UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e99516, p. 1-38, 2026 • https://dx.doi.org/10.5902/2357797599516
Submissão: 23/10/2026 • Aprovação: 16/11/2026 • Publicação: 23/11/2026

Artigos Dossiê

# Soberania quântica seletiva: cadeias de suprimentos, autonomia estratégica e defesa

## Selective quantum sovereignty: supply chains, strategic autonomy and defense

**Manoel Fernandes Amaral Filho**[I]
**Bruno Costa Marinho**[II]
**Anderson Fernandes Pereira dos Santos**[III]

[I]Universidade Federal do Amazonas, Manaus, AM, Brasil
[II]Instituto de Pesquisas do Exército na Amazônia, Manaus, AM, Brasil
[III]Instituto Militar de Engenharia, Rio de Janeiro, RJ, Brasil

## Resumo

Este artigo analisa os impactos geopolíticos e securitários das cadeias globais de suprimentos das tecnologias quânticas sobre a autonomia estratégica e a Defesa Nacional brasileira. Sob o referencial da interdependência armada (*weaponized interdependence*), investiga pontos de estrangulamento materiais, logísticos, cognitivos, financeiros e de *software* que limitam a liberdade de ação do Estado na transição para a era quântica. Adota-se estudo de caso comparativo sistemático, extraindo lições da experiência nuclear brasileira e dos controles contemporâneos sobre inteligência artificial avançada, e incorporam-se evidências difundidas em 2026 sobre o ecossistema quântico nacional. O mapeamento indica base acadêmica relevante, com 34 grupos, 139 pesquisadores, 73 projetos e 828 trabalhos acadêmicos, coexistindo com apenas 17 empresas identificadas e forte dependência de plataformas externas. Na cadeia de isótopos críticos, o *Quantum Isotope Supply Chain Risk Index* (QISCRI) classifica Sr-87 e Yb-171 como riscos críticos. No plano econômico, o investimento em *startups* quânticas alcançou US$ 12,6 bilhões em 2025, e a trajetória de aquisições da IonQ, que culmina no acordo de até US$ 1,3 bilhão pela Elisity, de segurança *Zero Trust*, mostra a consolidação alcançando a própria camada de segurança que a transição pós-quântica deverá proteger. Como resultado, propõe-se um modelo de Soberania Tecnológica Seletiva que combina criticidade tecnológica, concentração de fornecedores, jurisdição corporativa, estrutura de capital e capacidade endógena, priorizando a criptografia pós-quântica (PQC), o sensoriamento, as redes seguras, a inteligência de suprimentos e as capacidades *downstream* de interesse dual.

**Palavras-chave**: Tecnologias quânticas; Autonomia estratégica; Cadeia de suprimentos crítica; Soberania seletiva; Defesa nacional

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

## Abstract

This article analyzes the geopolitical and security impacts of global quantum technology supply chains on Brazil's strategic autonomy and national defense. Drawing on the *weaponized interdependence* framework, it investigates material, logistical, cognitive, financial and software chokepoints that constrain the State's freedom of action in the transition to the quantum era. It adopts a systematic comparative case study, drawing lessons from the Brazilian nuclear experience and from contemporary controls on advanced artificial intelligence, and incorporates evidence released in 2026 on the national quantum ecosystem. The mapping reveals a relevant academic base, with 34 research groups, 139 researchers, 73 projects and 828 academic works, coexisting with only 17 identified companies and a strong dependence on foreign platforms. In the critical isotope chain, the Quantum Isotope Supply Chain Risk Index (QISCRI) ranks Sr-87 and Yb-171 as critical risks. Economically, investment in quantum startups reached US$ 12.6 billion in 2025, and IonQ's acquisition trajectory, culminating in a deal of up to US$ 1.3 billion for the *Zero Trust* security firm Elisity, shows consolidation reaching the very security layer that the post-quantum transition must protect. As a result, the article proposes a Selective Technological Sovereignty model that combines technological criticality, supplier concentration, corporate jurisdiction, capital structure and endogenous capacity, prioritizing post-quantum cryptography (PQC), sensing, secure networks, supply intelligence and dual-use downstream capabilities.


**Keywords**: Quantum technologies; Strategic autonomy; Critical supply chain; Selective sovereignty; National defense

## 1 INTRODUÇÃO

A governança das tecnologias emergentes ingressou em um período de securitização acelerada, que desfez as ilusões liberais de neutralidade nas redes globais de valor. Nesse contexto, as tecnologias quânticas, computação de utilidade, sensoriamento, simulação e comunicações seguras, deixaram de habitar apenas o domínio da Física teórica.

O debate tradicional sobre a vulnerabilidade das potências médias costuma tratar a questão de forma excessivamente simplificada, como se tudo dependesse apenas de possuir ou não um computador quântico de grande escala e tolerante a falhas. No entanto, ter um computador quântico e dispor de uma máquina realmente útil para aplicações estratégicas são situações diferentes. Um equipamento com cerca de 100 qubits, por exemplo, pode representar um avanço científico importante, mas ainda não possui capacidade suficiente para quebrar algoritmos criptográficos assimétricos, como o RSA (Rivest–Shamir–Adleman), esquema de chave pública empregado em certificados digitais, assinaturas e protocolos seguros, cuja segurança

repousa na dificuldade de fatorar números inteiros muito grandes (RIVEST; SHAMIR; ADLEMAN, 1978). O algoritmo de Shor resolve esse problema em tempo polinomial (SHOR, 1997), mas as estimativas mais recentes ainda situam a fatoração de uma chave RSA de 2.048 bits na ordem de centenas de milhares a milhões de qubits físicos com baixas taxas de erro (GIDNEY; EKERÅ, 2021; GIDNEY, 2025). Por isso, a análise não deve considerar apenas a quantidade de qubits, mas também sua qualidade, as taxas de erro, a capacidade de correção, a estabilidade do sistema e a possibilidade de executar algoritmos complexos. Essa distinção permite reconhecer as conquistas já alcançadas pelo Brasil sem superestimar, ao mesmo tempo, a capacidade prática das tecnologias atualmente disponíveis.

O risco estrutural não decorre do atraso na contagem de qubits, mas da dependência assimétrica nos pontos de estrangulamento (*chokepoints*) oligopolizados da cadeia global. Das fundições de semicondutores à criogenia de ultrabaixa temperatura, necessária em algumas plataformas, dos Kits de Desenvolvimento de *Software* (SDKs) proprietários ao acesso remoto via nuvem, na modalidade de computação quântica como serviço (QCaaS), a infraestrutura quântica é controlada por poucas corporações, sob jurisdição de grandes potências.

O caso brasileiro é particularmente sensível. Potência média com responsabilidades de defesa sobre a Amazônia e o Atlântico Sul, o país depende de comunicações sigilosas, criptografia robusta e navegação resiliente, exatamente as capacidades que as tecnologias quânticas prometem revolucionar e, ao mesmo tempo, ameaçar.

Diante disso, o artigo busca responder à seguinte pergunta: *como o Brasil pode estruturar uma estratégia de resiliência e autonomia seletiva na cadeia de suprimentos das tecnologias quânticas, aprendendo com as restrições do setor nuclear e* com os controles contemporâneos sobre a inteligência artificial (IA) avançada?

O objetivo é duplo. Primeiro, desconstruir a anatomia material e lógica da cadeia quântica, contrastando os gargalos globais com a capacidade real do Brasil, hoje mais bem documentada por mapeamentos nacionais que evidenciam simultaneamente

densidade acadêmica, baixa participação empresarial e fragmentação institucional. Segundo, rejeitar tanto o isolacionismo autárquico quanto a passividade tecnológica, propondo um modelo de Soberania Tecnológica Seletiva capaz de transformar capacidades científicas dispersas em resiliência operacional para a Defesa. Como sintetizaram MIGON e ARAÚJO-MOREIRA (2026, p. A6), "o que está em jogo é a nossa capacidade de decidir sem dependência externa", o que exige identificar nichos nos quais o país já possui competência científica, demanda estratégica e possibilidade de articulação produtiva.

Há, ainda, uma camada de poder que não aparece na contagem de qubits: a estrutura de capital. O ciclo 2025–2026 combinou forte aceleração de investimento privado, abertura de capital de empresas de diferentes modalidades físicas e consolidação por fusões e aquisições. Para a soberania seletiva, o dado importa porque capital abundante pode transformar rapidamente fornecedores de nicho em plataformas dominantes, integrar verticalmente *hardware*, *software* e componentes e deslocar a jurisdição efetiva de tecnologias críticas. Assim, mapear quem financia, controla e consolida cada elo passa a ser parte da própria inteligência de suprimentos (MCKINSEY & COMPANY, 2026). O anúncio, em outubro de 2026, da aquisição da Elisity, empresa de microssegmentação *Zero Trust*, pela IonQ, que já controlava ativos de computação, redes, sensoriamento e fabricação, mostra que essa consolidação começa a alcançar também a camada de segurança das redes que a criptografia pós-quântica deverá proteger (QURECA, 2026).

## 2 REFERENCIAL TEÓRICO

A análise das dinâmicas de poder das tecnologias profundas exige abandonar os modelos que veem a integração tecnológica como dissolução simétrica das fronteiras de poder do Estado. O referencial deste artigo ancora-se na convergência entre autonomia estratégica e interdependência armada, formulada por FARRELL e NEWMAN (2019).

A autonomia estratégica não se resume à autossuficiência econômica, formulação obsoleta diante da complexidade produtiva contemporânea. Ela é a capacidade político-material de formular e implementar decisões soberanas de política externa, segurança e Defesa sem se submeter a constrangimentos ou vetos de potências estrangeiras (FIOTT, 2018). No campo das tecnologias críticas, liga-se ao grau de controle, auditabilidade e resiliência sobre *hardware*, *software* e infraestrutura física.

A teoria da interdependência armada subverte a ideia de que a integração econômica dispersa o poder. FARRELL e NEWMAN (2019) mostram que as redes globais, financeiras (como a rede de mensageria interbancária SWIFT, *Society for Worldwide Interbank Financial Telecommunication*, cooperativa sediada na Bélgica que conecta mais de 11 mil instituições em mais de 200 países e territórios; SWIFT, 2025), de cabos submarinos ou de semicondutores, não são descentralizadas: evoluem para uma topologia de escala livre, com nós centrais hiperconcentrados (*hubs*).

