Comunicações Quânticas para a Soberania Tecnológica Nacional

Jorge Frederico Vieira Campos Flores
Comando de Defesa Cibernética (ComDCiber), Brasília/DF – Brasil

***Resumo* – O artigo examina, de forma sucinta, o panorama das comunicações quânticas no cenário mundial e brasileiro, ressaltando seu papel estratégico para a soberania tecnológica e digital do país. São analisados o contexto histórico, os avanços recentes e as principais limitações e desafios enfrentados pelo Brasil, como a baixa capacidade industrial, a fragmentação de esforços de pesquisa e a dependência de insumos críticos externos. O texto supre uma lacuna na literatura ao consolidar um levantamento de fatores limitantes nacionais, apresentando uma análise qualitativa, a partir da qual propõem-se possibilidades de mitigação que podem orientar políticas públicas, investimentos e iniciativas de inovação, em prol do fortalecimento da autonomia nacional em comunicações quânticas.**

***Palavras-Chave* – Comunicações Quânticas, Tecnologias Quânticas, Soberania Tecnológica.**

I. INTRODUÇÃO

As Tecnologias Quânticas (TQ) utilizam princípios da física quântica para criar ferramentas e sistemas inovadores, viabilizando avanços em áreas como computação, comunicações e sensoriamento. Essas tecnologias prometem revolucionar setores industriais, científicos e de Defesa, tornando-se estratégicas para o futuro.

Diversos centros de competência nacionais pesquisam TQ, impulsionando avanços científicos e tecnológicos no país. Entre eles, o SENAI CIMATEC, em Salvador, abriga o Centro de Competência EMBRAPII em TQ e o *QuIIN*, atuando em pesquisa, formação de profissionais e inovação aberta, com forte apoio do MCTI e da EMBRAPII [1]-[2]. Universidades, como o IME, integram redes de comunicações quânticas [3]-[4] e colaboram em projetos de criptografia e comunicações seguras, conectando instituições por fibras óticas e feixes de fótons. Cerca de 30 instituições de ensino superior e centros de pesquisa [5] participam dessas iniciativas, consolidando o país no cenário internacional das TQ. Mesmo assim, o país constava apenas como o 21º lugar em produção científica em TQ em dezembro de 2024 [6].

As Nações Unidas elegeram o ano de 2025 como o Ano da Quântica, de forma a celebrar o centenário das TQ e suas aplicações [7]. Ao longo do tempo, foram registradas diversas iniciativas no país, como o Instituto do Milênio e a Rede KyaTera [8].

As Comunicações Quânticas e Criptografia Quântica são áreas intrinsecamente ligadas e coexistentes. Enquanto a comunicação quântica depende da criptografia quântica para estabelecer canais seguros, a criptografia quântica utiliza a comunicação quântica para transmitir as chaves de forma segura.

A soberania reflete a capacidade da defesa do poder do país sem interferências externas, no sentido de preservar a sua autodeterminação e não delegar decisões críticas do Estado a outros países e organizações. Há uma soberania tecnológica, no sentido de os domínios do ciberespaço e tecnológico do país deverem ser protegidos e dominados, e ainda, uma soberania digital, em prol da qual o país deve exercer controle sobre sua própria infraestrutura digital e uso de dados, independente de influências externas. Tal conceito é especialmente relevante no contexto contemporâneo de segurança de dados sensíveis, defesa cibernética e de tecnologias emergentes, como as TQ [9].

A. Metodologia

Embora diversas pesquisas tenham abordado a temática das comunicações quânticas, ainda há escassez na literatura de um levantamento consolidado de problemas que limitam o desenvolvimento das comunicações quânticas no Brasil, e de que forma eles podem ser mitigados.

De modo a contribuir para a solução do problema de pesquisa supracitado, a metodologia adotada incluiu a apresentação desse levantamento a partir de pesquisas e de revisão bibliográfica em bases de dados abertos de universidades, centros de pesquisa e órgãos governamentais do Brasil e do exterior, expondo resumidamente o contexto histórico desses desenvolvimentos em nível nacional e internacional. Além disso, foram identificados os principais problemas enfrentados pelo país no desenvolvimento desses tecnologias, bem como apresentada uma análise qualitativa desses problemas, a partir da qual são propostas soluções para mitigá-los.

Muitas das análises e recomendações aqui apresentadas repercutem discussões, coleta de informações e de possibilidades de soluções durante a Sala Temática de Comunicações Quânticas do 2º Encontro Nacional de Tecnologias Quânticas para a Defesa [10], realizado em novembro de 2024 em Brasília.

II. JUSTIFICATIVA HISTÓRICA: ALGUMAS INICIATIVAS BRASILEIRAS RECENTES EM TQ

Desde os anos 2000, o país tem investido recursos financeiros e empenhado recursos humanos significativos em diversas iniciativas tecnológicas emergentes, tais como:

- o Instituto do Milênio e a rede KyaTera [11], na qual foram instaladas fibras óticas apagadas, um dos pré-requisitos para implementação de redes quânticas;
- pesquisas do CEPESC da ABIN em equipamentos criptográficos integrando Redes Privadas Virtuais (VPN) [12] tradicionais com criptografia de Estado, e desenvolvimento

J. F. V. C. Flores, jorgefrederico.flores@eb.mil.br

de chaves criptográficas via curvas elípticas em um contexto pós-quântico [13]-[14];

