

TECNOLOGIAS QUÂNTICAS EM PROGRAMAS ESTRATÉGICOS DO EXÉRCITO BRASILEIRO: DESAFIOS E OPORTUNIDADES

QUANTUM TECHNOLOGIES IN STRATEGIC PROGRAMS OF THE BRAZILIAN ARMY: CHALLENGES AND OPPORTUNITIES

FERNANDA DAS GRAÇAS CORRÊA

RESUMO

Este artigo conclusivo da linha de pesquisa Tecnologia, Inovação e Emprego Militar mapeia, identifica e analisa os principais desafios de nichos tecnológicos de interesse da Força Terrestre, assim como as oportunidades em tecnologias quânticas que possam ser aplicadas em programas estratégicos do Exército Brasileiro, como o Sistema Integrado de Monitoramento de Fronteira e o de Defesa Cibernética. São prospectadas diversas tecnologias, como satélites, radares, sensores, criptografia e computação quântica, que poderão subsidiar o processo de transformação da Força Terrestre. Além de projetos de Pesquisa, Desenvolvimento & Inovação de Instituições Científicas, Tecnológicas e de Inovação subordinadas ao Exército Brasileiro em tecnologias quânticas, são destacados casos de ecossistemas em tecnologias quânticas de países emergentes que possuem variáveis semelhantes às do Brasil e que, se superadas, poderão contribuir com o aumento dos índices nacionais nos principais rankings de inovação internacionais, posicionando, a curto e médio prazos, o país na vanguarda de tecnologias quânticas.

PALAVRAS-CHAVE: Tecnologias Quânticas; Programas Estratégicos; Nichos Tecnológicos; Exército Brasileiro.

ABSTRACT

This conclusive article from the Technology, Innovation & Military Employment research line maps, identifies and analyzes the main challenges of technological niches of interest to the Land Force and opportunities in quantum technologies that can be applied in strategic programs of the Brazilian Army, such as the Integrated Border Monitoring System and Cyber Defense. Several technologies are prospectated, such as satellites, radars, sensors, cryptography and quantum computing, which could reformulate the process of transforming the Land Force. In addition to Research, Development & Innovation projects of Scientific, Technological and Innovation Institutions subordinated to the Brazilian Army in quantum technologies, cases of ecosystems in quantum technologies from emerging countries that have variables similar to the variables of Brazil and which, if overcome, could contribute to increasing Brazil's indices in the main international innovation rankings, positioning Brazil in the short and medium term at the forefront of quantum technologies.

KEYWORDS: Quantum Technologies; Strategic Programs; Technological Niches; Brazilian Army.

A AUTORA

Coordenadora de Prospecção Tecnológica e Gestão do Conhecimento no Departamento de Ciência, Tecnologia e Inovação (DECTI) da Secretaria de Produtos de Defesa (SEPROD) / Ministério da Defesa. Pós-doutoranda em Modelagem de Sistemas Complexos (EACH/USP). Pós-Doutora em Ciências Militares (ECEME). Doutora em Ciência Política na Área de Concentração Estudos Estratégicos (UFF). Pesquisadora na linha Tecnologia, Inovação e Emprego Militar (2022-2023) do Centro de Estudos Estratégicos do Exército (CEEEx).



Sumário Executivo

Este artigo conclusivo da linha de pesquisa Tecnologia, Inovação e Emprego Militar reúne alguns dos principais pontos debatidos nos ensaios científicos publicados ao longo deste ciclo do Núcleo de Estudos Prospectivos (NEP) do Centro de Estudos Estratégicos do Exército (CEEEEx), e aponta os principais desafios e oportunidades em tecnologias quânticas para a Força Terrestre.

O primeiro ensaio mapeou, identificou e analisou os principais nichos tecnológicos, entre eles, universidades, centros de pesquisa e laboratórios de pesquisa.

O segundo, discutiu os desafios relacionados aos Recursos Humanos para o desenvolvimento de projetos de Pesquisa, Desenvolvimento e Inovação (PD&I) na área de computação quântica.

O terceiro ensaio discute os dilemas atuais da computação quântica tendo como pano de fundo o contexto da Guerra na Ucrânia, especialmente os ataques cibernéticos a infraestruturas críticas e instituições financeiras.

Um dos principais dilemas no contexto dessa guerra é: como computadores clássicos podem resistir a ataques cibernéticos a partir de computadores quânticos? Daí a necessidade de o artigo conclusivo desta linha de pesquisa abordar os desafios e oportunidades do emprego de tecnologias quânticas em programas estratégicos do Exército Brasileiro (EB).

Este artigo é dividido em três partes: na primeira parte, são apresentadas diversas áreas tecnológicas quânticas e que podem ser de interesse do EB, tais como: computação, criptografia, comunicações, sensores, radares e metrologia.

A segunda parte aborda os desafios que países emergentes enfrentam na criação de seus ecossistemas quânticos com ênfase nos casos da Espanha, da Austrália e da China, destacando as áreas tecnológicas prioritárias do ecossistema quântico e seus programas educacionais de formação de recursos humanos.

A terceira parte trata das Organizações Militares (OM) reconhecidas pelo EB como Instituições Científicas, Tecnológicas e de Inovação (ICT), que reúnem capacidades para atuar em um ecossistema brasileiro de tecnologias quânticas e de suas aplicações militares em dois programas estratégicos do EB: o Sistema Integrado de Monitoramento de Fronteira (SISFRON) e o Defesa Cibernética. São ainda destacados projetos envolvendo ICT subordinadas ao EB, como o projeto de sensores quânticos do Instituto Militar de Engenharia (IME), a participação do IME em projeto experimental civil de Distribuição de Chave Quântica (QKD, sigla em inglês) na cidade do Rio de Janeiro, e o projeto de criação de ecossistema nacional de tecnologias quânticas do Centro de Desenvolvimento de Sistemas (CDS).