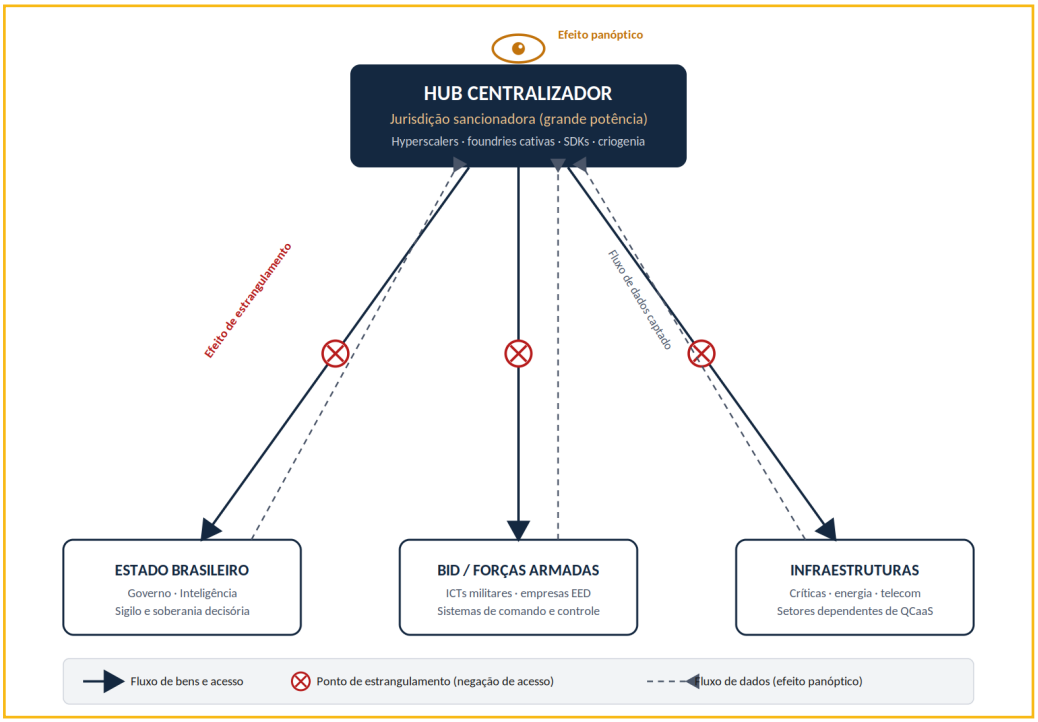
Dois episódios ilustram o argumento. A exclusão de sete bancos russos do sistema SWIFT, determinada pelo Regulamento (UE) 2022/345 do Conselho da União Europeia, de 1º de março de 2022, e efetivada em 12 de março daquele ano, mostrou como uma infraestrutura financeira pode ser convertida em instrumento de coerção (UNIÃO EUROPEIA, 2022). O mecanismo é instrutivo: por estar sediado em território europeu, o SWIFT cumpriu uma decisão do Conselho, e não uma escolha comercial própria, o que evidencia que é a jurisdição do controlador de um *hub* que define seu uso coercitivo. Os controles norte-americanos sobre semicondutores avançados demonstraram que dominar um único elo, a litografia, permite conter a trajetória tecnológica de um competidor.

Os Estados que controlam juridicamente esses *hubs* exercem dois mecanismos de coerção assimétrica. O efeito panóptico permite mapear e auditar os fluxos de informação e código que atravessam o nó central, antecipando movimentos e vulnerabilidades de concorrentes.

O efeito de estrangulamento é a capacidade de interromper, negar ou condicionar o acesso a bens e infraestruturas cruciais. Ele converte a dependência logística em vulnerabilidade imediata de segurança nacional, operando como arma de interdição de baixo custo militar e altíssimo impacto.

A resposta a essa assimetria não é a autarquia, inviável para qualquer economia contemporânea, mas a Soberania Tecnológica Seletiva: a capacidade de escolher, elo a elo, o que dominar, o que desenvolver em cooperação e o que apenas monitorar (EDLER *et al.*, 2020). Essa distinção orienta toda a análise que se segue.

Figura 1 – Modelo teórico de interdependência armada e pontos de estrangulamento




Fonte: Adaptado de FARRELL e NEWMAN (2019)

## 3 METODOLOGIA

Este estudo caracteriza-se como uma pesquisa qualitativa, de natureza aplicada, com objetivos exploratórios e descritivos, utilizando revisão de literatura, análise documental e análise comparativa.

A pesquisa bibliográfica foi realizada nas bases Scopus, Web of Science, IEEE Xplore, SpringerLink e Google Scholar, sendo complementada por documentos institucionais e regulatórios publicados por organismos nacionais e internacionais.

Os dados coletados foram submetidos à análise qualitativa de conteúdo, sendo organizados em cinco eixos temáticos: (i) anatomia da cadeia global de suprimentos das tecnologias quânticas; (ii) diagnóstico das capacidades nacionais; (iii) análise comparativa entre os setores nuclear, de inteligência artificial e de tecnologias quânticas, complementada pelo contraste entre as respostas estatais da China e da Alemanha aos regimes de controle; (iv) proposição de um modelo de Soberania Tecnológica Seletiva; e (v) implicações para a Base Industrial de Defesa (BID) e para a formulação de políticas públicas.

O corpus documental contempla trabalhos difundidos em 2026 no ecossistema brasileiro de tecnologias quânticas, incluindo: (i) o Mapa das Tecnologias Quânticas no Brasil, que organiza atores, projetos, empresas, startups e produção científica; (ii) análise sociotécnica da dependência brasileira de nuvens e infraestruturas quânticas estrangeiras; (iii) estudo sobre trajetórias formativas e institucionalização limitada da computação quântica; (iv) proposta aplicada de soberania digital baseada em criptografia pós-quântica (PQC), armazenamento soberano, *blockchain* permissionada e *Zero Trust*; e (v) o relatório executivo Isótopos Críticos para Computação Quântica, que propõe o *Quantum Isotope Supply Chain Risk Index* (QISCRI) e decompõe o risco em *upstream*, enriquecimento, concentração de produtores, exposição geopolítica, logística e substitutabilidade. Esses documentos foram utilizados como evidência contemporânea para triangulação do diagnóstico nacional, e não como substitutos das fontes normativas, técnicas e internacionais já examinadas.

Como principal contribuição metodológica do estudo, foi desenvolvida uma Matriz de Soberania Tecnológica Seletiva, construída a partir do cruzamento de três variáveis analíticas: criticidade estratégica para a Defesa Nacional; risco de bloqueio decorrente da concentração das cadeias globais de suprimentos; e capacidade nacional

de absorção tecnológica, complementadas por um multiplicador de concentração empresarial e jurisdicional que incorpora a jurisdição dinâmica e a estrutura de capital dos fornecedores. Essa matriz permitiu classificar os diferentes elos da cadeia quântica em quatro estratégias de intervenção, dominar nacionalmente, desenvolver em cooperação, diversificar fornecedores e aceitar dependência monitorada, constituindo o principal instrumento analítico proposto pelo artigo para orientar a priorização de investimentos, a mobilização da Base Industrial de Defesa e a formulação de políticas públicas voltadas à soberania tecnológica. Para ilustrar a operacionalização da categoria "dominar nacionalmente", recorre-se ao Índice de Maturidade em Criptografia Pós-Quântica (IM-PQC), instrumento de mensuração da prontidão organizacional para a transição criptográfica, cujas dimensões são apresentadas na seção 4.2.2 e detalhadas na seção 4.4.1.

# 4 RESULTADOS E DISCUSSÃO

## 4.1 Anatomia da cadeia de suprimentos quântica

Para compreender a vulnerabilidade estrutural, decompõe-se a cadeia em cinco camadas verticais interdependentes, mapeadas no Quadro 1.

A primeira camada reúne os insumos básicos e a física fina de materiais. Qubits de silício de spin exigem isótopos purificados de Silício-28, sem o Silício-29, que induz decoerência; seu refino concentra-se em poucas instalações. Já os sistemas criogênicos dependem de Hélio-3, isótopo escasso derivado sobretudo da manutenção de estoques de ogivas nucleares.

A segunda camada concentra o *hardware* crítico de suporte, com destaque para os refrigeradores de diluição sem líquido. Qubits supercondutores operam na casa dos milikelvin, para mitigar o ruído térmico que colapsa a superposição. O mercado é dominado pela finlandesa Bluefors e pela britânica Oxford Instruments.

Quadro 1 – Mapeamento de vulnerabilidade por camada industrial quântica

| Camada | Nome | Componentes críticos | Fornecedores dominantes | Risco | Regime regulatório |
|---|---|---|---|---|---|
| 5 | *Software* e Nuvem (QCaaS) | SDKs (Qiskit, Cirq), compiladores, APIs de acesso remoto | IBM, Google, AWS, Microsoft, Alibaba | CRÍTICO | Termos de uso privados / KYC dos EUA |
| 4 | Processadores (chips) | Qubits supercondutores, fotônicos, armadilhas de íons | IBM, Rigetti, Pasqal, IQM, Xanadu, Quantinuum | ALTO | Patentes cativas / ausência de foundries abertas |
| 3 | Eletrônica de controle e sinais | Geradores de forma de onda (AWGs), digitalizadores, RF | Zurich Instruments, Quantum Machines, Keysight | MÉDIO | Controle tecnológico OTAN / Suíça |
| 2 | *Hardware* de suporte crítico | Refrigeradores de diluição criogênica, lasers de estabilidade | Bluefors (Finlândia), Oxford Instruments, Toptica | CRÍTICO | Acordo de Wassenaar (duplo uso) |
| 1 | Insumos básicos e física fina | Isótopos puros de Silício-28, gás Hélio-3, gálio e germânio refinados | Instalações na Rússia, África do Sul, estoques de Defesa; refino de gálio e germânio na China | ALTO | Escassez mineral / subprodutos nucleares; controle de exportação chinês |

Fonte: Autores (2026)

Nota: A classificação de risco reflete a concentração de fornecedores e o regime regulatório. KYC: Know Your Customer (identificação obrigatória do cliente); OTAN: Organização do Tratado do Atlântico Norte.

Para átomos neutros e íons aprisionados, o gargalo desloca-se para os lasers de largura de linha ultraestreita, dominados pela alemã Toptica e por fornecedores norte-americanos, também sob barreiras de duplo uso.

A assimetria dessas duas primeiras camadas manifesta-se com clareza na resposta estratégica da China às restrições de duplo uso. Privadas do acesso a componentes de origem norte-americana pela inclusão na Entity List (caso da Origin Quantum, designada em maio de 2024), as instituições chinesas converteram o cerco em política de substituição forçada de importações, nacionalizando justamente o elo mais crítico do Quadro 1. No ecossistema de Hefei, a QuantumCTek, controlada pela China Telecom desde janeiro de 2025, desenvolveu com o Anhui Quantum Computing Engineering Research Center o refrigerador ez-Q, com temperatura-base da ordem de 10 mK. Segundo a fabricante, fornecedores chineses já respondem por cerca de 80%

do hardware do computador Origin Wukong, máquina supercondutora de 72 qubits operacionais desenvolvida pela própria Origin Quantum e lançada em janeiro de 2024 (IVEZIC, 2026a).

O elo mais revelador é o de habilitação. Os refrigeradores de diluição que resfriam a maioria dos computadores supercondutores vêm da finlandesa Bluefors e da britânica Oxford Instruments, que, juntas, superam 70% do mercado, enquanto a eletrônica de controle se divide entre Suíça, Israel e Alemanha (IVEZIC, 2026b). Para o Brasil, a leitura é estratégica, e não desalentadora: se nem os Estados Unidos dominam toda a pilha e dependem de aliados confiáveis, a via realista para uma potência média não é reproduzir o todo, mas escolher um nicho de excelência, a exemplo da fotônica e da criptografia, e nele tornar-se fornecedor reconhecido e interdependente, em vez de mero consumidor.

