/pt/geral>.
- ¹¹³ Karim El Aynaoui, "The Atlantic Ocean: A New Frontier for Global Cooperation and African Growth," *Brookings Institution*, 11 de fevereiro de 2025, <https://www.brookings.edu/articles/the-atlantic-ocean-a-new-frontier-for-global-cooperation-and-african-growth>.
- ¹¹⁴ Fundo de População das Nações Unidas (UNFPA), *Country Programme Document for Nigeria* (Nova York: ONU, dezembro de 2022), 2, <https://nigeria.unfpa.org/en/publications/united-nations-population-fund-country-programme-document-nigeria>.
- ¹¹⁵ Agência Gov, "Governo Institui Política Nacional de Fronteiras Para Aprimorar Integração e Segurança," 3 de junho de 2024, <https://agenciagov.ebc.com.br/noticias/202406/em-iniciativa-inedita-governo-federal-institui-a-politica-nacional-de-fronteiras>.
- ¹¹⁶ Irina A. Chindea et al., *Great-Power Competition and Conflict in Latin America* (Santa Monica: Rand Corporation, 2023), https://www.rand.org/pubs/research_reports/RR969-4.html.
- ¹¹⁷ Mélanie Barragán e Ariel Sribman, "El Ajedrez Geopolítico de América Latina en el Nuevo Orden Multipolar," *Revista CIDOB d'Afers Internacionals* 136 (2024): 11–33, <https://www.cidob.org/publicaciones/el-ajedrez-geopolitico-de-america-latina-en-el-nuevo-orden-multipolar>.
- ¹¹⁸ Diana Roy, "China's Growing Influence in Latin America," Council on Foreign Relations, 6 de junho de 2025, <https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri>; Luciano Nascimento, "Entenda a Lei Magnitsky Aplicada Pelos EUA Contra Alexandre de Moraes," *Agência Brasil*, 30 de julho de 2025, <https://agenciabrasil.ebc.com.br/internacional/noticia/2025-07/entenda-lei-magnitsky-aplicada-pelos-eua-contra-alexandre-de-moraes>.
- ¹¹⁹ "GM Registra Perda de US\$ 1,6 Bi com Carro Elétrico Após Fim de Subsídio do Governo e Recuo na Demanda," *O Globo*, 14 de outubro de 2025, <https://oglobo.globo.com/economia/noticia/2025/10/14/gm-registra-perda-de-us-16-bi-com-carro-eletrico-apos-fim-de-subsidio-do-governo-e-recuo-na-demanda.ghtml>; "Pequim: Encontro Empresarial Organizado Pela ApexBrasil é Marcado Por Anúncio Inédito de R\$ 27 Bilhões em Investimentos Chineses no Brasil," *ApexBrasil*, <https://apexbrasil.com.br/content/apexbrasil/br/pt/conteudo/noticias/Pequim-Encontro-empresarial-organizado-pela-ApexBrasil-e-marcado-por-anuncio-inedito-de-27-bilhoes-em>