No SISFRON, é possível o EB integrar criptografia, radares, sensores e comunicações quânticas em sistemas e plataformas aeroespaciais e terrestres. QKD podem substituir diversos dispositivos de criptografia convencional utilizados em satélites e em redes definidas por *softwares* empregadas no SISFRON. Radares e sensores utilizados pelo EB no âmbito do SISFRON também podem usar tecnologias quânticas.

O programa Defesa Cibernética pode se beneficiar de *hardwares*, *softwares*, sistemas de segurança da informação, programas de detecção de intrusão, simuladores de Defesa e Guerra Cibernética, antivírus, *chips* e supercomputadores. Diversos destes bens e serviços podem empregar também tecnologias quânticas, como dispositivos de QKD e de criptografia pós-quântica, oriundos do desenvolvimento conjunto com nichos tecnológicos nacionais e/ou de aquisições no mercado nacional e internacional de tecnologias ciberquânticas.

1. Tecnologias Quânticas e seu emprego militar

A ciência quântica estuda o desenvolvimento de algoritmos e *softwares* baseados em informações processadas por sistemas quânticos, como moléculas, átomos, partículas subatômicas, elétrons, prótons e fótons.

A computação quântica, por sua vez, faz uso de propriedades da mecânica quântica, como sobreposição e interferência, e se enquadra no contexto da teoria da complexidade com significativos transbordamentos para diversas áreas, como criptografia, inteligência artificial, metrologia, comunicações, sensoriamento, biomedicina e novos medicamentos, modelagem financeira, entre outras. A Computação Quântica estuda o desenvolvimento de algoritmos e *softwares* com base em informações que são processadas por sistemas quânticos, dentre eles, átomos, fótons e partículas subatômicas, para resolver problemas lógicos e complexos.

A teoria da computação quântica teve início na década de 1980, com os estudos de Richard Feynman sobre os efeitos da mecânica quântica em sistemas quânticos de partículas. Somente no início da década de 1990, esta teoria ganhou maior repercussão na comunidade científica, quando o algoritmo quântico *Shor* demonstrou capacidade de superar o modelo computacional clássico de *Turing*. Este novo algoritmo impulsionou tanto a busca por novos algoritmos criptográficos alternativos e algoritmos quânticos quanto a pesquisa aplicada, sobretudo, o desenvolvimento de computadores quânticos¹.

No final da década 1990, os primeiros computadores quânticos baseados em montagem térmica foram construídos no Instituto de

¹ Enquanto computadores clássicos operam com memória em *bits* (cada *bit* armazena “1” ou “0” de informação), os computadores quânticos operam com um conjunto de *qubits* (cada *qubit* armazena “1” ou “0” ou uma sobreposição de “1” ou “0” de informação). Em resumo, computadores quânticos manipulam estes *qubits*.

Tecnologia de Massachusetts (MIT, sigla em inglês). Em 2017, a empresa canadense *D-Wave* desenvolveu um computador híbrido denominado *Orion* com um processador quântico de 16 *qubits* que também processa bits convencionais e, em 2017, esta mesma empresa lançou o *2000Q*, modelo de computador quântico comercial com 2.000 *qubits*.

Em 2019, a comunidade científica foi surpreendida com o *Sycamore*, *chip* quântico da Administração Nacional da Aeronáutica e Espaço (NASA, em inglês) com 54 *qubits*, capaz de solucionar problemas complexos em minutos, e prever possíveis mudanças na configuração de uma molécula de diazeno (H₂N₂) utilizando apenas 12 dos 54 *qubits* presentes no processador. Um computador clássico utilizando um super processador só é capaz de realizar este feito em cerca de 10 mil anos.

Dentre as empresas que estão na fronteira do desenvolvimento deste tipo de supercomputador, destacam-se: IBM, Google e Microsoft. Embora hajam diversas iniciativas empreendedoras, como as citadas acima, a área de computação quântica ainda carece de muitos estudos para se consolidar.

Diversas destas tecnologias quânticas são aplicáveis na Defesa, em especial, nas áreas de computação, criptografia, sensores, radares e comunicações. No que diz respeito às diversas aplicações militares de Computadores Quânticos, encontra-se, por exemplo, a fatoração de números inteiros, permitindo a descryptografia de protocolos cibernéticos mais convencionalmente utilizados. Ataques cibernéticos a partir de computadores quânticos constituem uma ameaça cada vez mais real diante da importância que a comunicação e a informação seguras têm para a Defesa. Diante dessa ameaça, faz-se necessário atualizar toda a infraestrutura digital segura usando criptografia que seja “resistente a *quantum*”, ou seja, segura contra computadores quânticos e clássicos (AMERONGEN, 2021, p. 8).

Comunicação segura é um tema crítico na

área de Defesa. Historicamente, a criptografia² tem sido a principal técnica utilizada para atender a essa demanda, oferecendo segurança e privacidade. No entanto, a criptografia convencional tem sido objeto de ataque das mais recentes tecnologias de comunicações seguras lançadas na atualidade, envolvendo supercomputadores. Nesse contexto, crescem de importância os sistemas e dispositivos criptográficos com chave quântica (QKD³, sigla em inglês) utilizados em diversas tecnologias militares para aumentar a segurança dos dados distribuídos que trafegam em redes militares, como Redes Definidas por *Software* (RDS).

Em suma, é possível empregar QKD em satélites e em rádios militares que trafegam dados e informações estratégicas e que utilizam bandas de transmissão militares via *Internet*⁴.

2. Desafios relacionados ao desenvolvimento de tecnologias quânticas: os casos da Espanha, da Austrália e da China

Além de mão de obra permanentemente qualificada, o domínio de tecnologias

² Criptografia é, historicamente, uma ferramenta empregada para codificar mensagens a fim de criar um canal de comunicação seguro e confidencial de forma que outros não possam decodificar dados e informações enviadas.