- mapeamento de ecossistemas de pesquisa, formação de recursos humanos e produção científica por meio do Instituto Nacional de Ciência e Tecnologia de Informação Quântica (INCT-IQ) [5]; e

- proposta de uma rede de comunicações quânticas na Esplanada dos Ministérios pela RENASIC (GSI/PR) em 2010, para implementação de uma rede quântica com Distribuição de Chaves Quânticas (QKD) por fibra e ar, e concatenação com uma plataforma chamada "KeyBITS" com ciframento *one-time pad* (OTP) [15]. Tal rede não foi implementada, e não há evidência em fontes abertas de sua implantação, tanto que a primeira rede considerada quântica do Brasil [16] é a Rede Rio Quântica que, em 2021, surgiu como iniciativa de grupos de pesquisa acadêmicos [17]-[18], buscando construir e estabelecer uma rede de comunicação quântica metropolitana no Rio de Janeiro.

Desde 2021, por ocasião de um Seminário [19], a Secretaria de Produtos de Defesa (SEPROD) do Ministério da Defesa (MD) [20] divulgou suas ações de fomento e articulação estratégica de iniciativas de comunicações quânticas na tripla hélice (Defesa, Indústria de Defesa e Academia), integrando ICTs na discussão e execução de projetos. Sua atuação é fundamental para criar ecossistemas de TQ [21] com foco em Defesa, estabelecendo condições para diferentes iniciativas espalhadas pelo país poderem se articular de forma eficaz.

Desde 2023, o IME assumiu protagonismo no tema ao desenvolver componentes críticos internamente [22] e criar enlaces de Óptica de Espaço Livre (FSO) [18] com possibilidade de servir como *testbeds* para QKD terrestre, por meio do Projeto Quantum, em cujo bojo está inserido o Projeto Rede Hermes Quântica, inserido na Rede Rio Quântica.

Desde seu lançamento em 2023 e 2024, a iniciativa quântica da FAPESP, chamada *QuTIa* (*Quantum Technologies Initiative*) [23], tem desempenhado um papel estratégico no desenvolvimento de recursos humanos, infraestrutura de pesquisa e consolidação de comunicações quânticas no Brasil, incluindo infraestrutura de redes e *testbeds* em comunicações quânticas e consolidação do ecossistema e internacionalização.

Em 2023, a UFPE lançou um edital de uma iniciativa (Quanta UFPE) para desenvolver equipamentos e protocolos de base para uma futura estratégia nacional de comunicação quântica [24]. No mesmo ano, o ITA idealizou o projeto INFREQUANT, um dos pioneiros em QKD no Brasil, voltado para comunicações para uso dual e estratégico [25].

Em março de 2024, a FINEP lançou um edital de seleção pública para subvenção econômica à inovação em fluxo contínuo, voltado para o desenvolvimento de projetos baseados em TQ [26].

Em 2024, a Iniciativa em Inteligência Artificial em Tecnologias Quânticas (IATQ), do Programa Pró-Defesa V [27], articula cerca de 40 instituições públicas e privadas, civis e militares, em prol da segurança e defesa nacional e da formulação de políticas públicas em nível estratégico.

Em 14 de fevereiro de 2025, a Portaria GM-MD nº 840 divulgou as tecnologias críticas para defesa nacional. As TQ figuram como uma das categorias principais e explicitam as comunicações quânticas seguras e os sensores quânticos como especificidades tecnológicas prioritárias para o desenvolvimento de projetos estratégicos [28].

III. CONTEXTO MUNDIAL E TECNOLÓGICO DAS COMUNICAÇÕES QUÂNTICAS

Os enlaces de comunicações quânticas e das redes de distribuição de chaves ponto a ponto normalmente são redes distintas das existentes em redes metropolitanas normais envolvendo roteamento, algo que só será uma possibilidade em enlaces quânticos se houver mecanismos de Internet Quântica, ainda muito distantes de serem implementados [29].

Além disso, os enlaces quânticos, dependendo do protocolo a ser utilizado, não costumam ser muito resilientes à copropagação com os canais clássicos, exigindo a necessidade de fibras escuras para tráfego da informação quântica. Entretanto, atualmente, já se demonstrou ser viável a copropagação de sinais quânticos e clássicos por meio de técnicas de Multiplexação por Divisão de Comprimento de Onda (WDM) [30]. De qualquer forma, para funcionar bem, há a necessidade de uma camada adicional para a gestão das chaves, e transformar a gestão das chaves em uma rede própria responsável por receber, armazenar, processar, sincronizar, relatar e fornecer as chaves geradas pelos módulos quânticos para as aplicações criptográficas [31].

O canal de comunicações quânticas por fibra óptica, em via de regra, não deve ter extensão maior do que 100 km, uma limitação tecnológica em função da atenuação e da fragilidade dos estados quânticos, a não ser que haja um posto intermediário com um repetidor seguro ou nó confiável, possibilitando a extensão por mais 100 km adiante. É uma estrutura cara, mas viável de ser montada. Uma conexão por espaço livre pode ser mais custosa devido à necessidade de equipamentos de apontamento, rastreamento e correção das distorções causadas por efeitos atmosféricos. Corre o risco de indisponibilidade no caso de condições atmosféricas mais severas, e por isso nem sempre estará operacional, não se aplicando no caso de comunicações mais críticas.