A terceira camada abrange a eletrônica de sinais e o controle de micro-ondas. A leitura e a manipulação dos qubits exigem geradores de forma de onda (AWGs) e digitalizadores de altíssima velocidade e baixíssimo ruído de fase. Zurich Instruments, Quantum Machines e Keysight dominam esses ecossistemas, e a ausência de fabricação nacional gera dependência crônica de manutenção e reposição.

A quarta camada é o núcleo do processamento quântico. Diferente dos semicondutores clássicos, com fundições abertas, os chips quânticos de ponta, supercondutores (IBM, Rigetti), fotônicos (Xanadu, PsiQuantum) ou de íons (Quantinuum), são produzidos em instalações proprietárias e cativas. À periferia tecnológica resta o papel de consumidora de pastilhas prontas ou o acesso abstrato de nível superior.

A quinta camada é o *software*, os SDKs e o acesso em nuvem (QCaaS). Hoje, a maioria dos usuários, inclusive forças armadas, não opera *hardware* quântico local, mas remoto, via IBM Quantum, Amazon Braket, Google Quantum AI e Microsoft Azure Quantum, sob jurisdição norte-americana, ou Alibaba Cloud, no bloco chinês.

É o ponto de estrangulamento de maior volatilidade política. Os termos de uso incorporam cláusulas de sanções e segurança nacional, e uma inflexão diplomática pode bloquear IPs governamentais, revogar licenças de compiladores ou negar acesso aos SDKs, paralisando programas de criptoanálise ou simulação militar. Essa concentração, detectável, excludível e quantificável, é o que torna a cadeia de computação um ponto privilegiado de governança estatal (SASTRY *et al*., 2024).

A evidência brasileira recente reforça essa leitura ao descrever o acesso a recursos quânticos como participação predominantemente mediada por plataformas externas. A nuvem amplia a capacidade de experimentação e formação, mas não transfere domínio sobre a infraestrutura subjacente; ao contrário, pode converter provedores, SDKs e padrões proprietários em "pontos de passagem obrigatórios", deslocando a dependência do bem de capital para o controle cognitivo, logístico e informacional do ambiente de desenvolvimento (SOUZA; FRÓES; DIAS, 2026). Para a Defesa, portanto, soberania não se confunde com posse física de um processador: exige capacidade de executar, auditar, portar e preservar aplicações críticas fora de um único ecossistema estrangeiro.

### 4.1.1 Isótopos críticos: da abundância mineral à soberania funcional

Uma camada material adicional emerge quando a cadeia é observada a partir das arquiteturas de átomos neutros e íons aprisionados. A cadeia pode ser representada como feedstock → refino químico → enriquecimento isotópico → fonte atômica → unidade de processamento quântico (QPU). O relatório executivo Isótopos Críticos para Computação Quântica (2026) demonstra que a vulnerabilidade não decorre necessariamente da escassez do elemento químico, mas da combinação entre abundância isotópica, capacidade de enriquecimento, concentração dos produtores efetivos, exposição geopolítica, logística e baixa substitutabilidade depois que a espécie atômica é incorporada ao desenho da QPU. Essa constatação converge com a hipótese central deste artigo: o *chokepoint* relevante está no elo cuja substituição é lenta, opaca ou politicamente condicionável, e não necessariamente no componente

de maior valor unitário. Aplicado aos principais isótopos, o índice proposto no relatório, o QISCRI, classifica Sr-87 (81/100) e Yb-171 (80/100) como riscos críticos, Ca-43 (77/100) e Rb-87 (67/100) como altos e Cs-133 (52/100) como moderado, sendo instrumento de priorização, e não estimativa probabilística de ruptura (ISÓTOPOS Críticos..., 2026).

Outro achado converge diretamente com a discussão sobre jurisdição corporativa dinâmica: contar vendedores não equivale a contar produtores independentes. Dois distribuidores podem oferecer o mesmo isótopo e, sem transparência contratual, depender da mesma instalação de enriquecimento. Nesse caso, a aparente dupla fonte desaparece diante de uma sanção, falha de campanha, restrição de exportação ou mudança de controle do produtor. Para fins de Defesa, redundância só deve ser reconhecida quando houver evidência de instalações de enriquecimento distintas e, quando materialmente relevante, de *feedstocks upstream* que não convirjam para o mesmo país ou produtor dominante.

## 4.2 O mosaico brasileiro de iniciativas quânticas

A capacidade quântica do Brasil revela um paradoxo mais preciso do que o diagnóstico de simples atraso: existe massa crítica científica, porém sua conversão em capacidade tecnológica, industrial e estratégica permanece limitada. O Mapa das Tecnologias Quânticas no Brasil, divulgado em 2026, quantifica um ecossistema em consolidação, distribuído por diferentes regiões e instituições, mas ainda marcado por baixa articulação entre academia, setor produtivo e Estado (ABREU; VASSOLER; FARIAS, 2026).

O novo mapa nacional altera a escala do diagnóstico. Até a data de publicação, foram identificadas 17 empresas, das quais 12 *startups*, 4 iniciativas relacionadas a computadores quânticos e 8 iniciativas de redes quânticas experimentais. No plano acadêmico, o levantamento reuniu 34 grupos de pesquisa, 139 pesquisadores diretamente envolvidos, 73 projetos ativos, 109 artigos publicados em eventos da Sociedade Brasileira de Computação e 828 trabalhos acadêmicos, dos quais 641 dissertações de mestrado e 187 teses de doutorado (ABREU; VASSOLER; FARIAS, 2026). Esses números demonstram que a vulnerabilidade brasileira não deriva da

inexistência de conhecimento, mas da dificuldade de transformá-lo em infraestrutura, produtos, propriedade intelectual e capacidade operacional soberana.

Quadro 2 – Matriz de auditoria das iniciativas quânticas nacionais

| Polo | Instituições | Arquitetura declarada | Maturidade | Dependências | Confirmação |
|---|---|---|---|---|---|
| João Pessoa / PB | Governo da PB / Pq. Tec. Horizontes | Aquisição de *hardware* chinês (20 e 100 qubits) | Prospecção política; sem criogenia local | Fornecedores estatais chineses (HW, *firmware*, suporte) | Parcial |
| Recife / PE | UFPE / Física / spin-offs | Fotônica quântica, comunicações ópticas, QKD | Avançado (TRL 3-4); protótipos de bancada | Diodos laser, moduladores e detectores (SNSPDs) importados | Confirmado |
| Campinas / SP | UNICAMP / IFGW | Semicondutores e fotônica em silício integrado | Avançado (TRL 3); nanofabricação | Insumos ultrapuros e fotolitografia estrangeiros | Confirmado |
| Rio de Janeiro / RJ | CBPF / UFRJ | RMN, simulações e magnetometria | Consolidado; domínio de manipulação de spins | Espectrômetros de RMN importados; hélio líquido | Confirmado |
| Niterói / RJ | UFF / grupos associados | *Software* quântico, algoritmos e emuladores | Operacional; formação de pessoal | Dependência remota absoluta da nuvem IBM (EUA) | Confirmado |
| Rio de Janeiro / RJ (rede) | UFRJ e instituições parceiras — Rede Rio Quântica (RRQ) | Rede metropolitana com cinco nós em fibra e espaço livre; emaranhamento e protocolo *twin-field* | Experimental, em expansão (2026) | Fontes, detectores e eletrônica importados; *firmware* e manutenção externos | Confirmado |
| Rio de Janeiro / RJ (Defesa) | IME / Programa Quantum (IME/ FINEP) | P&D e formação em tecnologias quânticas de interesse dual; articulação academia–indústria–Estado | Em estruturação; formação de especialistas | Financiamento continuado e infraestrutura de testes | Confirmado |
| Nacional (mapeamento 2026) | 34 grupos, 139 pesquisadores; 17 empresas (12 *startups*) | Computação, comunicações (com ênfase em QKD) e sensoriamento | Academia como centro de gravidade; baixa densidade empresarial | Plataformas e nuvens estrangeiras (QCaaS); PI e fabricação externas | Confirmado |

Fonte: Adaptado de ABREU, VASSOLER e FARIAS (2026), AGUILAR (2026) e MIGON e ARAÚJO-MOREIRA (2026).

Nota: O quadro tem função de auditoria ilustrativa de polos selecionados e não pretende representar a totalidade do ecossistema brasileiro, hoje mais amplo do que o recorte geográfico apresentado. Siglas: QKD, distribuição quântica de chaves; TRL, nível de maturidade tecnológica (Technology Readiness Level); SNSPDs, detectores de fóton único de nanofio supercondutor; RMN, ressonância magnética nuclear.

Na comunicação quântica, o mapeamento nacional registra concentração importante de iniciativas em Distribuição Quântica de Chaves (QKD), mas também ressalta que seu papel futuro deve ser avaliado em conjunto com a criptografia pós-quântica, cuja adoção é compatível com infraestruturas clássicas. A implicação para a Defesa é evitar uma falsa escolha tecnológica: QKD pode integrar nichos de altíssima criticidade e enlaces controlados, enquanto PQC deve sustentar a migração ampla de sistemas legados, dispositivos embarcados e redes de grande escala.

O aspecto mais sensível encontra-se na camada de *software,* especialmente em grupos de pesquisa que dependem do acesso remoto a plataformas estrangeiras, como as disponibilizadas pela IBM, Google e Amazon Braket. Nesse modelo de computação quântica como serviço (QCaaS) o desenvolvimento nacional ocorre sobre uma infraestrutura controlada por empresas sediadas no exterior.

Entretanto, é necessário distinguir o uso acadêmico dessas plataformas de sua eventual utilização em aplicações militares, de inteligência ou relacionadas à Base Industrial de Defesa. Antes de afirmar que dados sensíveis e lógica algorítmica poderiam ser processados nesses ambientes, deve-se verificar se os contratos, termos de uso e políticas de segurança dos provedores permitem esse tipo de emprego e quais restrições seriam aplicáveis. Caso esse uso seja admitido, a dependência de infraestrutura estrangeira poderá gerar riscos relacionados à confidencialidade, à jurisdição sobre os dados, à continuidade do acesso e à possibilidade de interrupção do serviço por decisão empresarial, regulatória ou governamental. Essa verificação contratual, retomada na seção 4.3.3 à luz dos regimes nacionais de controle, deve preceder qualquer conclusão sobre o que pode ou não ser empregado pelas Forças Armadas.

Some-se a fragilidade do capital humano. Ainda que de alcance limitado, estudo qualitativo exploratório apresentado em 2026, com amostra reduzida (18 estudantes e três docentes) e sem pretensão de generalização, sugere que o interesse pela computação quântica no Brasil ainda emerge, em grande medida, de curiosidade individual, autodidatismo, redes informais e encontros contingentes com professores;

11 dos 18 estudantes relataram engajamento posterior em atividades relacionadas ao campo, mas o estudo não identificou percursos institucionais sistematicamente estruturados para entrada e progressão profissional (DANSA; CÉSAR, 2026).

### 4.2.1 Jurisdição corporativa dinâmica: fusões, aquisições e risco de continuidade

Os debates técnicos apresentados no Congresso Brasileiro de Ciências e Tecnologias Quânticas (CBCTQ) de 2026 reforçam uma dimensão que a análise tradicional de cadeias de suprimentos tende a subestimar: a nacionalidade formal do fornecedor não é um atributo estático de segurança. Fusões, aquisições, participações de controle e reorganizações societárias podem deslocar, em curto espaço de tempo, o centro efetivo de decisão, a jurisdição dominante e a exposição regulatória de um ativo considerado crítico.