³ A QKD tem o objetivo de gerar e transmitir com segurança uma chave secreta, normalmente para o uso de apenas duas pessoas. Parte da comunicação durante o processo de criação da chave é feita em um canal quântico, e parte em um clássico, sendo que as mensagens quânticas tomam vantagem do fato de ser impossível de medir integralmente ou copiar (clonar) uma função de onda. Dessa forma, enquanto a criptografia clássica preconiza que sempre é possível interceptar uma mensagem sem ser percebido, a criptografia quântica permite protocolos em que isto é impossível (PFEIFFER, PAIM & MOTTA, 2017, p. 3).

⁴ A Internet Quântica traz como princípio uma gama de possibilidades que não se verificavam na comunicação clássica, remodelando-a, de tal forma que, com a Internet Quântica, é possível complementar a Internet atual ou definitivamente utilizar somente meios quânticos. Apoiados nessa nova comunicação, pesquisadores abrem um universo de vantagens que tem como objetivo suprir as carências que a Internet convencional possui, como a segurança das informações trafegadas. Uma das principais aplicações conhecidas da Internet Quântica é a distribuição de chave quântica (QKD), onde duas partes produzem uma chave única e aleatória, que não seja conhecida por um terceiro (SOUSA et al., 2021, p. 2).

quânticas envolve diversas outras demandas que, se não superadas pelas economias nacionais, comprometem o sucesso de projetos e programas estratégicos de CT&I, tais como: aquisição/desenvolvimento de novos materiais, infraestrutura científica, tecnológica e industrial ampliada e fluxo contínuo de recursos financeiros.

EUA e Reino Unido são os países que, atualmente, estão na vanguarda das tecnologias quânticas e boa parte das suas organizações de base tecnológica tem superado com eficiência as variáveis que poderiam comprometer o desenvolvimento de seus ecossistemas produtivos quânticos. A União Europeia (EU) está no mesmo patamar alcançado por EUA e Reino Unido. Países, como Austrália, Áustria, China, Espanha e Israel, estão desenvolvendo seus ecossistemas produtivos quânticos tendo que criar toda a infraestrutura científica, tecnológica e industrial; formar, recrutar, qualificar, capacitar e conter a evasão de mão de obra; criar estratégias de acesso a novos materiais e otimizar mecanismos de fomento; além de explorar novas modalidades de aquisição/desenvolvimento de tecnologias quânticas.

2.1. O caso espanhol

O caso do ecossistema quântico espanhol em Defesa foi melhor detalhado no ensaio científico 2 desta linha de pesquisa, intitulado “Gestão de pessoas no planejamento estratégico do Exército Brasileiro na área de Computação Quântica”, no qual o Ministério da Defesa espanhol se aproveita do tecido tecnológico industrial civil para avançar em seus programas estratégicos e projetos tecnológicos na área quântica. Especificamente neste ensaio, foi citado projeto liderado pela empresa espanhola Satelliot de nanosatélites 5G IoT que utilizam dispositivos QKD para comunicações seguras.

A Espanha participa do OPEN QKD, consórcio europeu com sede em Viena, na Áustria, cuja ambição é reforçar a posição global

da Europa na vanguarda das capacidades de comunicação quântica e demonstrar a integração transparente de soluções de segurança quântica amplamente em todo o cenário digital europeu (CORRÊA, 2022b). O OPEN QKD atua como facilitador e multiplicador para soluções de criptografia baseadas em quântica, promovendo a cooperação da academia, da indústria e de *startups* europeias na implantação de testes abertos locais em toda a Europa, de forma acessível para partes interessadas realizarem testes de campo, aumentando significativamente a conscientização e o envolvimento com QKD. Dentre os objetivos do consórcio, encontram-se: estabelecer a primeira plataforma de experimentação habilitada para OPEN QKD; interfaces padronizadas; operação de casos de uso derivados das necessidades das Sociedades Seguras Gama de casos de uso; instalar teste aberto, robusto, confiável, modular e totalmente monitorado; contribuir para a padronização da criptografia quântica e esforços de certificação de segurança; lançar as bases para uma rede quântica pan-europeia; e promover maior competitividade em QKD na indústria europeia.

Uma das inovações no âmbito do OPEN QKD é o simulador de rede QKD (QKDNetSim), que consiste em um módulo de simulação projetado para expandir o simulador de rede NS-3 com funcionalidades de rede QKD. O principal objetivo do simulador de rede é a análise de diferentes abordagens para organizações de rede QKD, simulação de tecnologias de rede considerando a integração de sistemas QKD em redes de telecomunicações existentes. Este projeto recebeu financiamento do programa de pesquisa e inovação *Horizon 2020* da União Europeia.

2.2. O caso australiano

O Centro de Pesquisa do Exército da Austrália desenvolve estudos a fim de fornecer à sua Força Terrestre uma vantagem quântica em operações terrestres. De acordo com

o *Roadmap tecnológico quântico do Exército* (AUSTRÁLIA, 2021), três postos-chave enquadram a abordagem do Exército australiano à tecnologia quântica: 1) a Austrália enfrenta o desafio estratégico de converter sua liderança global em pesquisa de tecnologia quântica em vantagem industrial e de Defesa sustentável; 2) a Defesa tem o papel de alinhar a capacidade existente de pesquisa e desenvolvimento (P&D) aos problemas prioritários da Defesa⁵; e 3) esse processo deve estar alinhado aos temas estratégicos de pensamento adaptativo, parceria, indústria soberana e integração.

A fim de desenvolver a capacidade tecnológica quântica, o Exército australiano perseguirá quatro objetivos: 1) estabelecer rapidamente um ecossistema de inovação quântica focado em oportunidades de domínio da terra; 2) identificar aplicações mais disruptivas e vantajosas das tecnologias quânticas para o domínio terrestre; 3) desenvolver a tecnologia relacionada, conceitos operacionais e projetos de força modificados; e 4) apoiar o desenvolvimento da estratégia de tecnologia quântica da Defesa (AUSTRÁLIA, 2021, p. 2). Para tanto, pretende desenvolver as tecnologias quânticas por meio da habilitação de diversas tecnologias clássicas, nichos tecnológicos e mão de obra qualificada, considerando a existência de possíveis contramedidas para tecnologias quânticas que variam desde ruptura quântica até protocolos de criptografia pós-quântica.