Por conta das perdas sofridas nas fibras, são necessários algoritmos de reconciliação para geração de chaves, para garantir a coincidência perfeita das chaves geradas nas duas pontas. Além disso, é interessante a implementação de técnicas alternativas de QKD, como a distribuição baseada em coerência (TF-QKD) possibilitando dobrar a distância da transmissão segura e integrar comunicações quânticas à infraestrutura de comunicações clássicas já existente, reduzindo custos e complexidade [32].

Em compensação, a implementação de comunicações quânticas por espaço livre permite baixa latência. Em que pese o custo do equipamento (incluindo geradores e detectores de fótons e equipamentos de rastreamento e estabilização do feixe laser), e as limitações físicas inerentes às técnicas de FSO, existe um mercado de FSO passível de ser explorado para transmissão de fótons individuais e fótons compartilhados.

As técnicas de Criptografia Pós-quântica (PQC) e de QKD encontram-se atualmente em nível de prontidão tecnológica (TRL) alto [33]. Enquanto a PQC está com estágio avançado de padronização e implementações em software e hardware, a QKD, embora funcional e comercialmente disponível, ainda enfrenta desafios limitando seu TRL em larga escala. Existe um número crescente de

empresas estrangeiras desenvolvedoras de QKD, a exemplo da *IDQuantique* suíça e da *LuxQuanta* espanhola, podendo resultar em embargos tecnológicos a qualquer momento (produtos de uso geral em telecomunicações podem se tornar restritos e cerceados, se forem considerados por outros países como tecnologia dual de interesse da Defesa), além da questão de patentes registradas em outros países, e por outros países no Brasil, e de algumas barreiras significativas de infraestrutura, custo e interoperabilidade. Além disso, há uma vantagem tecnológica natural por parte dos países detentores de acesso mais fácil a insumos tecnológicos, infraestrutura científica, facilidades laboratoriais, financiamento em P&D e acesso ao hardware quântico, resultando em um *gap* iminente entre países tecnologicamente soberanos e países mais desfavorecidos economicamente sem condições de financiar pesquisas em QKD, PQC e computação quântica.

Um caso a ser colocado são as restrições impostas pela *State Cryptography Administration* (“SCA”) chinesa [34] para importação e exportação de equipamentos de criptografia. Além disso, alguns dos algoritmos de PQC do NIST norte-americano, embora desenvolvidos sob as condições de terem domínio público, sem patentes restritivas e disponíveis para implementação sem custos de licenciamento, são proprietários da IBM [35]-[36].

Os países do arco do conhecimento, a citar EUA, Reino Unido, Austrália, Alemanha, China e Rússia, possuem suas próprias iniciativas quânticas, aportando bilhões de dólares em pesquisa e desenvolvimento [37]-[38] e concebendo *roadmaps* para desenvolvimento de TQ para Defesa, incluindo comunicações [39].

Os enlaces de QKD por Variáveis Contínuas (CV-QKD) não requerem tecnologias em risco de serem restritas, porque são tecnologias e componentes comuns de telecomunicações clássicas (lasers contínuos, moduladores eletro-ópticos, fibras ópticas, detectores PIN e detectores homodinos relativamente simples), maduros e consolidados, com TRL mais elevado. Além disso, não precisam de tecnologias exóticas ou restritas, como detectores de fótons únicos e os refrigerados criogenicamente (podem ser utilizados detectores PIN e detectores convencionais de telecomunicações, exceto em casos bem específicos como aplicações aéreas e satelitais exigindo baixa relação sinal-ruído, precisão e estabilidade extrema), sendo plausível a sua miniaturização e integração espacial em equipamentos comerciais. Os sinais, normalmente provenientes de fontes clássicas, precisam ser preparados em uma configuração quântica, “traduzidos” para um estado quântico por meio de um mecanismo de *feature map*. Por conta disso, os cálculos são mais complexos, mas podem ser acelerados por hardwares de aceleração, por exemplo, embarcados em FPGAs ou em GPUs.

Em outros países, principalmente aqueles que buscam fortalecer a sua soberania tecnológica, há *startups* quânticas desenvolvedoras de tecnologias de interesse nacional, voltadas para setores estratégicos como comunicações seguras, sensoriamento e computação. Isso inclui tanto países altamente industrializados como economias emergentes, como por exemplo o Chile, que identificou nichos viáveis de serem implementados [40]-[41], com aplicabilidade real para a Defesa nas áreas de comunicações e criptografia quântica.

Há a questão dos protocolos: quando algum protocolo se mostra muito interessante, ele é extensivamente analisado, testado e auditado até realmente se atestar a sua segurança contra ataques. Isso vale tanto para criptografia clássica quanto para protocolos quânticos. Nesse sentido, vários protocolos para comunicações e criptografia quântica foram testados, chegando até um certo ponto que foram quebrados, ou tiveram vulnerabilidades exploradas de alguma forma. Até mesmo o BB-84, um dos mais conhecidos protocolos de QKD, já provou ser vulnerável ao ataque conhecido como *PNS Attack* [42].

As comunicações quânticas, devido a suas conhecidas limitações, são suscetíveis a negação de serviço, e a várias interferências, assim como a comunicação clássica, uma vez que a segurança da QKD garantida pelas leis da física não impede a obstrução, a interrupção ou a degradação do canal. A diferença é que, quando se trabalha com poucos fótons, as comunicações quânticas “revelam” o que ocorreu no canal, pois qualquer tentativa de interceptação ou modificação do canal quântico introduz erros mensuráveis.