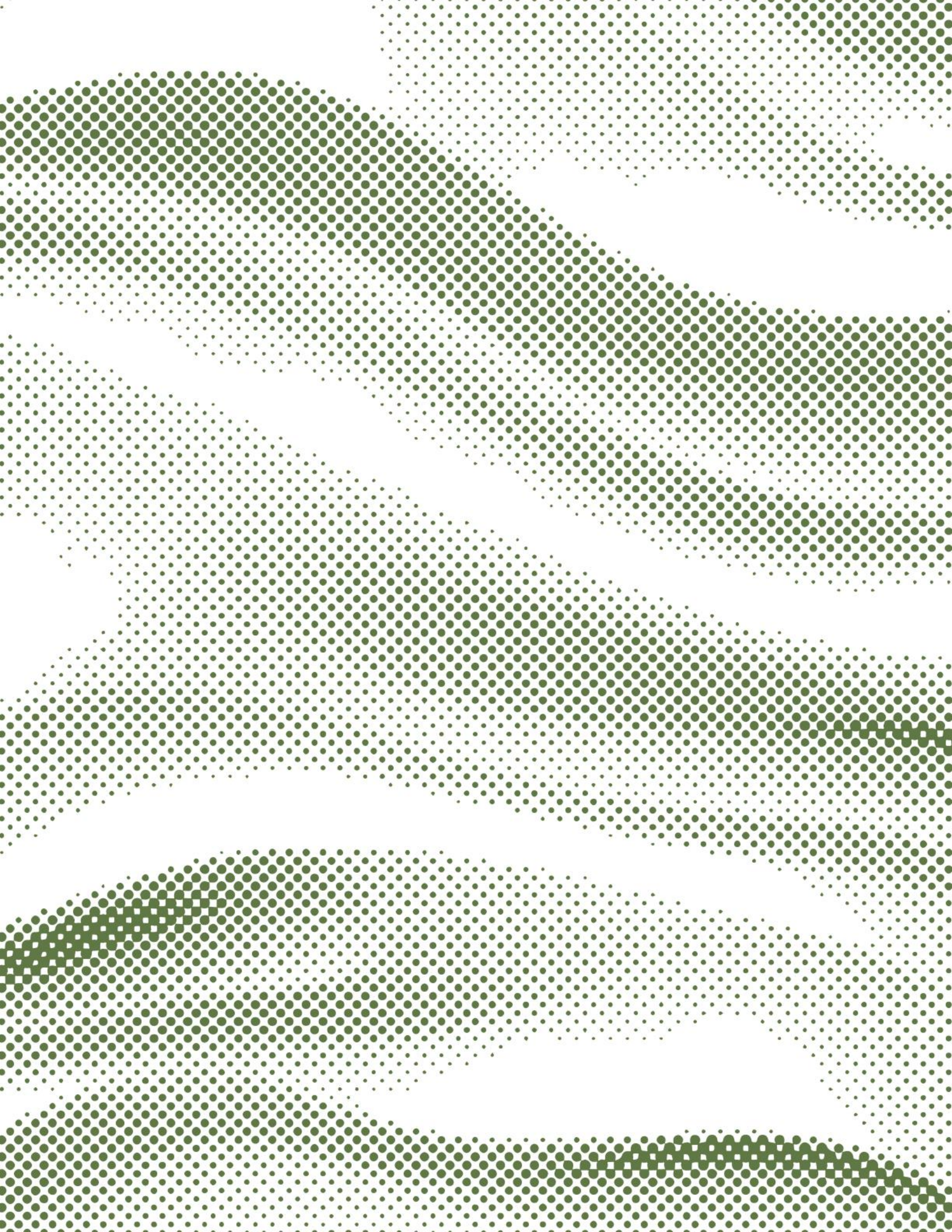


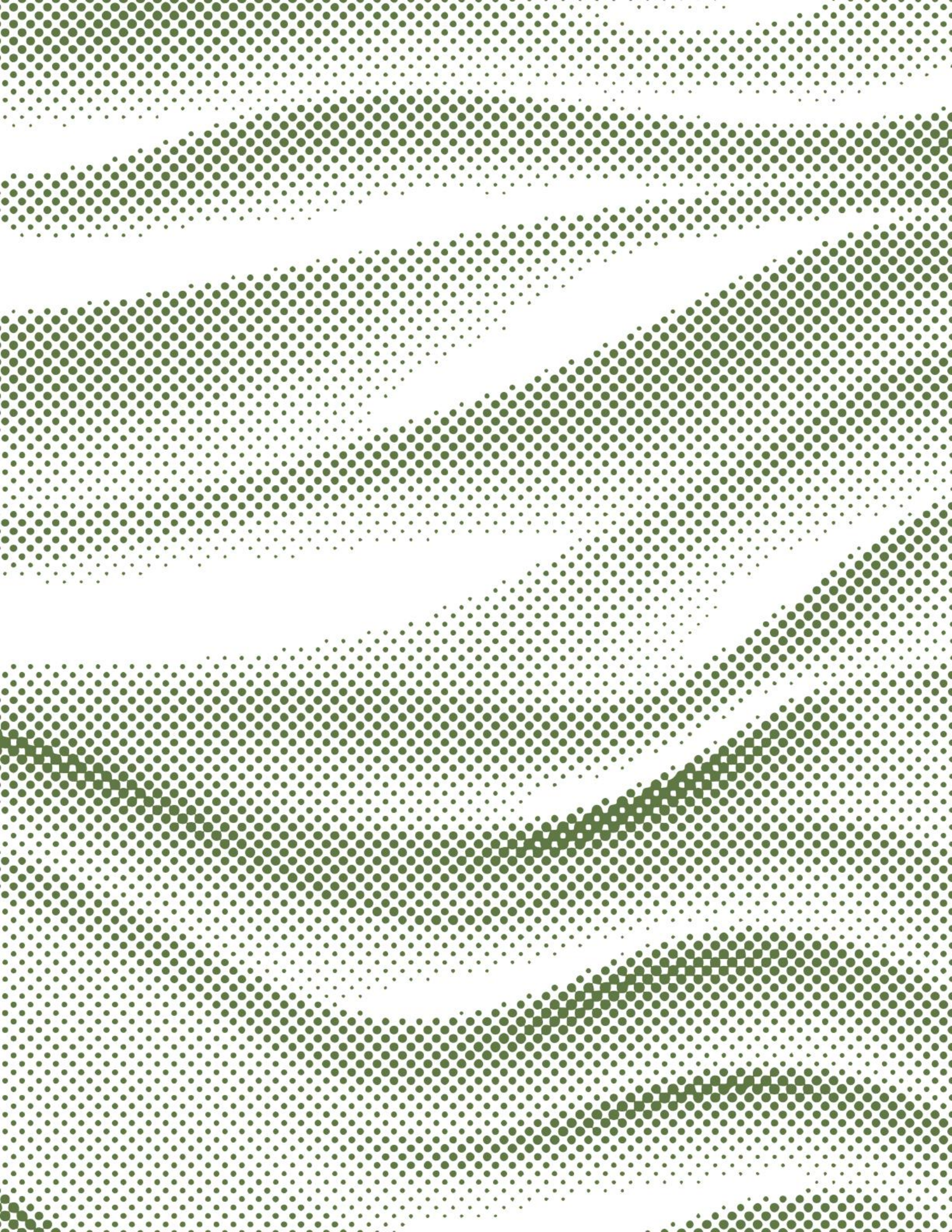
- [investimentos-chineses-no-Brasil.html](#); Andreia Verdélio, “Nova Fábrica de Carros Elétricos Mostra Confiança no Brasil, Diz Lula,” *Agência Brasil*, 9 de outubro de 2025, <https://agenciabrasil.ebc.com.br/economia/noticia/2025-10/nova-fabrica-de-carros-eletricos-mostra-confianca-no-brasil-diz-lula>.
- ¹²⁰ Werner Raza e Hannes Grohs, *Trade Aspects of China's Presence in Latin America and the Caribbean* (Bruxelas: Direção-Geral de Política Externa do Parlamento Europeu), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/702572/EXPO_BRI\(2022\)702572_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/702572/EXPO_BRI(2022)702572_EN.pdf).
- ¹²¹ ECNS, “China-Latin America Trade Volume Hits Record-high of \$518.4 Bln in 2024,” 14 de maio de 2025, <https://www.ecns.cn/news/cns-wire/2025-05-14/detail-ihernfey9435916.shtml>.
- ¹²² Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP), *Boletim de Recursos e Reservas de Petróleo e Gás Natural 2024* (2024), <https://www.gov.br/anp/pt-br/centrais-de-conteudo/dados-estatisticos/arquivos-reservas-nacionais-de-petroleo-e-gas-natural/boletim-anual-reservas-2024.pdf>.
- ¹²³ Organização dos Países Exportadores de Petróleo (OPEP), *2025 OPEC Annual Statistical Bulletin* (2025), <https://www.opec.org/assets/assetdb/asb-2025.pdf>.
- ¹²⁴ United States Geological Survey (USGS), *Mineral Commodity Summaries 2024* (Reston: USGS, 2024), 111, <https://doi.org/10.3133/mcs2024>.
- ¹²⁵ United States Geological Survey (USGS), *Mineral Commodity Summaries 2024* (Reston: USGS, 2024), 145, <https://doi.org/10.3133/mcs2024>.