Vislumbra-se, na **tabela 1**, o cronograma de como o Exército australiano pretende alcançar o cenário ideal do panorama de tecnologias quânticas. Dentro de cinco anos, pretende, na área de sensoriamento e imagem, desenvolver magnetômetros quânticos e, na área de comunicações e criptografia, pretende desenvolver redes simples de QKD de curto alcance.

⁵ Isso inclui moldar e orientar essas tecnologias à medida que elas se desenvolvem para facilitar a transição de conceitos de tecnologia em capacidade para o combatente.

Tabela 1 - Estado atual e cronogramas de desenvolvimento de projetos de diferentes tecnologias quânticas do Centro de Pesquisa do Exército da Austrália

Estado de desenvolvimento atual	Em produção/estágios avançados de P&D da indústria	P&D da indústria intermediária/estágios avançados de pesquisa acadêmica	Estágios iniciais de P&D da indústria/estágios intermediários de pesquisa acadêmica
Tempo estimado para aplicação em Defesa	< 5 anos	5-10 anos	> 10 anos
Sensoriamento e imagem	Magnetômetros, giroscópios e relógios de acelerômetros quânticos e microscópios quânticos	Espectrômetros e detectores quânticos, analisadores bio/ químicos em escala de chip e imagem por Ressonância Magnética quântica aprimorada	Magnetoencefalografia (MEG) vestível, nanossensores quânticos para biomedicina
Comunicações e criptografia	Redes simples de distribuição de chaves quânticas de curto alcance	Repetidores quânticos, portas quânticas de longo alcance complexo, redes de distribuição de chaves quânticas, sincronização de relógios	Memórias quânticas, redes de sensores quânticos e computadores
Computação e simulação	Computadores mainframe NISQ ⁶	Computadores NISQ distribuídos e de borda integrados em redes clássicas e computadores mainframe com correção de erros	Computadores mainframe de grande escala com correção de erros com capacidade de criptografia e computadores com correção de erros distribuídos em redes quânticas

Fonte: (AUSTRÁLIA 2021, p.3)⁷

2.3. O caso chinês

A China conseguiu estruturar seu ecossistema quântico por meio de uma articulada e integrada relação Governo-Indústria-Academia. A estratégia do governo chinês para criar seu ecossistema quântico teve início com a formação de mão de obra qualificada e sua integração às redes internacionais isoladas de tecnologias quânticas de centros de pesquisa e universidades estadunidenses e europeias. A espinha dorsal do ecossistema quântico chinês é a Universidade de Ciência e Tecnologia da China (USTC, sigla em inglês), subordinada à Academia Chinesa de Ciências (CAS), cujas atividades estão listadas na **tabela 2**.

O mentor do ecossistema quântico chinês é Pan Jianwei, chefe do Departamento de Física Quântica e Pesquisa da Informação da USTC.

O Departamento é constituído por 55 pesquisadores seniores, dos quais mais da metade realizaram doutorado ou pós-doutorado no exterior⁸, em especial, na Alemanha e na Áustria. Este Departamento também abriga 171 alunos de doutorado e 24 alunos de pós-doutorado, cuja maior concentração está na linha de pesquisa de computação quântica supercondutora (JULIENNE,2022, p. 16).

⁸ De acordo com o relatório da Strider, as principais fontes de financiamento europeu desses pesquisadores são: Conselho Europeu de Pesquisa, União Europeia, Sétimo Programa-Quadro, Deutsche Forschungsgemeinschaft, Ações Marie Curie, Landstiftung e Alexander Von Humbolt – Fundação Stiftung e Konrad-Adenauer Stiftung; tendo esses pesquisadores mantido relações de pesquisa colaborativa com os seguintes centros de pesquisa e universidades estrangeiras: Heidelberg University, Louisiana State University, University of Calgary, Trento University, Max Planck Institute of Optics, Cambridge University e University of New South Wales.

⁶ Quantum de escala intermediária ruidosa (NISQ, sigla em inglês).

⁷ Tradução livre da autora.

Tabela 2 - Áreas tecnológicas e linhas de pesquisa da USTC

Áreas tecnológicas	Linhas de pesquisa
Fundamentos da física quântica e comunicação quântica	Comunicação quântica urbana e interurbana, comunicação quântica por satélite, instrumentação.
Computação quântica e simulação	Computação quântica óptica (ou fotônica), computação quântica supercondutora, simulação quântica de <i>bósons ultrafrios</i> .
Medição de precisão quântica	Interferência atômica, interferência <i>multifóton</i> , imagem quântica.
Física quântica teórica	Teoria quântica da informação e comunicação, teoria da simulação quântica, teoria quântica.

Fonte: elaborada pela autora

Ao longo da década de 2010, a China enviou diversos pesquisadores chineses para laboratórios, centros de pesquisa e universidades no exterior com a garantia individual de que esses pesquisadores voltassem para a China e aplicassem os conhecimentos absorvidos no desenvolvimento de projetos de PD&I, na potencialização de nichos tecnológicos e empresas locais e na criação do ecossistema quântico chinês. Em 2011, a China inaugurou o Centro de Inovação para Informação Quântica e Fronteiras Quânticas envolvendo inicialmente a USTC, a Universidade de Nanjing, o Instituto de Física Técnica de Xangai/ CAS, o Instituto de Semicondutores/CAS e a Universidade Nacional de Tecnologia de Defesa (NUDT). Embora a NUDT reúna o grupo Quanta, o Centro Interdisciplinar de Informação Quântica e estruturas próprias do Exército de pesquisa em física quântica, as autoridades governamentais favorecem a maior centralização de recursos à USTC. Acredita-se que isso se deve ao baixo nível de maturidade tecnológica, às necessidades de financiamento e à escassez de talentos na NUDT quando comparada à USTC (JULIENNE, 2022, p. 18). Em 2017, foi fundada a Academia de Ciências da Informação Quântica de Pequim (BAQIS), a qual reúne a CAS, a Universidade de Tsinghua, a Universidade de Pequim e empresas.