Por fim, existe um “vale da morte” referindo-se a um vácuo entre pesquisa científica (TRL baixo) e aplicações comerciais e operacionais (TRL alto), pois muitas tecnologias quânticas, inclusive comunicações, enfrentam longos ciclos de maturação, alta complexidade de prototipagem, custo elevado de infraestrutura, falta de interoperabilidade e padronização, e baixa conexão entre academia e indústria.

IV. PROBLEMAS BRASILEIROS NA ÁREA DE COMUNICAÇÕES QUÂNTICAS

As linhas de pesquisa no país não são puramente vocacionadas para TQ. Na realidade, elas são inseridas em grupos de pesquisa maiores já consolidados nas áreas de Telecomunicações, Física, Informática, Materiais, entre outros.

O país se tornou gradualmente incipiente na área de microeletrônica e de optoeletrônicos. Já houve programas estratégicos importantes, como o Programa Nacional de Microeletrônica (PNM) e iniciativas como o CEITEC no estado do Rio Grande do Sul, mas faltou continuidade de investimento e estratégia industrial de longo prazo, não se consolidando uma cadeia produtiva nacional em semicondutores, e causando uma dependência em termos de importações de componentes críticos para QKD, geradores quânticos de números aleatórios (QRNG), FSO e detecção óptica de precisão. Hoje, os grupos de pesquisa e empresas com conhecimento e competência em crescimento de materiais, dispositivos fotônicos e processos de microfabricação, essenciais para o futuro das comunicações quânticas, são incipientes, dispersos e com baixa capacidade de produção em escala, em um contexto de perda de competitividade global, além de sofrer o impacto da evasão de talentos para o exterior, em virtude da falta de perspectiva de carreira em TQ no país.

Além disso, há falta de consórcios no país a exemplo dos estabelecidos pela União Europeia. Falta uma mentalidade de colimação de esforços de alinhamento dos múltiplos atores da tríplice hélice em torno de objetivos estratégicos comuns.

Em adição, há um baixo número de indústrias de TIC no Brasil, sendo que esse setor está majoritariamente concentrado em serviços de desenvolvimento de software, consultoria em TIC, suporte técnico, infraestrutura e operadoras de telecomunicações. Em compensação, é pouco representado nas áreas de base tecnológica estratégica, crítica e emergente, como fabricação de hardware, projetos de semicondutores, produção de dispositivos fotônicos e ópticos

e computação quântica, essenciais para a soberania tecnológica e o futuro das comunicações seguras.

Também existe um número considerável de depósito de patentes estrangeiras em TQ no Brasil, exigindo um esforço posterior de solicitação de licenciamento e pagamento de *royalties*. Tal fato traz implicações estratégicas tais como o ônus ao desenvolvimento industrial e comercial em setores estratégicos, o risco de dependência tecnológica e vulnerabilidades geopolíticas, exigindo monitoramento contínuo do portfólio de patentes no país para evitar litígios legais posteriores.

Por fim, é característico da gestão orçamentária brasileira haver contingenciamentos e cortes parciais de recursos financeiros nas Forças Armadas e nas universidades, fator que afeta projetos estratégicos de Defesa, manutenção de equipamentos e infraestrutura, e P&D em produtos de uso dual, e também a produção científica, tecnológica e de inovação do país. Com isso, os projetos do Ministério da Defesa, mesmo sendo considerados sensíveis ou prioritários, possuem um andamento mais lento do que o planejado e sofrem atrasos.

V. PROPOSTAS DE SOLUÇÕES PARA ALCANÇAR A SOBERANIA TECNOLÓGICA EM COMUNICAÇÕES QUÂNTICAS NO PAÍS

Considerando os fatores históricos e conjunturais apresentados nas seções II e III, e com base na análise dos problemas listados na Seção IV, uma extensa lista de propostas de soluções é apresentada a seguir, visando mitigar ou eliminar as dificuldades e, assim, alcançar a soberania tecnológica e o desenvolvimento tecnológico autóctone em comunicações quânticas no país:

1) O provimento de recursos orçamentários e humanos por meio do Plano Nacional de Computação Quântica, até 2034, em linhas de esforço críticas e cruciais em TQ [43].

2) A busca de possibilidades via FNDCT, e articulações com a EMBRAPII como catalisadora, fomentadora e financiadora ágil e desburocratizada com foco em TRL médios e altos, por meio de seleção de centros vocacionados para temas como fotônica, comunicações ópticas, microeletrônica, segurança da informação e computação de alto desempenho, direcionando chamadas específicas para desenvolvimento de QKD, QRNG e FSO, redes quânticas e dispositivos críticos, e também por meio da indução de formação de consórcios público-privados entre Instituições Científicas-Tecnológicas (ICT), empresas nacionais de TIC, Defesa, Base Industrial de Defesa e *startups deep tech*, buscando mitigar lacunas históricas como a falta de coordenação entre ciência e indústria, a incipiência de infraestrutura institucional, o baixo volume de patentes nacionais em TQ e a dependência de insumos críticos importados.

3) A formação de redes e de ecossistemas robustos e maduros, a constituição de ligas acadêmicas e a criação de comunidades de prática em TQ, essenciais para transformar a capacidade científica dispersa em soberania tecnológica estruturada. Essas redes promovem integração, compartilhamento, inovação colaborativa, capilaridade de esforços e presença estratégica, combatendo a fragmentação e a evasão de talentos do país.