- ¹²⁶ Agência Brasileira de Inteligência (ABIN), “ABIN Coordena Ações de Inteligência para Desintrusão da Terra Indígena Uru-Eu-Wau-Wau,” 11 de setembro de 2025, <https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-coordena-acoes-de-inteligencia-para-desintrusao-da-terra-indigena-uru-eu-wau-wau>.
- ¹²⁷ Fundação Nacional dos Povos Indígenas (FUNAI), “Governo Federal Cumpre Metas de Proteção a Indígenas e STF Encerra Ação,” 2 de outubro de 2025, <https://www.gov.br/funai/pt-br/assuntos/noticias/2025/governo-federal-cumpr-metas-de-protecao-a-indigenas-e-stf-encerra-acao>.
- ¹²⁸ Agência Nacional de Águas e Saneamento Básico (ANA), “Disponibilidade Hídrica dos Sistemas Aquíferos – Poroso,” 14 de março de 2022, atualizado em 22 de maio de 2024, https://dadosabertos.ana.gov.br/datasets/1c2d988d74d4457b9a3c2444ef929efb_0/about.
- ¹²⁹ Daniel Cerqueira e Samira Bueno, coords., *Atlas da Violência 2025* (Brasília: Instituto de Pesquisa Econômica Aplicada; Fórum Brasileiro de Segurança Pública, 2025), 8, <https://forumseguranca.org.br/wp-content/uploads/2025/05/atlas-violencia-2025.pdf>.
- ¹³⁰ Euro News, “Trump Warns Fight Against South American ‘Narcoterrorist’ Cartels Will Escalate,” 17 de setembro de 2025, <https://www.euronews.com/2025/09/17/trump-warns-fight-against-narcoterrorist-cartels-is-to-escalate>.
- ¹³¹ Agência Brasileira de Inteligência; Direção Nacional de Inteligência da Colômbia, *Desafios da Amazônia Compartilhada: Brasil-Colômbia* (Brasília: Abin, 2025), <https://www.gov.br/abin/pt-br/>