Em função dos esforços de Xi Jinping

em promover, desde 2015, a fusão civil-militar, houve uma relação de maior proximidade entre a USTC e NUDT. No âmbito dessa relação, o Exército chinês tem se mostrado particularmente interessado nos campos de comunicação quântica segura, criptografia, radares e imagens quânticas, bem como giroscópios quânticos que ofereceriam a aeronaves, navios, submarinos e tanques um sistema de posicionamento preciso, com economia de espaço e independente de satélite (JULIENNE, 2022, p. 18).

Em 2016, a China lançou ao espaço o satélite *Micius*, o primeiro a fazer uso de criptografia quântica em seus protocolos de comunicação. A partir do lançamento deste satélite, diversas outras inovações surgiram, em especial, a *Internet* quântica. O *Micius* tornou possível que duas estações terrestres ligadas a ele, que se encontram a uma distância de 1,2 mil quilômetros uma da outra, fossem capazes de se conectar por meio de um *link* direto gerado pelo sistema, cuja segurança não dependia do satélite.

Em 2017, empresas do conglomerado naval chinês *China Shipbuilding Industry Corporation* (CSIC) estabeleceram instrumento jurídico com a USTC para instalar três laboratórios de pesquisa nas áreas de navegação, comunicação e sensoriamento quântico em Wuhan. O USTC também assinou um acordo de cooperação estratégica com o grupo de

eletrônica de Defesa *China Electronics Technology Group Corporation (CETC)*, incluindo colaboração em detecção quântica e comunicação (JULIENNE, 2022, p. 18). *Experts* em tecnologias disruptivas têm produzido conhecimento e publicado sobre navegação quântica, o que remonta ao desenvolvimento de dispositivos de sensoriamento quântico para navegação e posicionamento, comunicação e detecção submarina. Magnetômetros quânticos são capazes de assegurar posicionamento de com altos níveis de precisão baseados em espaço sem necessidade de sistema de posicionamento global (GPS, sigla em inglês) e otimizar a capacidade de ataque de precisão de mísseis. Em função da sua capacidade de medir anomalias no campo magnético da Terra, magnetômetros são utilizados para detectar submarinos desde a 2ª Guerra Mundial. Diversas tecnologias, como eletroímãs e cascos não metálicos, desde então, têm sido utilizadas para reduzir a assinatura magnética de submarinos. A China e a Austrália vêm desenvolvendo diversos tipos de tecnologias quânticas para serem incorporadas em magnetômetros, como *Superconducting Quantum Interference Device* (SQUID) e Amplificador de Expansão Mecânica (MEA, sigla em inglês), com a finalidade principal de detectar a anomalia magnética causadas por submarinos e navios de superfície a longas distâncias. Um magnetômetro quântico MEA instalado em um satélite, por exemplo, pode determinar o curso da guerra antissubmarina nos mares da região Ásia-Pacífico.

2.4. A coordenação de pesquisa

Na Espanha, sob coordenação da Doutora Alba Cervera Lierta, o Centro de Supercomputação de Barcelona - Centro Nacional de Supercomputação (BSC-CNS) é o responsável pela gestão da participação de todas as entidades do ecossistema quântico espanhol.

Na China, a instituição responsável pela criação do ecossistema quântico é a Universidade de Ciência e Tecnologia da China, sob mentoria de Pan Jianwei, chefe do Departamento de Física Quântica e Pesquisa da Informação desta Universidade.

Na Austrália, a Doutora Cathy Foley lidera o desenvolvimento da primeira estratégia quântica da Austrália e, desde novembro de 2021, preside o Comitê Nacional de Quânticos, com membros representantes da indústria e da academia.

No caso brasileiro, deve-se registrar que o SENAI-CIMATEC, junto à rede SOFTEX, foi selecionado pelo Ministério da Ciência, Tecnologia e Inovação (MCTI) para formar mão de obra qualificada na área quântica e o EB, por meio da Escola Nacional de Defesa Cibernética (ENADCIBER), já está capacitando pesquisadores militares das três Forças Armadas brasileiras em áreas estratégicas, como supercomputação, *big data*, simulação quântica, entre outras. No entanto, o desafio do MCTI é definir qual ICT (civil, militar, pública ou privada) será responsável por abrigar um futuro computador quântico nacional e como será conduzida a liderança.

3. Desafios e oportunidades para programas estratégicos do Exército Brasileiro em Tecnologias Quânticas

O EB possui 41 Instituições Científicas, Tecnológicas e de Inovação do Ministério da Defesa (ICTMD)⁹ que atuam nas mais diversas áreas tecnológicas, com potencial de cooperar tecnologicamente para

⁹ Recentemente, todas as Instituições Científicas, Tecnológicas e de Inovação das três Forças Armadas e do próprio MD foram convencionalmente denominadas Instituições Científicas, Tecnológicas e de Inovação do Ministério da Defesa (ICTMD), conforme Portaria GM-MD Nº 3.439, de 18 de agosto de 2021, que aprova a Política de Propriedade Intelectual do Ministério da Defesa (PPIMD).

gerar inovações disruptivas em Defesa e de se beneficiar de parcerias, bens e serviços com nichos tecnológicos (CORRÊA, 2022, p. 63-64).

Algumas dessas ICTMD atuam em programas do Portfólio Estratégico do EB, e podem se beneficiar de bens e serviços inovadores em Tecnologias Quânticas, tais como o CDCIBER, a DSG, o CITEEx e o CCOMGEX¹⁰.

IME e CTEEx são ICTMD que podem participar de forma atuante no desenvolvimento dessas tecnologias.

Destacaremos na **tabela 3** dois programas estratégicos que se beneficiariam de tecnologias quânticas: Sistema Integrado de Monitoramento de Fronteira (SISFRON) e Defesa Cibernética.