4) O pivoteamento das indústrias, inclusive por meio da Indústria 4.0 (política de neoindustrialização brasileira, abrangendo áreas como IA, TQ, Internet das Coisas, automação industrial e segurança cibernética) com o propósito de aproveitar as plantas industriais comuns de TIC e convertê-las em áreas fabris de desenvolvimento de comunicações quânticas, aliado à formação de parcerias e à cultura de *startups*, algo que começou a ser valorizado e incentivado na última década e pode ser fomentado pela Defesa em função da alta tolerância a riscos garantido pela Lei Complementar nº 182/2021 (Lei das *Startups*), um contexto favorável para a aposta em pesquisa.

5) O maior engajamento da Base Industrial de Defesa como fator fundamental para o desenvolvimento de comunicações quânticas em ambientes seguros de interesse estratégico, além da fabricação de componentes chave para comunicações quânticas essenciais para a Defesa, tais como sensores para aplicações aéreas, terrestres e satelitais.

6) O desenvolvimento da capacidade de certificação de produtos de comunicações e criptografia quântica, por exemplo, no sentido de atestar se os QRNG são verdadeiros (*True Random*), contribuindo para aumentar sobremaneira a segurança de sistemas criptográficos de Defesa, com garantia de funcionalidade e segurança real, e prevenção contra produtos de "caixa-preta" com *backdoors*, atendendo a requisitos para segurança de Estado e Defesa.

7) A visão clara, estratégica e coordenada de objetivos e requisitos operacionais, com o apoio direto da Defesa no processo de desenvolvimento de TQ de interesse dual para o país, com a previsão de um financiamento dedicado por meio de uma ação orçamentária exclusiva para desenvolvimento de TQ para mitigar efeitos de contingenciamento de verba, algo que contribuirá para trazer vantagem estratégica, como abordado inclusive na Concepção Estratégica de Futuro do Exército ("Força 40") [44] com visão de curto, médio e longo prazo, focando nos ciclos quadrienais das Leis Orçamentárias Anuais (LOA) e em orçamento exclusivo. Uma possibilidade é a busca de cooperação e de aportes de recursos junto à FINEP e ao CNPq, engajamento da BID, além da busca de fabricantes alternativos, países e rotas tecnológicas alternativas. Todas essas iniciativas devem primar por entregáveis tangíveis em prol da sociedade.

8) A utilização do capital intelectual brasileiro, na indústria, na Defesa e no meio acadêmico, para redirecionar esforços no desenvolvimento das áreas de microeletrônica, optoeletrônicos e fotônicos. É importante e vital criar uma indústria nacional de microeletrônica e de dispositivos fotônicos. Com a quantidade de aplicações diferentes propiciadas pelas comunicações quânticas, há um vasto campo de possibilidades, nos próximos anos, de criação de laboratórios de óptica quântica e formação de mercado na área, algo fundamental para o Brasil alcançar autonomia e competitividade em TQ, especialmente em comunicações.

9) O direcionamento estratégico para tecnologias livres de embargos, de fácil e rápida nacionalização por empresas brasileiras, visando à autonomia tecnológica em comunicações quânticas. Uma opção é a fabricação de detectores convencionais, tais como os fotodiodos avalanche (APD) e diodos de avalanche de fóton único (SPAD). Outra é a produção de geradores quânticos de números aleatórios. Isso representaria um ganho significativo para a nacionalização de sistemas. Além disso, é interessante a formação de grupos de trabalho para analisar quais seriam os componentes críticos a serem desenvolvidos, para quais componentes deveria ser desenvolvido maior esforço de pesquisa e industrialização, com o aproveitamento do

fomento de *startups* ou empresas com base no *know-how* existente em termos de competências humanas.

10) O desenvolvimento de um plano de manutenção do ciclo de vida de TQ no país, incluindo aspectos como logística, transporte, treinamento e cuidados com o manuseio, para garantir a sustentabilidade e a continuidade das iniciativas brasileiras em TQ ao longo do tempo, assegurando a capacidade operacional, técnica e estratégica do país em comunicações e criptografia quântica ao longo dos anos.

11) A formação de alianças estratégicas com outros países, no sentido de receber transferência real de tecnologia (capacitação, acesso a processos produtivos, desenvolvimento conjunto e compartilhamento de *know-how*) para o desenvolvimento de TQ, incluindo comunicações quânticas, algo muito mais eficaz do que a simples importação de equipamentos. Isso reflete uma estratégia internacional consagrada para o desenvolvimento tecnológico sustentável, especialmente em áreas de alta complexidade e impacto estratégico como as TQ.

12) Alta disponibilidade nas redes óticas e satelitais, especialmente necessária quando se trata de comunicações seguras para a Defesa. A utilização das fibras óticas apagadas pode ser uma estratégia eficaz para comunicação, testes, desenvolvimento de protótipos de comunicação seguras e de *testbeds* para a Defesa em redes já existentes e ociosas, e em aneis óticos interligando instituições de interesse. O aspecto mais crítico a ser cuidado é a qualidade da fibra óptica, de forma a evitar interrupções no sinal e promover a alta disponibilidade necessária para um contexto de comunicações entre *data centers* de interesse da Defesa.

13) Testes piloto com FSO entre organizações militares da Defesa, com o objetivo de realizar provas de conceito, uma vez que um enlace com ângulos de abertura extremamente estreitos (de centenas ou milésimos de milirradianos), característicos de feixes de laser, são muito difíceis de serem interceptados, conferindo assim alto grau de confiabilidade e segurança no *link* quântico, permitindo a validação de comunicações quânticas seguras no espaço livre, especialmente em ambientes militares.