Um caso recente ilustra o problema. A ID Quantique, empresa sediada em Genebra e reconhecida internacionalmente por soluções de QKD e detecção quântica, passou em maio de 2025 ao controle da norte-americana IonQ, que concluiu a aquisição de participação controladora da companhia suíça. Documentos corporativos e regulatórios posteriores identificam a id Quantique SA, na Suíça, entre as subsidiárias da IonQ. O episódio é relevante não porque implique, por si só, comportamento inadequado de qualquer empresa ou governo, mas porque demonstra que a origem geográfica aparente de um fornecedor pode divergir da jurisdição do controlador econômico e das obrigações regulatórias às quais o grupo empresarial está submetido (IONQ, 2025; U.S. SEC, 2026).

A consequência metodológica é direta: a matriz de soberania seletiva deve incorporar a variável ‘jurisdição dinâmica’. Para cada fornecedor crítico, a análise de dependência precisa registrar não apenas país-sede, mas também estrutura de controle, beneficiário final, localização da propriedade intelectual, jurisdição aplicável a exportações, dependência de atualizações remotas, capacidade de manutenção local, possibilidade de substituição e histórico de aquisições. Uma mudança societária

relevante deve acionar nova avaliação de risco, tal como já ocorre em setores sensíveis submetidos a mecanismos de *investment screening*, controle de exportações e segurança de infraestrutura crítica.

O movimento de consolidação vertical também amplia essa preocupação. Em 2026, a própria IonQ concluiu a aquisição da SkyWater Technology, fundição norte-americana de semicondutores, apresentando a operação como parte de uma estratégia de integração da cadeia de computação, redes, segurança e sensoriamento quânticos. A concentração de propriedade intelectual, fabricação, componentes de rede e plataformas em conglomerados verticalizados pode aumentar eficiência e acelerar inovação, mas também reduz a quantidade de fornecedores verdadeiramente independentes. Para países que não controlam esses grupos, a diversificação nominal de marcas pode esconder concentração jurisdicional substantiva (IONQ, 2026a). A trajetória completa dessas aquisições, sintetizada no Quadro 3 e examinada na subseção seguinte, mostra que o fenômeno não é episódico.

### 4.2.2 O caso IonQ–Elisity: quando a consolidação da cadeia quântica alcança a camada de segurança

O caso mais recente e ilustrativo dessa dinâmica ocorreu em 12 de outubro de 2026, quando a IonQ anunciou acordo para adquirir a Elisity, empresa norte-americana fundada em 2019 e especializada em microssegmentação de redes baseada em identidade, princípio central das arquiteturas *Zero Trust*. A operação, integralmente paga em ações, foi avaliada em até US$ 1,3 bilhão, incluindo até US$ 150 milhões em *earnouts* condicionados ao desempenho futuro da adquirida, e tem conclusão prevista para o quarto trimestre de 2026, sujeita a aprovação regulatória. Trata-se da segunda aquisição da IonQ acima de US$ 1 bilhão no mesmo ano, após a SkyWater (cerca de US$ 1,8 bilhão) (QURECA, 2026; YAHOO FINANCE, 2026).

Na arquitetura *Zero Trust*, nenhum usuário, dispositivo ou fluxo é considerado confiável apenas por estar dentro do perímetro da rede: cada acesso é autenticado,

autorizado e continuamente reavaliado (ROSE *et al.*, 2020). A microssegmentação operacionaliza esse princípio ao dividir a rede em segmentos governados por políticas de identidade, de modo que um dispositivo comprometido não consiga mover-se lateralmente. É esse o diferencial atribuído à Elisity: impedir que invasores e *ransomware* se propaguem pela rede, em mais de cem implantações concentradas sobretudo em hospitais, empresas de saúde, indústria farmacêutica e manufatura (QURECA, 2026; IVEZIC, 2026c).

Isoladamente, a operação poderia ser lida como diversificação comercial. Observada em série, revela um padrão de integração da cadeia de suprimentos. Desde o fim de 2024, a IonQ adquiriu ou anunciou a aquisição de pelo menos onze empresas que, em conjunto, alcançam quase todas as camadas mapeadas no Quadro 1: fabricação de semicondutores e fotônica integrada, processadores de íons aprisionados e seu controle eletrônico, interconexões e memórias quânticas, distribuição quântica de chaves e geração quântica de números aleatórios, sensores e relógios atômicos, comunicações ópticas e satélites e, agora, segurança de redes clássicas (Quadro 3). A empresa passou a apresentar-se, ademais, como fornecedora mercantil (*merchant supplier*) de outros desenvolvedores: relógios atômicos, componentes de rede e sensores já são vendidos a empresas de computação quântica e a contratantes governamentais, e a fundição herdada da SkyWater deverá ofertar componentes fotônicos integrados ao restante do ecossistema (NASDAQ, 2026; IONQ, 2026b). Na linguagem de FARRELL e NEWMAN (2019), forma-se um *hub* corporativo do qual passam a depender não apenas clientes finais, mas também concorrentes.

O passo representado pela Elisity é qualitativamente distinto dos anteriores. Até então, as aquisições concentravam-se na pilha quântica propriamente dita; com a Elisity, a consolidação ultrapassa essa pilha e alcança a camada de segurança das redes clássicas, isto é, o ambiente que a transição pós-quântica deverá proteger. O próprio presidente da IonQ, Niccolo de Masi, justificou a operação afirmando que o mundo ingressa nos “anos mais perigosos” em matéria de riscos cibernéticos e associando-a

à preparação de empresas e do governo norte-americano para o *Q-Day*, momento em que computadores quânticos poderão romper a criptografia de chave pública amplamente utilizada (YAHOO FINANCE, 2026). A estratégia declarada é combinar os produtos de PQC e QKD do grupo, herdados em grande parte da ID Quantique, à plataforma *Zero Trust* da Elisity e ao seu acesso direto aos responsáveis pela segurança da informação (CISOs) de empresas e governos (IVEZIC, 2026c).

Quadro 3 – Aquisições da IonQ e camadas da cadeia quântica alcançadas (2024–2026)

| Empresa | Data | Especialidade | Camada / domínio alcançado |
|---|---|---|---|
| Qubitekk | Anúncio nov. 2024; conclusão jan. 2025 | Redes quânticas, emaranhamento e distribuição quântica de chaves | Comunicações quânticas |
| ID Quantique (IDQ) | Maio 2025 (controle) | QKD, QRNG e segurança quântica | Comunicações e segurança quânticas |
| Lightsynq Technologies | Maio 2025 | Memórias quânticas e interconexões fotônicas | Camada 4 (interconexão de processadores) |
| Capella Space | Jul. 2025 (≈ US$ 311 mi em ações) | Satélites e radar de abertura sintética (SAR) | Espaço (base para QKD por satélite) |
| Oxford Ionics | Set. 2025 (≈ US$ 1,08 bi) | Processadores de íons aprisionados com controle eletrônico de qubits | Camadas 3 e 4 |
| Vector Atomic | Out. 2025 | Sensores quânticos, relógios atômicos e tecnologias de posicionamento, navegação e tempo (PNT) | Sensoriamento quântico |
| Skyloom Global | Jan. 2026 | Comunicações ópticas espaciais | Redes e espaço |
| Seed Innovations | Jan. 2026 | Pesquisa e desenvolvimento de *software* e tecnologias | Camada 5 (*software*) |
| SkyWater Technology | Jul. 2026 (≈ US$ 1,8 bi) | Fabricação de semicondutores e integração de *hardware* | Camada 4 (fabricação) e fornecimento a terceiros |
| Nexus Photonics | Set. 2026 | Fotônica integrada heterogênea (lasers e moduladores em *chip*) | Camada 2 (lasers e óptica) |
| Elisity | Anúncio 12 out. 2026; conclusão prevista no 4º trim. 2026 (até US$ 1,3 bi) | Microssegmentação *Zero Trust* baseada em identidade | Segurança de redes clássicas (fora da pilha quântica) |

Fonte: Adaptado de IONQ (2025, 2026a, 2026b, 2026c), U.S. SEC (2026), NASDAQ (2026), IVEZIC (2026c) e QURECA (2026).

Nota: Datas de conclusão, salvo indicação em contrário; valores aproximados, quando divulgados. A operação com a Elisity permanecia pendente de aprovação regulatória no fechamento deste artigo. QRNG: gerador quântico de números aleatórios.

Do ponto de vista da soberania seletiva, o resultado é uma convergência inédita de papéis sob um único controlador: o mesmo grupo empresarial desenvolve a capacidade computacional que ameaça a criptografia atual, oferta as contramedidas quânticas e pós-quânticas e passa a fornecer a política de contenção da rede do cliente. Há, ainda, uma dimensão panóptica específica. Plataformas de microssegmentação dependem, por construção, de um inventário detalhado de dispositivos, identidades e fluxos; quando gerenciadas por fornecedor estrangeiro, esse mapa da rede, que em uma organização de Defesa equivale a um retrato de sua superfície de ataque, passa a situar-se na órbita jurisdicional do controlador. Para operadores brasileiros de infraestrutura crítica, hospitais inclusive, a adoção de uma pilha integrada desse tipo concentraria em uma mesma jurisdição as camadas criptográfica, de rede e de telemetria, exatamente a combinação que a variável de jurisdição dinâmica pretende tornar visível.

A consolidação, contudo, não equivale à oferta de uma transição pós-quântica completa. Análise publicada logo após o anúncio sustenta que a operação torna a IonQ uma empresa de segurança maior sem preencher a maior parte das lacunas de sua oferta pós-quântica: a segmentação limita o que um dispositivo vulnerável pode alcançar, mas não protege tráfego já interceptado por um adversário nem impede assinaturas forjadas; não foram identificados produtos públicos do grupo para certificados pós-quânticos ou assinatura de código; o módulo da ID Quantique declarado “pronto para FIPS 140-3” ainda não dispunha de certificado do National Institute of Standards and Technology (NIST); e a base de clientes da Elisity, concentrada em hospitais e fabricantes, reúne justamente os dispositivos menos aptos a executar algoritmos pós-quânticos (IVEZIC, 2026c). A ressalva reforça a tese deste artigo: assim como QKD e PQC (seção 4.2), *Zero Trust* e PQC são camadas complementares, e não substitutas. A segmentação contém o dano, mas não neutraliza a estratégia Harvest Now, Decrypt Later (HNDL), de captura presente de dados cifrados para decifração futura, cujo enfrentamento continua a depender de inventário criptográfico, migração de algoritmos e governança de chaves e certificados.

O caso oferece, por isso, um teste concreto para o IM-PQC, cujas quatro dimensões, prontidão técnica (D1), conformidade legal-regulatória (D2), maturidade de governança (D3) e exposição ao risco quântico (D4), são detalhadas na seção 4.4.1. Um índice de maturidade que avaliasse apenas a presença de soluções contratadas poderia classificar como madura uma organização que tivesse adquirido, de um único fornecedor estrangeiro, um pacote integrado de PQC, QKD e *Zero Trust*. A leitura de soberania seletiva sugere o contrário: a dimensão de governança (D3) deve registrar a estrutura de controle e a jurisdição dos fornecedores criptográficos e de segurança de rede, tratando mudanças societárias como gatilho de reavaliação; a dimensão de exposição ao risco quântico (D4) deve considerar a concentração dessas camadas em um mesmo controlador; e a prontidão técnica (D1) deve exigir que o inventário criptográfico seja auditável pela própria organização, e não exclusivamente derivado da telemetria do fornecedor.