Tabela 3 – Programas estratégicos e ICTMD que atuam na área quântica

Programa Estratégico	Objetivos	ICTMD
SISFRON	Fortalecer a presença e a capacidade de monitoramento e de ação do Estado na faixa de fronteira terrestre, potencializando a atuação dos entes governamentais com responsabilidades sobre a área.	CCOMGEX e DSG
Defesa Cibernética	Capacitação de recursos humanos, possibilitando o domínio de temas multidisciplinares com especial enfoque no desenvolvimento de doutrina de proteção de ativos próprios, desenvolvimento de capacidade de atuação em rede, implementação de pesquisa científica voltada ao tema e indução da capacidade tecnológica nacional.	CDCIBER e CITEEX

Fonte: EPEX

Analisaremos, a seguir, a situação de cada um desses programas

3.1 SISFRON

O SISFRON é um sistema operacional de sensoriamento e de apoio à decisão, que atua de forma integrada, monitorando as áreas de fronteira e assegurando o fluxo contínuo e seguro de dados entre diversos escalões da Força Terrestre e, devendo produzir informações confiáveis e oportunas.

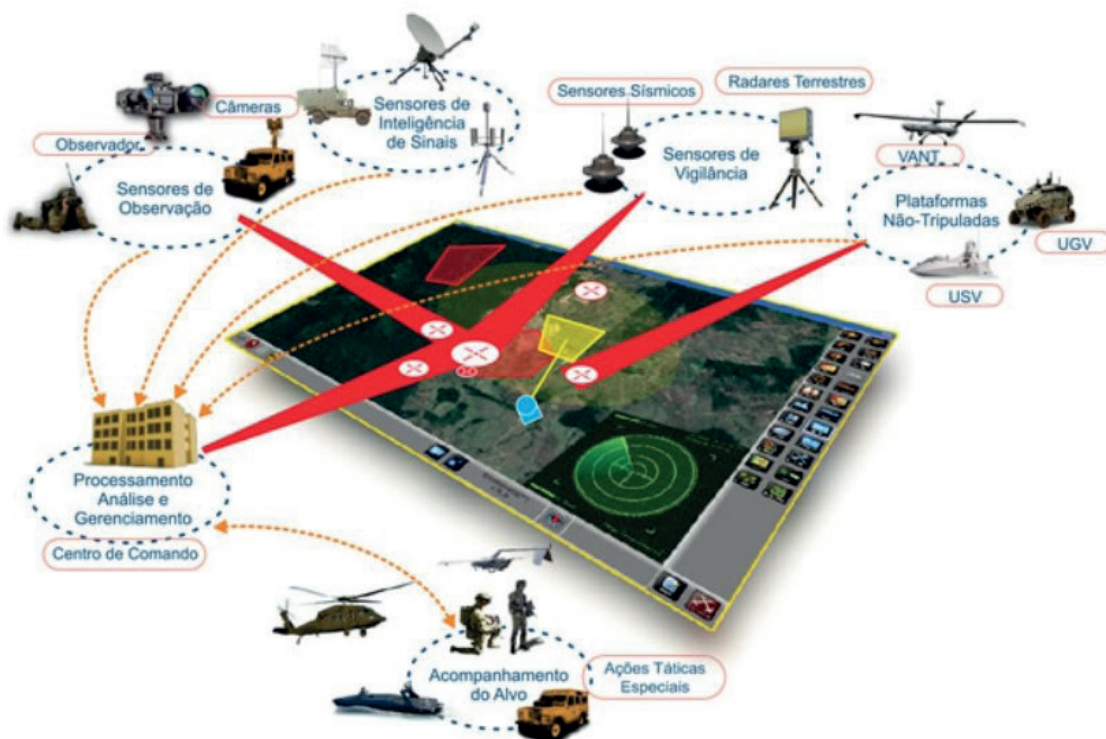
As operações do EB no âmbito do SISFRON, sejam elas isoladas, em conjunto com as outras Forças Armadas ou, ainda, em ambiente interagências, com outros órgãos governamentais, requerem um sistema complexo de comunicação segura que empregue “protocolo de distribuição de chaves que seja realmente

imune ao monitoramento não autorizado” (JABOUR NETO; DUARTE, 2016, p. 2).

Dentre as tecnologias usadas no SISFRON que podem empregar tecnologias quânticas, encontram-se satélites, sensores, radares e redes definidas por *softwares*. O QKD, por exemplo, pode ser aplicado em satélites, em sensores, em radares e em redes definidas por *softwares* empregadas no SISFRON, nos moldes do projeto liderado pela empresa espanhola *Sateliot* que está em andamento para posicionar a Espanha como referência mundial em constelações de nanossatélites de baixa órbita 5G, Internet das Coisas (IoT) e comunicações globais seguras. Essa rede de 96 nanossatélites promete conectar elementos IoT no padrão 5G, compatível com mais de 70 operadoras móveis, e garantir comunicação segura, ao introduzir dispositivo de criptografia por meio de QKD (CORRÊA, 2022, p. 54-55).

¹⁰Aqui nos concentraremos apenas nas ICTMD-mães.

Figura 1 – SISFRON



Fonte: EB

Cabe ao CITEx implantar e manter o Sistema Estratégico de Comando e Controle do EB, integrado ao Sistema de Comando e Controle da Força Terrestre, a fim de permitir fluxo seguro e oportuno de informações aos comandantes em todos os níveis, contribuindo para o incremento do poder de combate do EB e para o desenvolvimento nacional. O CITEx e suas OM subordinadas são responsáveis por manter todas as OM do EB conectadas por meio de sistema de provedores de *Internet* com rede exclusiva da Força.