14) A conexão entre *data centers* com possibilidades de demonstração dos mecanismos de distribuição de chaves quânticas por protocolos ou métodos OTP, em comunicações em nuvem e em VPN, e com possibilidade até mesmo de emprego de *blockchain* por algum canal quântico. Uma vez demonstrados, deve haver um plano de sustentabilidade sólido para adoção de TQ pela Defesa, para as equipes de TIC da Defesa aproveitarem todas as vantagens das TQ em prol das comunicações, com parcerias para manutenção e P&D contínua em sistema de gestão e otimização de redes e chaves, com computação de alto desempenho (HPC) e computação quântica para *buffers* de chaves, sistemas de gestão de nós confiáveis e de gestão da banda para troca de chaves, dependendo da distância do enlace. Tal contexto permite uma adoção sustentável e operacional de comunicações quânticas no contexto da Defesa, integrando QKD, TIC, nuvem, VPN, *blockchain* e HPC, com foco em segurança e soberania nacional.

15) O incentivo à pesquisa de *couriers* como alternativa viável para distribuição de chaves seguras em aplicações militares navais e aeronáuticas, onde as restrições físicas e geográficas podem limitar o uso de QKD em tempo real. Uma possibilidade de aplicação naval: as bases navais receberiam as chaves concentradas por meio de canais seguros quânticos, e os navios aportando por ali trocariam chaves por uma conexão interna local, recebendo um conjunto de chaves grandes para utilização durante um certo período. No setor aéreo, de forma similar: aeronaves pousando em uma determinada base receberiam chaves armazenadas em aeroportos. Se houver conexão entre as bases, o modelo de rede pode ser utilizado para distribuição das chaves no momento do pouso das aeronaves ou da atracação dos navios. Essa alternativa contornaria as limitações atuais do QKD, especialmente no contexto geográfico e operativo das Forças Armadas.

16) O uso de satélites, partindo da premissa de haver mais do que um nó e conectar todo o planeta por meio da atmosfera. Mesmo com as limitações da interferência da reflexão solar, é interessante o emprego de nanossatélites brasileiros (*CubeSat*) para, em contexto de Defesa, realizar a comunicação com submarinos, estações terrestres e aeronaves.

17) A revisão e a reavaliação dos protocolos de comunicações e criptografia quânticas voltadas para o aspecto da segurança, especialmente no contexto da Defesa, visando identificar quais protocolos de comunicações quânticas para a Defesa são mais resilientes a ataques quânticos ou clássicos.

18) A possibilidade de sistemas híbridos envolvendo QKD e PQC. Ambas são abordagens complementares e factíveis para desenvolver redes *Quantum Safe*, mesmo com suas respectivas limitações. Essa integração deve ser objeto de pesquisa prioritário, sobretudo para aplicações críticas de Defesa.

19) O desenvolvimento de sistemas de estabilização e de óptica adaptativa, essenciais para garantir desempenho e segurança, especialmente em ambientes móveis ou dinâmicos, como operações de Defesa, e para superar o desafio de lidar com a turbulência em comunicações quânticas via FSO.

VI. CONCLUSÃO

O presente artigo apresentou uma lista de problemas consolidados nas áreas de pesquisa, infraestrutura tecnológica, indústria, inovação, propriedade intelectual e gestão orçamentária, que representam um fator limitante para o desenvolvimento das comunicações quânticas no país.

Foi realizada uma análise de documentos normativos, de referências técnicas, entre outros, a partir da qual foi possível mapear um histórico sucinto de desenvolvimento das comunicações quânticas no Brasil e no exterior, bem como apontar problemas para o desenvolvimento delas no país. Com base nesses subsídios, foi possível ao autor analisar essas informações e apresentar uma extensa lista de propostas para mitigar aqueles problemas e buscar obter e fortalecer a soberania tecnológica e digital no país.

REFERÊNCIAS

[1] EMBRAPII. Mundo quântico. Disponível em <https://embrapii.org.br/mundo-quantico/>. Acesso em 25/06/2025

[2] AGÊNCIA GOV. MCTI e Embrapii vão investir R$ 60 milhões em centro de tecnologia quântica. Disponível em <https://agenciagov.ebc.com.br/noticias/202310/mcti-e-embrapii-vao-investir-r-60-milhoes-em-centro-de-tecnologia-quantica>. Acesso em 25/06/2025.

[3] BRASIL. Ministério da Ciência, Tecnologia e Inovação. Cientistas apresentam possibilidades para desenvolver a computação e internet quântica

no Brasil. Disponível em <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/08/cientistas-apresentam-possibilidades-para-desenvolver-a-computacao-e-internet-quantica-no-brasil>. Acesso em 25/06/2025

[4] UNIVERSIDADE FEDERAL FLUMINENSE. Rede de internet quântica integra instituições de ensino e pesquisa no Rio. Disponível em <https://www.uff.br/16-09-2024/rede-de-internet-quantica-integra-instituicoes-de-ensino-e-pesquisa-no-rio/>. Acesso em 25/06/2025

[5] INCT-IQ. O INCT Informação Quântica. Disponível em <https://inctiq.if.ufrj.br/about/>. Acesso em 25/06/2025.