### 4.2.3 Capital, estrutura de mercado e concentração do *quantum stack*

A concentração de propriedade tem um correspondente financeiro. O Quantum Technology Monitor 2026, da McKinsey, estima que o investimento em startups de tecnologias quânticas alcançou US$ 12,6 bilhões em 2025, o que corresponde a 6,3 vezes o volume de 2024. A mudança não foi apenas quantitativa: a parcela proveniente de fontes públicas caiu de cerca de um terço em 2024 para apenas 3% em 2025, enquanto aproximadamente 60% do capital do ano se concentrou nos dez maiores negócios. No mesmo período, empresas de computação quântica superaram US$ 1 bilhão em receita global. Os universos estatísticos não são idênticos, investimento abrange startups de tecnologias quânticas, ao passo que a receita citada se refere a empresas de computação quântica, e, por isso, esses números não devem ser convertidos mecanicamente em uma razão contábil “capital/receita”. Em conjunto, porém, eles descrevem um setor ainda jovem, de receita relativamente estreita e forte concentração de capital privado (MCKINSEY & COMPANY, 2026).

Ao fim de agosto de 2026, pelo menos cinco empresas de computação quântica

haviam alcançado bolsas dos Estados Unidos naquele ano (Infleqtion, Xanadu, Quantinuum, IQM e Pasqal), evidenciando uma mudança relevante na estrutura de financiamento do setor (INFLEQTION, 2026; XANADU, 2026; QUANTINUUM, 2026; IQM, 2026; PASQAL, 2026).

Quadro 4 — Sinais de mercado e de Estado na cadeia quântica (8 a 15 out. 2026)

| Ator / evento | Fato | Sinal para a soberania seletiva |
|---|---|---|
| Departamento de Guerra dos EUA, Subsecretaria de Pesquisa e Engenharia (USW(R&E)) | Pacote de cerca de US$ 350 milhões (8 out.): ≈ US$ 200 milhões para empresas no Estágio C da Quantum Benchmarking Initiative (QBI) da Defense Advanced Research Projects Agency (DARPA) e empréstimo condicional de ≈ US$ 150 milhões do *Office of Strategic Capital* à PsiQuantum, para manufatura e prototipagem | O capital público, reduzido a 3% do investimento em *startups* em 2025, retorna como crédito estratégico à capacidade fabril doméstica: a Defesa passa a ancorar a cadeia, e não apenas a comprá-la. |
| DARPA – QBI, Estágio C | Atom Computing, Diraq, IBM e IonQ (acordo de até US$ 300 milhões) somam-se a Microsoft e PsiQuantum: seis empresas e seis modalidades em fase de verificação da escala de utilidade até 2033 | O Estado não escolhe vencedora: financia verificação independente de múltiplas modalidades, lógica coerente com a recomendação de não apostar prematuramente em uma única arquitetura. |
| Universal Quantum (Reino Unido) | Série A superior a US$ 100 milhões; execução de contrato de US$ 77 milhões com o Centro Aeroespacial Alemão (DLR) | Confirma o DLR como contratante-âncora (seção 4.5): a encomenda pública precede e atrai o capital privado. |
| Qilimanjaro Quantum Tech (Espanha) | Primeiro fechamento de Série A de € 19,6 milhões: € 10 milhões da Indra, via IndraMind, e € 9,6 milhões da SETT, entidade pública vinculada ao Ministério para a Transformação Digital | Empresa de defesa e ente público ancoram capacidade soberana para defesa, segurança e indústria, arranjo análogo ao proposto para as Empresas Estratégicas de Defesa (EED) brasileiras. |
| Infleqtion, Leonardo e Nova Systems | £ 9 milhões da Innovate UK para sistema dual de radiogoniometria com átomos de Rydberg, desenvolvido com a Leonardo; parceria com a Nova Systems para avaliar sistemas quânticos para a Defesa australiana (AUKUS) | Integradores de defesa, com capacidade de teste e avaliação, fazem a ponte entre tecnologia promissora e capacidade confiável, o salto de TRL 3 para TRL 6 visado na seção 4.4.2. |

Fonte: Adaptado de QURECA (2026), *Quantum Signal*, ed. 16, 15 out. 2026.

Nota: A coluna “sinal” constitui interpretação dos autores à luz da matriz de soberania seletiva.

A semana que se seguiu ao anúncio da Elisity ofereceu, ademais, um retrato condensado de como capital privado e poder estatal passaram a operar em conjunto na cadeia quântica. O boletim *Quantum Signal*, da QURECA, reuniu em sua 16ª edição (15 de outubro de 2026) eventos que, lidos pela matriz deste artigo, confirmam três

tendências: o retorno do Estado como financiador direto da manufatura, sob a forma de crédito e encomenda; o papel de contratantes-âncora de Defesa e de agências espaciais na conversão de protótipos em capacidades; e a articulação entre empresas de defesa e *startups* quânticas para formar capacidade soberana. O Quadro 4 preserva a lógica do boletim, que associa a cada fato um "sinal" interpretativo, e a traduz para a leitura de soberania seletiva.

### 4.3 Lições cruzadas: nuclear e inteligência artificial

A estratégia de resiliência quântica não parte de um vácuo institucional. O Brasil acumula experiência de enfrentamento a regimes de negação tecnológica na Defesa e testemunha, hoje, novos mecanismos de estrangulamento na computação voltada à IA (SCHARRE, 2023). O cruzamento dessas trajetórias oferece o mapa preditivo das barreiras que incidirão sobre o esforço quântico.

#### 4.3.1 O legado nuclear brasileiro

Iniciado de forma estruturada nos anos 1970 sob liderança das Forças Armadas, e consolidado pela propulsão nuclear da Marinha e por empresas como Nuclep e Amazul, o Programa Nuclear Brasileiro é a mais robusta experiência endógena de superação de interdições. O Acordo Brasil-Alemanha de 1975 buscava a transferência integral do ciclo do combustível.

Sob pressão dos EUA e dos arranjos que criaram o Grupo de Fornecedores Nucleares (NSG), os componentes mais críticos foram sonegados ou transferidos de forma incompleta (PATTI, 2021). A resposta brasileira não foi capitular, mas desenvolver rota nativa: o enriquecimento por ultracentrifugação com mancais magnéticos, no Centro Tecnológico da Marinha em São Paulo (Aramar).

A lição é transponível. A autonomia nuclear não veio de dominar toda a cadeia, mas de identificar o elo insubstituível, o enriquecimento, e protegê-lo com investimento contínuo e quadros estáveis. O mesmo raciocínio seletivo deve orientar a resposta quântica.

### 4.3.2 A governança de compute na era da IA

No século XXI, os regimes de negação migraram da fiscalização física de materiais radioativos para a interdição lógica de *clusters* de alto desempenho (*compute governance*). As regras do Bureau of Industry and Security (BIS) dos EUA marcaram um divisor de águas na governança da IA (ALLEN, 2022).

Sob o argumento de conter a modernização militar de rivais, impuseram limites à exportação de GPUs de ponta e do maquinário de litografia EUV da holandesa ASML (ALLISON *et al.*, 2021). A lição decisiva para o setor quântico vem da expansão dessas regras para a nuvem.

Como entidades sancionadas contornavam o bloqueio de chips alugando processamento em *data centers* ocidentais, os EUA impuseram exigências de *Know-Your-Customer* (KYC) a provedores de nuvem (BUCHANAN; IMBRIE, 2022). Encerramentos unilaterais de contas comprovaram que a nuvem é extensão territorializada do poder do Estado onde ficam os servidores, com revogação sumária de acesso, sem defesa comercial ou diplomática.

A transposição para a quântica é direta. O acesso a computadores quânticos far-se-á, por anos, via nuvem (QCaaS), camada já sujeita aos mesmos mecanismos de KYC e revogação hoje aplicados à IA. Quem depender de nuvem estrangeira para criptoanálise ou simulação militar herdará, automaticamente, a vulnerabilidade demonstrada no setor de inteligência artificial.

Para sistematizar essa hipótese, o Quadro 5 compara três experiências de restrição tecnológica, nuclear, inteligência artificial e tecnologias quânticas, a partir de quatro vetores comuns: natureza dual, foco da interdição, mecanismos de controle e capital humano.

O cruzamento revela uma dupla pinça sobre a quântica: ela herda as restrições físicas de duplo uso do setor nuclear (criogenia e lasers) e sofre a interdição lógica por KYC em nuvem, típica da IA. Ignorar essa classificação é condenar os futuros sistemas de comando e controle a um colapso operacional programado por terceiros.

Quadro 5 – Matriz de transposição analítica (Nuclear × IA × Quântica)

| Vetor | Programa Nuclear | Inteligência Artificial | Tecnologias Quânticas | Lição para o Brasil |
|---|---|---|---|---|
| Natureza dual | Delimitada por tratados (pacífico vs. bélico) | Difusa, difícil fiscalizar na camada de *software* | Intrínseca e imediata (sensores, relógios, PQC) | O nexo militar é nativo; a Defesa não pode esperar a comercialização. |
| Foco da interdição | Insumos físicos escassos (urânio), metalurgia | Capacidade computacional (*compute*) e litografia EUV | Suporte físico (criogenia) e acesso QCaaS | O bloqueio migra da compra de *hardware* para o corte de acesso à nuvem. |
| Mecanismo de controle | Inspeções físicas e selos da Agência Internacional de Energia Atômica (AIEA) | Regulação de KYC digital e listas de entidades | Listas de duplo uso (Wassenaar) e travas no *firmware* | O *hardware* importado traz amarras digitais (travas por GPS/ *firmware*). |
| Capital humano | Engenharia nuclear e metalurgia de Estado | Especialistas em *deep learning* nas *big techs* | Física de materiais e engenharia de RF | Risco de *brain drain*; reter talentos em instituições científicas e tecnológicas militares. |

Fonte: Autores (2026)

### 4.3.3 O regime de controle das tecnologias quânticas: mapeamento das imposições nacionais

As lições cruzadas deixam de ser prospectivas quando se examina o regime de controle já em vigor sobre a própria cadeia quântica. Com o Arranjo de Wassenaar paralisado pelo veto russo desde 2022, os controles migraram para a lógica do "*Wassenaar minus one*": Estados Unidos, Reino Unido, França, Espanha, Países Baixos, Canadá, Itália, Japão e Austrália passaram a editar controles nacionais harmonizados, porém unilaterais, sobre computação quântica, semicondutores e manufatura aditiva (CSIS, 2024; PARLAMENTO EUROPEU, 2025). O traço comum é a incidência sobre bens de duplo uso, cuja natureza militar-civil é, na quântica, indissociável desde a origem.