O conjunto das ações que compõem a defesa cibernética possui objetivos distintos, portanto faz-se necessário pontuar as categorias principais. Essas ações podem ser de três naturezas, designadas doutrinariamente, no âmbito da Defesa Nacional, como: proteção cibernética, exploração cibernética e ataque cibernético. Neste contexto, as ações de proteção cibernética preservam a segurança dos

dados digitais que sejam de interesse da Defesa Nacional, dos respectivos sistemas que os processam e das redes por onde trafegam no espaço cibernético. As ações de exploração cibernética buscam, no ciberespaço, obter informações que provejam consciência situacional e apoio à decisão nos vários níveis de comando e controle das operações cibernéticas. Por fim, as ações de ataque cibernético têm por alvo os sistemas informacionais digitais localizados no espaço cibernético, cujo comprometimento neutralizaria ou degradaria a capacidade ofensiva de um agente ameaçador à soberania nacional (BRASIL 2014 apud VIANNA; CAMELO, 2020, p. 130-131).

O CITEx seria uma das ICTMD que mais se beneficiariam como operadora da *Internet* quântica, à medida que seria capaz de garantir total segurança dos dados digitais e a privacidade no trânsito de todos os bancos de dados da Força Terrestre, incluindo a transmissão de documentos, imagens, vozes, vídeos e conversas privadas em tempos de paz e em tempos de guerra.

3.2 Defesa Cibernética

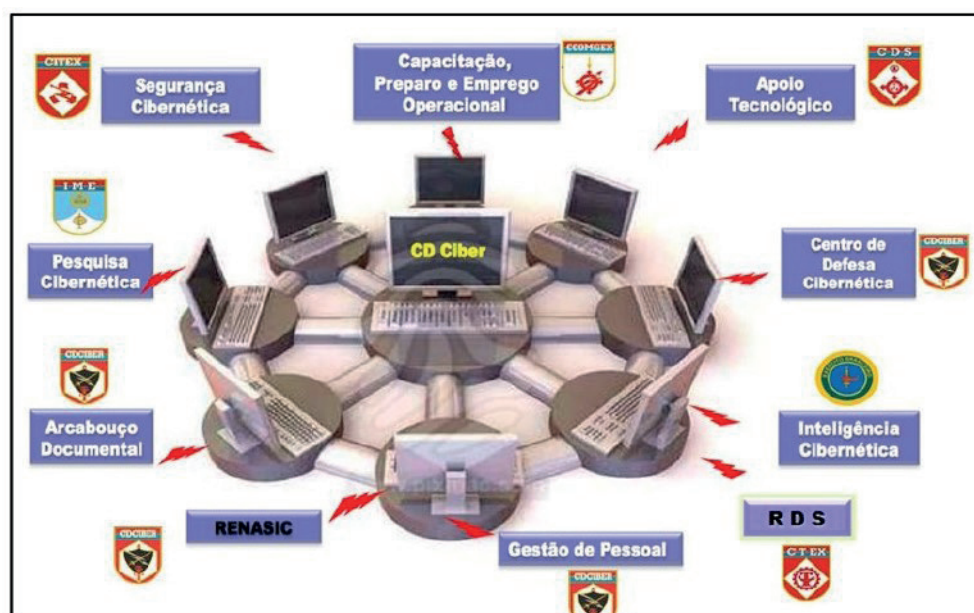
O programa estratégico de Defesa Cibernética do EB impulsionou a criação do CDCiber¹¹, encarregado de exercer a governança, de forma colaborativa, entre os vetores naturalmente vocacionados para compor a Defesa na área cibernética. Dentre os projetos demandados na área de Defesa Cibernética, que envolvem o CDCiber, encontram-se: organização do Centro de Defesa Cibernética, Arcabouço Documental, Gestão Pessoal e a Rede Nacional da Segurança da Informação e Criptografia (RENASIC). Dentre os produtos demandados ao EB, que incluem o CDCiber nessa área, encontram-se: o Antivírus Defesa.Br, o Simulador de Operações Cibernéticas e a Segurança Cibernética em Grandes Eventos.

A **figura 2** ilustra o programa estratégico Defesa Cibernética, o qual possui atualmente seis

projetos estruturantes com o objetivo de criar a capacidade cibernética no EB.

Os projetos estruturantes são conduzidos, atualmente, pelas seguintes ICTMD: IME, CCOMGEx, CDS, CITEx e CDCiber. Embora não seja ICTMD, o Centro de Inteligência do Exército (CIE) também atua em projetos estruturantes desse programa estratégico.¹² Dentre os bens e serviços inovadores que podem surgir de parcerias entre ICTMD e nichos tecnológicos no âmbito do programa estratégico Defesa Cibernética, encontram-se sistemas de segurança da informação, programas de detecção de intrusão, *hardware* para a composição de laboratórios e simuladores de Defesa e Guerra Cibernética, antivírus, *chips*, supercomputadores e computadores quânticos. Criptografia quântica, por exemplo, aumentaria a segurança e privacidade de dados trafegados em computadores utilizados pelo EB.

Figura 2 – Programa Estratégico Defesa Cibernética



Fonte: CDCIBER

¹¹ Além do CDCiber, integram o Sistema Militar de Defesa Cibernética outras ICTMD, como o CITEx, CDS, IME, CCOMGEx e CTEEx. O CDCiber foi concebido para atuar em cinco áreas de competência: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos.

¹² Para conhecer mais o programa estratégico de Defesa Cibernética, acesse: < <http://www.epex.eb.mil.br/index.php/defesa-cibernetica>>.

Observa-se no cenário atual da Guerra na Ucrânia, por exemplo, que diversas agências governamentais e bancos ucranianos se tornaram alvos de ataques cibernéticos, como conexão ao servidor C&C, ataque de força bruta, ataque a aplicativos *web*, *malwares*, ataques distribuídos de negação de serviço (DDoS, sigla em inglês) etc. (CORRÊA 2023, p. 51-52). Nesse contexto, um dos temas que mais tem despontado mundialmente nos principais debates na área de Defesa é: como um computador clássico pode resistir a um ataque cibernético a partir de um computador quântico? Daí o destaque ainda maior que bens e serviços em criptografia pós-quântica (PQC, sigla em inglês) tem obtido no mercado de Segurança e de Defesa Ciberquântica. PQC se refere a novos algoritmos criptográficos clássicos que nem mesmo os computadores quânticos serão capazes de resolver.