[6] BORI AGÊNCIA. Em dez anos, Brasil perde força em pesquisa na área quântica, tema fundamental para soberania nacional. Disponível em <https://abori.com.br/ciencia/producao-ciencia-tecnologia-quanticas/>. Acesso em 25/06/2025

[7] UNESP. UNESCO celebra 2025 como o Ano Internacional da Ciência e Tecnologia Quânticas. Jornal da Unesp, 04/02/2025. Disponível em <https://jornal.unesp.br/2025/02/04/unesco-celebra-2025-como-o-ano-internacional-da-ciencia-e-tecnologia-quanticas/>. Acesso em 25/06/2025

[8] UNESP. A tecnologia quântica de segunda geração vai chegar ao Brasil?. Jornal da Unesp, 06/02/2023. Disponível em <https://jornal.unesp.br/2023/02/06/a-tecnologia-quantica-de-segunda-geracao-vai-chegar-ao-brasil/>. Acesso em 25/06/2025

[9] UNISINOS. Com o digital, nasceu uma nova soberania. Disponível em <https://www.ihu.unisinos.br/categorias/613336-com-o-digital-nasceu-uma-nova-soberania-entrevista-com-luciano-floridi>. Acesso em 25/06/2025.

[10] ABDI. ABDI marca presença em evento sobre tecnologias para a Defesa. Disponível em: <https://www.abdi.com.br/abdi-marca-presenca-em-evento-sobre-tecnologias-para-a-defesa/>. Acesso em: 01/09/2025.

[11] INOVAÇÃO TECNOLÓGICA. Rede Kyatera: a Internet da ciência brasileira. Disponível em: <https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=010150050603&id=010150050603>. Acesso em 25/06/2025

[12] CENTRO DE PESQUISA E DESENVOLVIMENTO PARA A SEGURANÇA DAS COMUNICAÇÕES (CEPESC). "Coletânea CEPESC": CEPESC, 2024. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/tecnologia/CEPESC_coletanea.pdf>. Acesso em 25/06/2025

[13] BRASIL. Ministério da Ciência, Tecnologia e Inovação. 28/11: 5. ABIN – Criptografia de Estado: uma decisão estratégica. YouTube, 2 dez. 2022. Disponível em: <https://www.youtube.com/watch?v=skw43EvvX58>. Acesso em 25/06/2025

[14] AGÊNCIA GOV. Abin é oficializada como Instituição Científica, Tecnológica e de Inovação. Disponível em: <https://agenciagov.ebc.com.br/noticias/202411/abin-e-oficializada-como-instituicao-cientifica-tecnologica-e-de-inovacao>. Acesso em 25/06/2025

[15] BARBOSA, Geraldo A. Infovia Quântica (QKD/keyBITS). [Apresentação]. Brasília, RENASIC/QuantaSEC, 26-27 out. 2010. 1 imagem. Disponível em: [RENASIC 1.png]. Acesso em: 25/06/2025.

[16] FAPESP. Primeira rede quântica do Brasil conecta cinco instituições no Rio. Disponível em: <https://namidia.fapesp.br/primeira-rede-quantica-do-brasil-conecta-cinco-instituicoes-no-rio/633490>. Acesso em: 01/09/2025.

[17] KHOURY, A. Z.; ALVES JR., N. "Projeto Rede Rio Quântica: sumário de divulgação". Disponível em: <https://rederio.br/sites/default/files/files/downloads/RRQ_Sumario_divulgacao.pdf>. Acesso em: 26/06/2025

[18] DEFESA NET. Instalado o primeiro link laser de comunicação no espaço livre do Exército Brasileiro. Disponível em: <https://www.defesanet.com.br/laser/instalado-o-primeiro-link-laser-de-comunicacao-no-espaco-livre-do-exercito-brasileiro/>. Acesso em: 25/06/2025.

[19] BRASIL. Ministério da Defesa. SEPROD promove Seminário de Tecnologias de Interesse da Defesa. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/seprod/noticias/seprod-promove-o-seminario-de-tecnologias-de-interesse-da-defesa>. Acesso em: 25/06/2025

[20] BRASIL. Ministério da Defesa. Conheça a Secretaria de Produtos de Defesa (SEPROD). Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/conheca-a-secretaria-de-produtos-de-defesa-seprod>. Acesso em: 25/06/2025

[21] CORRÊA, Fernanda. Ecossistema Quântico para Defesa. Palestra proferida no XXXI Ciclo de Estudos Estratégicos da ECEME, Rio de Janeiro, 17 jun. 2025.

[22] DEFESA AÉREA E NAVAL. IME desenvolve dispositivo emissor de fótons únicos. Disponível em: <https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/ime-desenvolve-dispositivo-emissor-de-fotons-unicos>. Acesso em: 25/06/2025

[23] FAPESP. QuTia. Disponível em: <https://fapesp.br/qutia>. Acesso em: 25/06/2025

[24] BRASIL. Ministério da Educação. Universidade Federal Rural de Pernambuco. Projeto de comunicação quântica contemplando em edital do CNPq com valor de R$ 2,9 milhões. Disponível em: <https://www.ufrpe.br/br/content/projeto-de-comunica%C3%A7%C3%A3o-qu%C3%A2ntica-contemplando-em-edital-do-cnpq-com-valor-de-r-29-milh%C3%B5es>. Acesso em: 25/06/2025

[25] FUNDAÇÃO CASIMIRO MONTENEGRO FILHO. Projeto INFREQUANT: iniciativa de pesquisadores do ITA é pioneira no campo da informação quântica. Disponível em: <https://fcmf.org.br/projeto-infrequant-iniciativa-de-pesquisadores-do-ita-e-pioneira-no-campo-da-informacao-quantica/>. Acesso em: 25/06/2025