O exemplo mais concreto dessa harmonização é o limiar técnico de corte. Em julho de 2024, Reino Unido, França, Espanha, Países Baixos e Canadá adotaram, de forma idêntica, restrições à exportação de computadores quânticos com mais de 34

qubits e taxa de erro abaixo de determinado patamar, invocando segurança nacional (SPARKES, 2024). Para uma potência média, o dado relevante não é o número, mas o precedente: o acesso a *hardware* acima de um patamar de utilidade criptoanalítica passa a depender de licença discricionária do país de origem.

A restrição mais sensível para a periferia tecnológica, contudo, não recai sobre a compra de máquinas, mas sobre o acesso remoto via nuvem (QCaaS), onde a coerção opera por contrato, e não apenas por lista de exportação. Os termos de uso das principais plataformas ocidentais incorporam cláusulas de conformidade com sanções, de suspensão discricionária e de inspeção das cargas de trabalho: a IBM declara ter inserido linguagem contratual que barra aplicações potencialmente danosas e condiciona o acesso aos sistemas de ponta a contratos identificados; a Microsoft Azure Quantum reserva-se o direito de processar e inspecionar os circuitos submetidos; e o Google Quantum AI sequer oferece cadastro aberto, admitindo apenas usuários previamente aprovados (IVEZIC, 2026d). Nesses instrumentos, a distinção entre uso militar e civil raramente é nominal: ela ingressa por incorporação do regime de sanções e exportação do país-sede e pela faculdade de revogação sumária do acesso. Daí decorre uma implicação prática direta para a auditoria contratual: verificar um contrato de QCaaS ou de computação de alto desempenho exige examinar não a existência de uma cláusula explícita de “uso militar”, mas as cláusulas de lei aplicável, de conformidade com controles de exportação e de rescisão unilateral, por onde a hipótese de interdição efetivamente se realiza.

### 4.3.4 Respostas estatais comparadas: a resiliência física chinesa e a imunidade lógica alemã

Se a subseção anterior mapeou as imposições, cabe examinar como dois Estados as converteram em estratégia. China e Alemanha oferecem arquétipos opostos e complementares: a primeira persegue a resiliência física do *hardware* contra sanções externas; a segunda, a imunidade lógica de suas infraestruturas críticas de informação. Nenhum dos modelos é integralmente transponível ao Brasil, mas a combinação de ambos delimita o repertório disponível a uma potência média.

A resposta chinesa, cuja vertente de substituição de importações na criogenia foi descrita na seção 4.1, articulou *hardware* proprietário e nuvem soberana. Em maio de 2023, a China Telecom capitalizou com cerca de 3 bilhões de yuans uma subsidiária dedicada, a China Telecom Quantum Group (CTQG), que opera a plataforma Tianyan, lançada em novembro do mesmo ano. Em dezembro de 2024 foi apresentado o Tianyan-504, computador supercondutor baseado no chip Xiaohong, de 504 qubits, desenvolvido com o Centro de Excelência em Informação Quântica da Academia Chinesa de Ciências e a QuantumCTek. Até julho de 2025, a plataforma acumulava mais de 37 milhões de acessos de usuários em 60 países e mais de 2 milhões de experimentos processados (THE QUANTUM INSIDER, 2025; IVEZIC, 2026a). O efeito estratégico é preciso: ao dispor de QCaaS estatal, Pequim neutraliza sobre si os efeitos panóptico e de estrangulamento que as plataformas norte-americanas exercem, invertendo a lógica da interdependência armada descrita na seção 2.

A resposta alemã opera na camada lógica e é normativa, não industrial. O *Bundesamt für Sicherheit in der Informationstechnik* (BSI) antecipou-se ao mercado ao tornar vinculante, na diretriz técnica TR-02102-1 atualizada em 2025, o uso de arquiteturas híbridas, que combinam um algoritmo pós-quântico a um esquema clássico executado simultaneamente, em todas as implantações de PQC. Mais relevante para a Defesa, o BSI não se limitou a adotar os padrões do NIST: recomenda também FrodoKEM e Classic McEliece como alternativas conservadoras, de modo a não concentrar todo o risco criptográfico em uma única família matemática. Os prazos são explícitos, migração até 2030 para operadores de infraestrutura crítica e até 2032 para as demais organizações, em linha com a declaração conjunta firmada com dezessete parceiros europeus em novembro de 2024 (BSI, 2025).

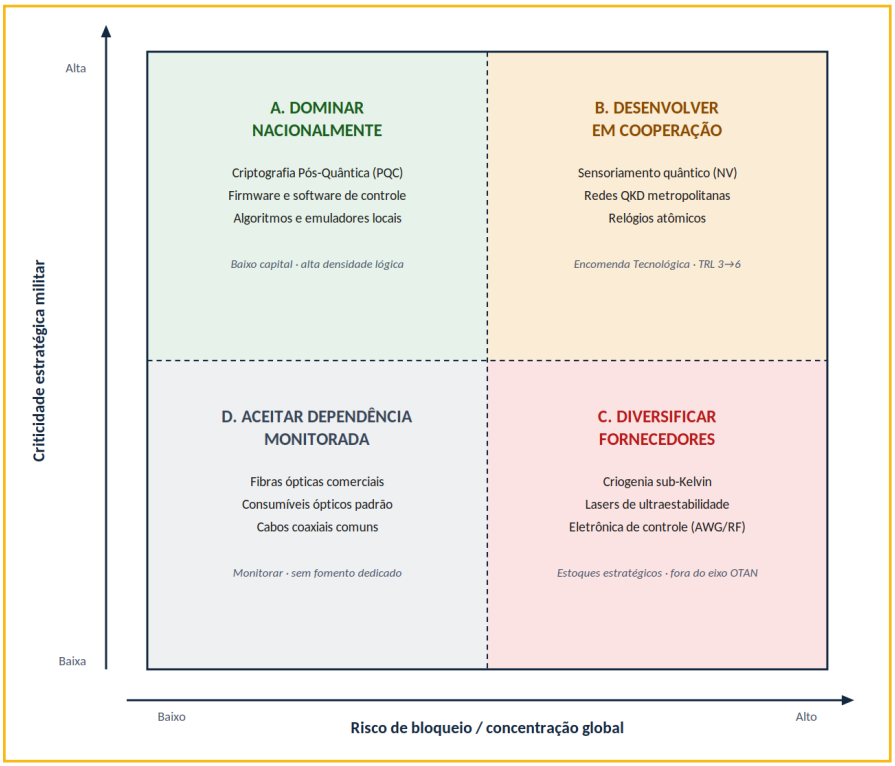
A leitura conjunta revela que nenhuma das potências examinadas persegue autossuficiência integral: cada uma consolida o elo em que já possuía vantagem preexistente e o protege com salvaguarda própria: controle de exportação nos Estados Unidos (seção 4.3.3); substituição de importações e nuvem estatal na China; e regulação prospectiva e encomenda pública na Alemanha. É precisamente essa lógica seletiva, e não a nacionalização integral, que a matriz proposta a seguir transpõe ao caso brasileiro.

## 4.4 A matriz de soberania seletiva

A cadeia quântica é densamente oligopolizada e vulnerável à interdependência armada, o que impõe rejeitar a autossuficiência integral. Diante das restrições orçamentárias e da alta barreira de capital das fundições avançadas, o país deve adotar a doutrina da Soberania Tecnológica Seletiva (EDLER *et al*., 2020; MOREIRA, 2014).

Essa abordagem discrimina os elos da cadeia em quatro categorias de intervenção, orientadas por três variáveis centrais, criticidade militar do elo, risco de bloqueio internacional e capacidade endógena preexistente de absorção tecnológica, e complementadas por um multiplicador de concentração empresarial/jurisdicional. Esse multiplicador captura situações em que marcas, fornecedores ou produtos aparentemente distintos convergem para o mesmo controlador, mesma infraestrutura crítica ou mesmo *layer* habilitador. A Figura 2 sintetiza o modelo.

Figura 2 – Matriz estratégica de criticidade vs. risco de bloqueio




Fonte: Autores (2026)

### 4.4.1 Dominar nacionalmente

Esta categoria reúne os elos de máxima criticidade para o sigilo de Estado, com baixa barreira de capital e alta densidade de conhecimento lógico executável localmente. O alvo primordial é a Criptografia Pós-Quântica (PQC).

A transição dos sistemas do governo e das Forças Armadas, hoje baseados em RSA ou curvas elípticas, vulneráveis ao algoritmo de Shor, para algoritmos resistentes é tarefa eminentemente de *software*. Como o código pode ser auditado e compilado em servidores isolados (*air-gapped*), sem insumos físicos exóticos, o Brasil tem a obrigação estratégica de dominar esse elo, o que pode ser realizado por intermédio do Instituto Militar de Engenharia (IME), do Instituto Tecnológico de Aeronáutica (ITA) e das agências de inteligência.

A substância técnica desse domínio já está disponível. Em 2024, o NIST padronizou os primeiros algoritmos pós-quânticos, FIPS 203, 204 e 205, oferecendo uma base madura para a migração (NIST, 2024). O desafio brasileiro não é inventar criptografia, mas implementá-la com cripto-agilidade: a capacidade de trocar algoritmos sem redesenhar sistemas.

O risco não se limita à confidencialidade. A validade jurídica das assinaturas digitais brasileiras, ancorada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), depende de algoritmos que um computador quântico poderá forjar; a continuidade das autoridades certificadoras exige, assim, um plano de migração criptográfica com a mesma prioridade dada à proteção de dados.

Isso pressupõe um inventário criptográfico nacional, o mapeamento de todos os certificados, chaves e algoritmos em uso no governo e nas Forças Armadas. Sem esse inventário, é impossível priorizar a migração ou medir o progresso, o que torna indispensável um instrumento de maturidade como o descrito a seguir.

Um exemplo concreto de operacionalização da estratégia de dominar nacionalmente é o Índice de Maturidade em Criptografia Pós-Quântica (IM-PQC),

construído a partir de uma revisão sistemática de literatura (PRISMA 2020, 47 estudos) para medir a prontidão organizacional na transição para a PQC (AUTOR, 2026).

O índice integra quatro dimensões, prontidão técnica (D1), conformidade legal-regulatória (D2), maturidade de governança (D3) e exposição ao risco quântico (D4), e combina os métodos Fuzzy-AHP (Analytic Hierarchy Process difuso) e TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) em um escore auditável de 0 a 100, estratificado em quatro níveis de maturidade (N1 a N4).

A aplicabilidade imediata desse domínio também aparece em arquiteturas nacionais propostas para preservação de evidências digitais. Modelo apresentado no CBCTQ 2026 combina PQC, captura em borda, *blockchain* permissionada, armazenamento soberano e princípios de *Zero Trust* para preservar autenticidade, integridade, rastreabilidade e não repúdio de dados que precisam permanecer verificáveis por longos períodos (PAULA; GONÇALVES, 2026). Embora concebida para cidades inteligentes e cadeia de custódia, a arquitetura oferece uma analogia operacional direta para a Defesa: registros de missão, telemetria, inteligência, logs de comando e evidências cibernéticas exigem proteção criptográfica durável e auditável, sem dependência exclusiva de serviços estrangeiros. Essa mesma combinação entre PQC e *Zero Trust* começa a ser oferecida em pacote por grupos estrangeiros, como sinaliza a operação IonQ–Elisity (seção 4.2.2); a diferença estratégica não está na arquitetura em si, mas em quem detém o controle de suas chaves, políticas e inventários.