[centrais-de-conteudo/publicacoes/desafios-da-amazonia-compartilhada/desafios-da-amazonia-compartilhada.](#)

- ¹³² Milton Carlos Bragatti e Brigitte Weiffen, "The Deterioration of South America's Security Architecture: From Cooperation to Coexistence?," *International Relations* 39, no. 2 (2023): 301–324, <https://doi.org/10.1177/00471178231195246>.
- ¹³³ Palácio do Planalto, "Governo Federal Anuncia Retorno do Brasil à Unasul," 07 de abril de 2023, <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2023/04/governo-federal-anuncia-retorno-do-brasil-a-unasul>.
- ¹³⁴ Ministério das Relações Exteriores, "Retorno do Brasil à CELAC," 5 de janeiro de 2023, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/retorno-do-brasil-a-celac.
- ¹³⁵ Ministério das Relações Exteriores, "Consenso de Brasília – 30 de Maio de 2023," 30 de maio de 2023, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/consenso-de-brasilia-2013-30-de-maio-de-2023.
- ¹³⁶ Organização do Tratado de Cooperação Amazônica, *Declaração de Belém - IV Reunião de Presidentes dos Estados Partes no Tratado de Cooperação Amazônica* (2023), <https://otca.org/pt/wp-content/uploads/2023/10/Declaracao-de-Belem.pdf>.
- ¹³⁷ Ministério do Planejamento e Orçamento (MPO), *Rotas de Integração Sul-Americana: Relatório 2025* (2025), <https://www.gov.br/planejamento/pt-br/assuntos/articulacao-institucional/publicacoes/relatorio-2025-rotas-de-integracao-sul-americana/>.
- ¹³⁸ Consenso de Brasília, "Mapa do Caminho Para a Integração da América do Sul," 5 de outubro de 2023, https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/MapadoCaminhoparaaIntegraodaAmricadoSul.pdf.
- ¹³⁹ Pedro Silva Barros, "Avaliação Crítica da IIRSA e do Cosiplan e Contribuições Para a Nova Agenda de Integração de Infraestrutura na América do Sul," in *Uma Nova Agenda de Infraestrutura Para a América do Sul*, ed. Pedro Silva Barros (Brasília: FUNAG; IPEA, 2024), 89–102.
- ¹⁴⁰ Banco Mundial, "Logistics Performance Index," <https://lpi.worldbank.org/international/global>.
- ¹⁴¹ Ministério da Fazenda, "Governo Lança Plano Brasil Soberano Para Proteger Exportadores e Trabalhadores de Sobretaxas dos EUA," 13 de agosto de 2025, <https://www.gov.br/fazenda/pt-br/assuntos/noticias/2025/agosto/governo-lanca-plano-brasil-soberano-para-proteger-exportadores-e-trabalhadores-de-sobretaxas-dos-eua>; CNN Brasil, "Trump Assina Decreto Que Oficializa Tarifas de 50% ao Brasil," 30 de julho de 2025, <https://www.cnnbrasil.com.br/economia/macroeconomia/trump-assina-decreto-que-oficializa-tarifas-de-50-ao-brasil/>.







Este livro foi impresso nas oficinas gráficas da ABIN em novembro de 2025.

O texto e os títulos da obra foram compostos em Titillium Web (fonte licenciada pelo Google Fonts) alguns destaques em Elido (fonte licenciada pela Adobe Fonts).



A ABIN é um órgão da Presidência da República, vinculada à Casa Civil e responsável por fornecer ao presidente da República e a seus ministros informações e análises estratégicas, oportunas e confiáveis, úteis para os processos de decisão do Governo Federal.

Desafios de Inteligência é um documento analítico público preparado pela Agência Brasileira de Inteligência (ABIN). Mobiliza recursos de pesquisa e análise prospectiva para avaliar os riscos de segurança para o Brasil em quatro dimensões: global, internacional, regional e nacional.