[26] FINEP. "SELEÇÃO PÚBLICA MCTI/FINEP/FNDCT Subvenção Econômica à Inovação em Fluxo Contínuo Mais Inovação Brasil – Tecnologias Digitais". Disponível em: <http://www.finep.gov.br/images/chamadas-publicas/2024/04_03_2024_TC_Anexo_Rerratificado.pdf>. Acesso em: 25/06/2025

[27] BRASIL. ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO. XXXI Ciclo de Estudos Estratégicos. Disponível em: <https://www.eceme.eb.mil.br/noticias-eceme-m-pt/1945-cee-25-1>. Acesso em: 25/06/2025

[28] BRASIL. Ministério da Defesa. Portaria GM-MD nº 840, de 14 de fevereiro de 2025. Dispõe sobre as diretrizes para o desenvolvimento de capacidades autônomas no setor de defesa. Diário Oficial da União: seção 1, Brasília, DF, 17 fev. 2025. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-gm-md-n-840-de-14-de-fevereiro-de-2025-613426661>. Acesso em: 25/06/2025

[29] SWISSINFO. Pesquisadores fazem grande avanço na internet quântica. Disponível em: <https://www.swissinfo.ch/por/pesquisadores-fazem-grande-avan%C3%A7o-na-internet-qu%C3%A2ntica/47624510>. Acesso em: 25/06/2025

[30] INOVAÇÃO TECNOLÓGICA. Canais de dados quânticos e clássicos fluem pela mesma fibra óptica. Disponível em: <https://www.inovacaotecnologica.com.br/noticias/noticia.php?artigo=canais-dados-quanticos-classicos-fluem-pela-mesma-fibra-optica&id=010150230216>. Acesso em: 25/06/2025

[31] ITU. "Quantum Information Technology for Networks (QIT4N) – Deliverable D2.3 part 2: Quantum Network Architecture and Functional Building Blocks". Genebra, 2024. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/qit4n/Documents/D2.3%20part%202.pdf>. Acesso em: 25/06/2025

[32] DRIVINECO. Comunicação quântica quebra recordes: mensagens percorrem 254 km por cabos de fibra óptica convencionais. Disponível em: <https://www.drivingeco.com/pt/comunicacion-cuantica-rompe-records-mensajes-viajan-254-km-traves-cables-fibra-optica-convencional/>. Acesso em: 25/06/2025

[33] M. Krelina, "Quantum technology for military applications", EPJ Quantum Technology, vol. 8, n. 24, p. 22, 2021. Disponível em: <https://doi.org/10.1140/epjqt/s40507-021-00113-y>. Acesso em: 26/06/2025.

[34] COVINGTON. China Enacts Encryption Law. Inside Privacy, 31/10/2019. Disponível em <https://www.insideprivacy.com/data-security/china-enacts-encryption-law/>. Acesso em 26/06/2025

[35] CYBER MAGAZINE. NIST Standardises IBM's Post-Quantum Cryptography Algorithms Disponível em: <https://cybermagazine.com/articles/nist-standardises-ibms-post-quantum-cryptography-algorithms>. Acesso em: 25/06/2025

[36] IBM. Quantum-safe TLS. Disponível em: <https://www.ibm.com/docs/en/quantum-safe/quantum-safe-remediator/1.1.0?topic=cryptography-quantum-safe-tls>. Acesso em: 25/06/2025

[37] REINO UNIDO. UK National Quantum Technologies Programme. Disponível em: <https://uknqt.ukri.org/>. Acesso em: 25/06/2025

[38] ROHDE&SCHWARZ. Próxima parada: a próxima geração. Disponível em: <https://www.rohde-schwarz.com/br/sobre/magazine/quantum-technology/tecnologia-quantica_255950.html>. Acesso em: 25/06/2025

[39] AUSTRÁLIA. Army Quantum Technology Roadmap. Disponível em: <https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf>. Acesso em: 25/06/2025

[40] FAPESP. Startup quântica desenvolve gerador de números aleatórios usado em loteria. Pesquisa FAPESP, n. 339, mai. 24. Disponível em: <https://revistapesquisa.fapesp.br/startup-quantica-desenvolve-gerador-de-numeros-aleatorios-usado-em-loteria>. Acesso em: 25/06/2025

[41] UNIVERSIDAD DE CONCEPCIÓN. SeQure Quantum planea llevar su generador cuántico de números aleatorios a la nube. Noticias UdeC. Disponível em: <https://noticias.udec.cl/sequre-quantum-planea-llevar-su-generador-cuantico-de-numeros-aleatorios-a-la-nube>. Acesso em: 25/06/2025

[42] INSPIREHEP. Photon Number Splitting Attack – Proposal and Analysis of an Experimental Scheme. Disponível em: <https://inspirehep.net/literature/2807215>. Acesso em: 25/06/2025

[43] COINTELEGRAPH. Computação quântica: Governo Lula projeta investimento de R$ 5 bilhões após Plano Brasileiro de IA. Disponível em: <https://br.cointelegraph.com/news/after-brazils-ai-plan-lulas-government-wants-r5-billion-invested-in-quantum-computing>. Acesso em: 28/06/2025.

[44] BRASIL. Ministério da Defesa. Exército Brasileiro. Concepção de Transformação do Exército Brasileiro e do Desenho da Força 40 2024-2039, 1ª Edição, p. 3-2, 2024. Disponível em: <https://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=181261856&act=sep>. Acesso em: 01/09/2025