A lacuna que o IM-PQC preenche é visível no setor financeiro: as Resoluções CMN nº 4.893/2021 e BCB nº 85/2021 exigem políticas de segurança cibernética, mas não a prontidão pós-quântica. A urgência é reforçada pela estratégia HNDL, que expõe hoje dados a serem decifrados no futuro, e pelo teorema de Mosca (X + Y > Z), segundo o qual há risco sempre que o tempo de sigilo exigido (X), somado ao tempo de migração (Y), supera o prazo até a existência de um computador quântico criptograficamente relevante (Z), raciocínio que se estende às infraestruturas de Defesa Nacional.

No plano material, a mesma lógica recomenda domínio seletivo das etapas *downstream* dos isótopos críticos, e não uma corrida indiscriminada por plantas de enriquecimento. Preparação de fontes atômicas, encapsulamento, células e *dispensers*, validação de ensaio e pureza química e rastreabilidade de lotes são capacidades de capital e sensibilidade regulatória inferiores às de separação isotópica, mas elevam controle, auditabilidade e resiliência. Para uma potência média, esse é precisamente o tipo de elo em que a soberania por unidade de investimento tende a ser maior.

### 4.4.2 Desenvolver em cooperação

Abrange ativos de elevada relevância tática e forte caráter dual, com alto risco de bloqueio externo, mas nos quais o Brasil já detém massa crítica científica em nível inicial de maturidade tecnológica (Technology Readiness Level, TRL), passível de impulso pelo poder de compra do Estado. Os alvos são o sensoriamento quântico (gravímetros e magnetômetros com centros nitrogênio-vacância (NV) em diamante), as redes metropolitanas de QKD e os relógios atômicos de alta estabilidade.

Gravímetros e magnetômetros quânticos são divisores de águas para a navegação inercial autônoma do PROSUB, permitindo trânsito indetectável sem depender de sinais externos. O Estado deve financiar consórcios entre Instituições Científicas, Tecnológicas e de Inovação (ICTs) públicas com competências já identificadas no Quadro 2, como UFPE, UNICAMP, CBPF e UFRJ, em articulação com ICTs militares como o IME, o IEAv e o IPqM, e empresas da BID, via Encomenda Tecnológica, elevando esses sistemas de bancada (TRL 3) ao padrão de homologação militar (TRL 6). Experiências recentes, como a parceria da Infleqtion com a Leonardo, no Reino Unido, e com a Nova Systems, na Austrália (Quadro 4), mostram que esse salto depende de integradores de defesa com capacidade própria de teste, avaliação e garantia de capacidade.

### 4.4.3 Diversificar fornecedores

Aplica-se a componentes físicos de alta complexidade industrial, cuja produção nacional do zero é economicamente proibitiva a médio prazo, como o *hardware*

criogênico sub-Kelvin e os lasers de ultraestabilidade. A estratégia substitui a dependência de fornecedor único por diversificação geográfica e diplomática, homologando fornecedores fora do eixo da OTAN e mantendo estoques estratégicos de reposição sob controle das Forças Armadas.

### 4.4.4 Aceitar dependência monitorada

Aplica-se a componentes de baixa criticidade militar e alta substituibilidade comercial, como consumíveis ópticos padrão, fibras comerciais e cabos coaxiais. Aqui o Estado não deve gastar recursos escassos de fomento, aceitando a dependência das cadeias globais e limitando-se ao monitoramento de vulnerabilidades e a testes de integridade.

## 4.5 Implicações para a Base Industrial de Defesa

Operacionalizar a Matriz de Soberania Tecnológica Seletiva exige superar a governança fragmentada e mobilizar de forma coordenada os instrumentos da BID. O ecossistema institucional, a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END), tem uma lacuna crítica: embora eleja os setores espacial, cibernético e nuclear como pilares, permanece silente quanto à quântica (BRASIL, 2020a; 2020b), tratada como subcomponente do cibernético e não como infraestrutura crítica transversal.

O primeiro passo é rever a END, inserindo as tecnologias quânticas e a IA disruptiva como sub-eixo estratégico prioritário. Isso legitima que o Ministério da Defesa, com o Ministério da Ciência, Tecnologia e Inovação (MCTI) e o Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC), criem um comitê interministerial permanente, uma Iniciativa Quântica de Defesa, para atuar como inteligência de mercado do Estado, mapear vulnerabilidades das ICTs e blindar projetos contra descontinuidades fiscais.

A mobilização da BID deve aplicar com rigor a Lei nº 12.598/2012 (BRASIL, 2012). O Estado deve certificar as poucas empresas de fotônica e *software* quântico como Empresas Estratégicas de Defesa (EED), com proteção contra a desnacionalização predatória, incentivos fiscais e preferência nas compras públicas do Ministério da Defesa.

A inteligência de suprimentos deve alcançar também o controle empresarial do *quantum stack*. Além de estoques, *lead times* e países de origem, a Iniciativa Quântica de Defesa deveria manter um mapa de controle societário e de financiamento dos fornecedores estratégicos, identificando aquisições, SPACs, IPOs, participações de controle e concentração em plataformas habilitadoras. A finalidade não é acompanhar preços de ativos financeiros, mas detectar cedo quando uma mudança de capital altera a jurisdição, a autonomia de manutenção, a política de licenciamento ou a quantidade de fontes realmente independentes. Em setores jovens e fortemente financiados por capital privado, a estrutura societária pode mudar mais rapidamente do que o ciclo de aquisição de um sistema militar. A operação IonQ–Elisity exemplifica o tipo de evento que esse monitoramento deveria capturar: um anúncio societário ocorrido no exterior que, se concluído, altera simultaneamente o controlador de soluções de segurança de rede, de QKD e de PQC potencialmente presentes em infraestruturas nacionais.

O desenho institucional dessa mobilização pode inspirar-se em modelo já testado. A Alemanha utiliza o Centro Aeroespacial Alemão (DLR) como contratante-âncora: por meio da *DLR Quantum Computing Initiative*, o ministério federal da economia destinou 740 milhões de Euros em quatro anos a partir de 2022, dos quais cerca de 80% são investidos diretamente na indústria, mediante contratos com consórcios sujeitos a metas rígidas de entrega de protótipos operados em instalações soberanas (ALEMANHA, 2022). O modelo continua a produzir efeitos: em outubro de 2026, a britânica Universal Quantum, ao captar mais de US$ 100 milhões, já executava contrato de US$ 77 milhões com o DLR (QURECA, 2026), evidência de que a encomenda pública previsível atrai capital privado, em vez de substituí-lo. O arranjo resolve dois problemas que afligem o fomento brasileiro: assegura demanda pública previsível e ancora em território nacional a propriedade intelectual gerada.

Por fim, a dependência de QCaaS exige uma estratégia de transição combinando emulação local de alto desempenho, ambientes soberanos para dados sensíveis, portabilidade entre SDKs e participação seletiva em plataformas externas para

pesquisa não classificada. Enquanto não houver *hardware* quântico soberano em escala operacional, a Defesa deve impedir que dados de inteligência, chaves, modelos criptográficos sensíveis ou cargas classificadas sejam enviados a nuvens estrangeiras. A supercomputação clássica nacional pode sustentar emuladores e bancadas de teste, enquanto uma infraestrutura distribuída conecta ICTs e laboratórios sob regras comuns de segurança, reduzindo simultaneamente o efeito panóptico e a dependência de um único provedor.

## 5 CONCLUSÃO

A transição para a era quântica não é fenômeno estritamente técnico, mas um rearranjo das estruturas de poder e coerção internacional. Ao mostrar que a cadeia quântica está crivada de pontos de estrangulamento controlados de forma assimétrica, o artigo evidenciou que o risco para o Brasil é contemporâneo e estrutural, manifesto na perda silenciosa de autonomia decisória.

Cinco eixos sustentam a resposta soberana: governança interministerial capaz de mapear dependências; retenção e formação estruturada de capital humano; infraestrutura científica distribuída e interoperável; inteligência de suprimentos que inclua controle societário, concentração de capital e jurisdição; e priorização seletiva dos elos realmente críticos. Os dados de 2026 reforçam que o país dispõe de base acadêmica suficiente para abandonar o diagnóstico de "ausência de capacidade", mas ainda precisa construir mecanismos capazes de converter essa capacidade em autonomia tecnológica e operacional.

A incorporação dos isótopos críticos torna essa conclusão ainda mais concreta. A cadeia feedstock–refino–enriquecimento–fonte atômica–QPU demonstra que a soberania quântica pode ser perdida em miligramas de materiais invisíveis às estatísticas agregadas. O Estado não precisa nacionalizar toda a cadeia, mas precisa saber quanto consome, quem realmente enriquece, quantas instalações independentes sustentam a reposição, qual a jurisdição efetiva dessas instalações e por quanto tempo seu estoque mantém a plataforma operacional.

Concretamente, isso significa dominar nacionalmente a PQC e seus processos de migração, mobilizar a BID por encomendas tecnológicas em sensoriamento e comunicações de interesse dual, estruturar trajetórias de formação e retenção de especialistas, desenvolver capacidades *downstream* de materiais e mitigar a dependência de nuvem por ambientes locais e infraestrutura distribuída. A competição quântica brasileira não será decidida pela simples contagem de qubits adquiridos nem pelo número de startups declaradas, mas pela capacidade do Estado de transformar conhecimento disperso em cadeias resilientes, propriedade intelectual controlável, produtos homologáveis e liberdade de ação.

Para a Defesa Nacional, isso inclui institucionalizar due diligence periódica sobre a jurisdição efetiva e a estrutura de controle dos fornecedores, tratar fusões, aquisições e mudanças de capital como gatilhos de reavaliação e evitar que uma diversificação apenas nominal esconda concentração funcional em poucos produtores, plataformas ou *layers* habilitadores. O anúncio da aquisição da Elisity pela IonQ, em outubro de 2026, demonstra que esse gatilho deixou de ser hipotético: a consolidação que começou nos componentes da pilha quântica já alcança a camada de segurança das redes, e a transição pós-quântica de setores críticos só será soberana se o Estado for capaz de medir, por instrumentos como o IM-PQC, não apenas a maturidade técnica das organizações, mas também a jurisdição de quem lhes fornece a proteção.

## REFERÊNCIAS

ABREU, D.; VASSOLER, G.; FARIAS, F. Mapa das Tecnologias Quânticas no Brasil: Plataforma de Observação do Ecossistema Nacional. *In*: 46º CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO; 1º SIMPÓSIO BRASILEIRO DE COMPUTAÇÃO E COMUNICAÇÃO QUÂNTICAS, 2026, Gramado. **Anais [...]**. 2026.

AGUILAR, G. H. **Implementation of a quantum network within the city of Rio de Janeiro. Plenary Session 5**. Congresso Brasileiro de Ciências e Tecnologias Quânticas (CBCTQ 2026), Niterói, RJ, 25 set. 2026. Comunicação oral.

ALEMANHA. Deutsches Zentrum für Luft- und Raumfahrt (DLR). **DLR Quantum Computing Initiative (QCI)**. Colônia: DLR, 2022.

ALLEN, G. C. **Choking off China's Access to the Future of AI. Washington, D.C.**: Center for Strategic and International Studies (CSIS), 2022.

ALLISON, G. et al. **The Great Tech Rivalry: China vs the U.S. Cambridge, MA**: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2021.

AUTOR. [Referência omitida para garantir a avaliação cega pelos pares]. 2026.

BRASIL. **Lei nº 12.598, de 21 de março de 2012**. Diário Oficial da União, Brasília, 22 mar. 2012.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa (END)**. Brasília: MD, 2020a.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa (PND)**. Brasília: MD, 2020b.

BUCHANAN, B.; IMBRIE, A. **The New Fire**: War, Peace, and Democracy in the Age of AI. Cambridge, MA: MIT Press, 2022.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). **Kryptographische Verfahren**: Empfehlungen und Schlüssellängen. Technische Richtlinie TR-02102-1, versão 2025-01. Bonn: BSI, 2025.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS). **Rethinking the Wassenaar Minus One Strategy**. Washington, D.C.: CSIS, 2024.

DANSA, C.; CÉSAR, M. Quem se interessa por computação quântica no Brasil? Curiosidade, trajetórias formativas e institucionalização limitada. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS E TECNOLOGIAS QUÂNTICAS (CBCTQ), 2026, Niterói. **Anais [...]**. 2026.

EDLER, J. et al. **Technology sovereignty**: from demand to concept. Fraunhofer ISI Discussion Papers Innovation Systems, n. 66, 2020.

FARRELL, H.; NEWMAN, A. Weaponized interdependence: how global economic networks shape state coercion. **International Security**, v. 44, n. 1, p. 42-79, 2019. DOI: 10.1162/ISEC_a_00351.

FIOTT, D. **Strategic autonomy**: towards a European political concept. Paris: European Union Institute for Security Studies (EUISS), Brief 30, 2018.

GIDNEY, C. **How to factor 2048 bit RSA integers with less than a million noisy qubits**. arXiv:2505.15917, 2025. DOI: 10.48550/arXiv.2505.15917.

GIDNEY, C.; EKERÅ, M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **Quantum**, v. 5, p. 433, 2021. DOI: 10.22331/q-2021-04-15-433.

INFLEQTION. **Infleqtion Becomes First Neutral-Atom Quantum Company to Go Public**. 17 fev. 2026. NYSE: INFQ.

IONQ. **IonQ Completes Acquisition of ID Quantique, Cementing Leadership in Quantum Networking and Secure Communications**. College Park, MD, 6 maio 2025.

IONQ. **IonQ Completes Acquisition of Nexus Photonics, Securing Scalable Manufacturing for Quantum Systems**. College Park, MD, 10 set. 2026b.

IONQ. **IonQ Completes Acquisition of Skyloom, Expanding Quantum Networking and Secure Communications Capabilities**. College Park, MD, 28 jan. 2026c.

IONQ. **IonQ Completes Acquisition of SkyWater Technology**. College Park, MD, 31 jul. 2026a.

IQM QUANTUM COMPUTERS. **IQM, a Global Leader for Quantum Computing, to Become the First Listed European Quantum Company, Through Merger with Real Asset Acquisition Corp**. 23 fev. 2026; e início de negociação pública em jul. 2026.

**ISÓTOPOS CRÍTICOS PARA COMPUTAÇÃO QUÂNTICA**: risco da cadeia de suprimentos e implicações para o Brasil. Relatório executivo para tomadores de decisão. Data-base: 4 set. 2026.

IVEZIC, M. **China's quantum supply chain: how export controls are building what they sought to prevent**. PostQuantum.com, 9 abr. 2026a. Disponível em: https://postquantum.com/china-quantum-ambition/china-supply-chain-self-sufficiency/. Acesso em: 10 set. 2026.

IVEZIC, M. **Every US quantum computer runs on foreign parts and foreign inventions**. PostQuantum.com, 15 jul. 2026b. Disponível em: https://postquantum.com/quantum-sovereignty/who-built-the-quantum-stack/.

IVEZIC, M. **IonQ is buying Elisity for access to CISOs**: most of the post-quantum capabilities those CISOs need first are still missing. PostQuantum.com, 13 out. 2026c. Disponível em: https://postquantum.com/security-pqc/ionq-elisity-acquisition/.

IVEZIC, M. **"They'll Just Rent One"**: the quantum threat model nobody bothered to check. PostQuantum.com, 20 maio 2026d. Disponível em: https://postquantum.com/post-quantum/criminals-rent-quantum-crqc/.

MCKINSEY & COMPANY. McKinsey Quantum Technology Monitor 2026: A commercial tipping point. 28 abr. 2026. Inclui dados de investimento, concentração de deals e receita do setor de computação quântica.

MIGON, E. X. F. G.; ARAÚJO-MOREIRA, F. M. **Soberania tecnológica começa na Física**. O Estado de S. Paulo, São Paulo, p. A6, 17 out. 2026. Espaço Aberto.

MOREIRA, W. S. Cerceamento e restrições tecnológicas à indústria de Defesa. *In*: ALMEIDA, P.; ACIOLY, L. (org.). **Estratégias de defesa nacional**: desafios para o Brasil no novo milênio. Rio de Janeiro: Ipea, 2014.

NASDAQ. **How IonQ is growing its merchant supplier role in quantum space**. Nova York: Nasdaq, 2026. Disponível em: https://www.nasdaq.com/articles/how-ionq-growing-its-merchant-supplier-role-quantum-space.

NIST. **Post-quantum cryptography standards**: FIPS 203, FIPS 204 e FIPS 205. Gaithersburg: National Institute of Standards and Technology, 2024.

PARLAMENTO EUROPEU. **Dual-use export controls as tools of EU economic security**. Bruxelas: European Parliamentary Research Service (EPRS), Briefing PE 777.960, 2025.

PASQAL. **Pasqal and Bleichroeder Acquisition Corp. II Complete Business Combination**. Paris/New York, 27 ago. 2026. Ações passaram a negociar na Nasdaq sob o ticker PSQL em 28 ago. 2026.

PATTI, C. **Brazil in the Global Nuclear Order**, 1945-2018. Baltimore: Johns Hopkins University Press, 2021.

PAULA, M. D.; GONÇALVES, P. H. Soberania Digital e Criptografia Pós-Quântica Aplicadas à Cadeia de Custódia de Evidências Digitais em Cidades Inteligentes. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS E TECNOLOGIAS QUÂNTICAS (CBCTQ), 2026, Niterói. **Anais [...]**. 2026.

QUANTINUUM. **Quantinuum Announces Closing of Upsized Initial Public Offering**. Broomfield, CO, 5 jun. 2026. IPO na Nasdaq (QNT), com US$ 1,68 bilhão em recursos brutos.

QURECA. **Quantum Signal by QURECA**: from breakthroughs to impact. Issue 16 (Weekly Signal). Londres: QURECA, 15 out. 2026.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM, v. 21, n. 2, p. 120-126, 1978. DOI: 10.1145/359340.359342.

ROSE, S. et al. **Zero Trust Architecture**. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207.

SASTRY, G. et al. **Computing Power and the Governance of Artificial Intelligence**. arXiv:2402.08797, 2024. DOI: 10.48550/arXiv.2402.08797.

SCHARRE, P. **Four Battlegrounds**: Power in the Age of Artificial Intelligence. New York: W. W. Norton & Company, 2023.

SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, v. 26, n. 5, p. 1484-1509, 1997. DOI: 10.1137/S0097539795293172.

SOUZA, S. G.; FRÓES, M. M.; DIAS, A. F. S. Computação Quântica Brasileira: Entre o Avanço Científico e a Dependência Estrutural Global. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS E TECNOLOGIAS QUÂNTICAS (CBCTQ), 2026, Niterói. **Anais [...]**. 2026.

SPARKES, M. S**ecretive international discussions impose export controls on quantum computers**. New Scientist, Londres, jul. 2024.

SWIFT. **About Swift**. La Hulpe, Bélgica: SWIFT, 2025. Disponível em: https://www.swift.com/about-us.

THE QUANTUM INSIDER. **China opens its superconducting quantum computer for commercial use**. 14 out. 2025.

UNIÃO EUROPEIA. Conselho da União Europeia. Regulamento (UE) 2022/345 do Conselho, de 1 de março de 2022, que altera o Regulamento (UE) n.º 833/2014 que impõe medidas restritivas tendo em conta as ações da Rússia que desestabilizam a situação na Ucrânia. **Jornal Oficial da União Europeia**, L 63, p. 1-4, 2 mar. 2022.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION (U.S. SEC). **IonQ, Inc. Exhibit 21.1**: List of Subsidiaries as of February 25, 2026. Washington, D.C., 2026.

XANADU. **Xanadu Quantum Technologies Limited Announces Closing of Business Combination with Crane Harbor Acquisition Corp**. 26 mar. 2026. Nasdaq/TSX: XNDU.

YAHOO FINANCE. **IonQ to acquire cybersecurity firm Elisity**. 12 out. 2026. Disponível em: https://finance.yahoo.com/technology/ai/articles/ionq-acquire-cybersecurity-firm-elisity-113002861.html. Acesso em: 10 set. 2026.

## Autoria


### 1 Manoel Fernandes Amaral Filho

Graduado em Ciências Militares e Direito; Pesquisador; Coronel Veterano do Exército Brasileiro; Mestre em Operações Militares pela Escola de Aperfeiçoamento de Oficiais; Doutorando em Engenharia Elétrica

https://orcid.org/0009-0006-6496-0539 • manoel.amaral@ufam.edu.br

### 2 Bruno Costa Marinho

Graduado em Ciências Militares pela Academia Militar das Agulhas Negras; Graduado em Direito pela Universidade Estácio de Sá; Mestre em Direito Ambiental pela Universidade do Estado do Amazonas; Doutor em Propriedade Intelectual e Inovação pelo Instituto Nacional da Propriedade Industrial; Professor Colaborador da Universidade do Estado do Amazonas; Pesquisador do Laboratório de Ciências Militares da Escola de Comando e Estado-Maior do Exército; Chefe

https://orcid.org/0000-0002-5394-5652 • marinho.bruno@ime.eb.br

### 3 Anderson Fernandes Pereira dos Santos

Engenheiro de Computação pelo Instituto Militar de Engenharia; Doutor em Modelagem Computacional pelo Laboratório Nacional de Computação Científica; Pós-Doutorado em Computação Quântica pelo Laboratório Nacional de Computação Científica; Pesquisador do Centro de Inovação Tecnológica Venturus em tecnologias computação quântica e segurança cibernética; Pesquisador, Professor

https://orcid.org/0000-0002-6754-4809 • anderson@ime.eb.br


## Como citar este artigo

AMARAL FILHO, M. F.; MARINHO, B. C.; SANTOS, A. F. P. Soberania quântica seletiva: cadeias de suprimentos, autonomia estratégica e defesa. **InterAção**, Santa Maria, v. 17, n. 3, e99516, p. 1-38, 2026. DOI 10.5902/2357797599516. Disponível em: https://dx.doi.org/10.5902/2357797599516. Acesso em: dia mês abreviado. ano.

## DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Ferramentas de inteligência artificial foram utilizadas como apoio à redação, à revisão, à formatação e à verificação de referências, sob supervisão integral dos autores, que revisaram todo o conteúdo e assumem responsabilidade exclusiva pela formulação teórica, pela análise e pelas conclusões.