Caberá ao IME, CDS e ao CTE_x apoiar nichos tecnológicos no desenvolvimento de projetos de PD&I, na área quântica e pós-quântica, no âmbito do programa estratégico Defesa Cibernética, e ao CITE_x e ao CDCiber fornecer a infraestrutura de teste e validação e o acesso a operadores militares usuários finais. Embora não seja uma ICTMD, o Comando de Defesa Cibernética (ComDCiber) enquanto Comando Operacional Conjunto que integra a estrutura regimental do EB, além de contribuir com o

IME, o CDS, o CTE_x e nichos tecnológicos no desenvolvimento de novos projetos de PD&I em Defesa Cibernética, pode organizar diversos tipos de eventos, como simulações, *hackathons* e exercícios operacionais. Caberia ao Sistema Defesa, Indústria e Academia de Inovação (SisDIA), sistema de inovação baseado na Tríplice Hélice do EB, e ao MD mapearem, identificarem, atraírem e potencializarem nichos tecnológicos quânticos no âmbito do programa Defesa Cibernética. O CIE poderá contribuir na retenção do pessoal que atua em projetos de PD&I no programa estratégico, evitando assim a evasão de mão de obra brasileira altamente qualificada para outros países.

3.3 Outras iniciativas em pesquisa quântica

De acordo com o PEE_x 2020-2023, o EB pretende dominar a computação quântica para acelerar a computação de alto desempenho (HPC, sigla em inglês). Para tanto, ganham relevância os trabalhos desenvolvidos em suas Instituições Científicas, Tecnológicas e de Inovação (ICT) que atuam na área quântica, tais como o Instituto Militar de Engenharia (IME) e o Centro de Desenvolvimento de Sistemas (CDS), além de outras ICT subordinadas ao EB, conforme **tabela 4**.

Tabela 4 – Áreas tecnológicas quânticas e competências das ICT subordinadas ao EB

ICTMD	Áreas tecnológicas quânticas	Competências na área quântica
IME	Comunicação e sensores	Pesquisa e desenvolve
CDS	Computação, criptografia e comunicação	Pesquisa, desenvolve e produz
CTEX	Comunicação, computação, radares, sensores e criptografia	Desenvolve e produz
CDCIBER	Computação e criptografia	Testa, avalia e opera
DSG e seus cinco CGEO	Comunicação, radares e sensores	Testa, avalia e opera
CITE _x e seus doze CT e CTA	Computação e comunicação	Testa, avalia e opera
CCOMGEX, CIGE, EsCom, 1º BGE e Cia C2	Comunicação, radares, sensores e criptografia	Testa, avalia e opera

Fonte: Elaborado pela autora

Ainda é possível identificar na tabela acima as ICT subordinadas ao EB que poderão implementar métodos, processos ou sistemas, realizar a gestão técnica de projetos, realizar ensaios não destrutivos em sistemas e até avaliar protótipos, mas não realizam Pesquisa, Desenvolvimento & Inovação (PD&I) nesta área, tais como Centro de Defesa Cibernética (CDCiber), Diretoria de Serviço Geográfico (DSG) e seus cinco Centros de Geoinformação (CGEO), Centro Integrado de Telemática do Exército (CITEx) e seus doze Centros de Telemática (CT) e Centros de Telemática de Área (CTA), Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx), Centro Instrução e Guerra Eletrônica (CIGE), Escola de Comunicações (EsCom), 1º Batalhão de Guerra Eletrônica (1º BGE) e Companhia de Comando e Controle (Cia C2).

Dentre os projetos tecnológicos nos quais algumas ICTMD subordinadas ao EB estão envolvidas, podemos citar o projeto “Desenvolvimento e inovação de sensores, biossensores, detectores nacionais e produtos estratégicos relacionados a agentes químicos, biológicos, radiológicos e nucleares (QBRN) de uso dual visando ao aumento da capacidade operacional e de defesa do Exército Brasileiro”, o projeto “Rede Rio Quântico” e o projeto “Soberania Quântica”.

O primeiro projeto foi aprovado recentemente pela Financiadora de Estudos e Projetos (FINEP)¹³ e está sendo desenvolvido pelo Instituto Militar de Engenharia (IME), em parceria com o Instituto de Defesa Química, Biológica, Radiológica e Nuclear (IDQBRN) e o Instituto de Biologia do Exército (IBEx). Essas instituições são responsáveis pela pesquisa básica, pesquisa aplicada, formação, aperfeiçoamento e

especialização de recursos humanos no campo científico-tecnológico, assessoramento técnico e prestação de serviços do Sistema de Defesa Química, Biológica, Radiológica e Nuclear do Exército (SisDQBRNEx). O projeto prevê o desenvolvimento de dispositivos de uso dual para Defesa QBRN, como sensores, biossensores e detectores, e dará especial ênfase à aplicação de tecnologias quânticas, buscando atingir os seguintes objetivos principais¹⁴:

- dominar todo o ciclo de obtenção de dispositivos inovadores¹⁵, incluindo disruptivos, e produtos estratégicos relacionados a agentes QBRN que serão empregados pelo EB na Defesa Nacional, em benefício próprio e das demais Forças Armadas;

- manter, modernizar e ampliar a infraestrutura laboratorial do SisDQBRNEx para criar condições de melhorar cada vez mais os serviços prestados; e

- prover melhores condições para promover ensino, pesquisa científica básica e aplicada em proveito do sistema SisDQBRNEx e de diversas organizações nacionais e internacionais que atuam na área de DQBRN.

O projeto *Rede Rio Quântica*, do qual o IME é parceiro, é uma iniciativa dos Grupos de Pesquisa em Ótica e Informação Quântica da Universidade Federal Fluminense (UFF), Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), Universidade Federal do Rio de Janeiro (UFRJ) e Centro Brasileiro de Pesquisas Físicas (CBPF)¹⁶ para “criar um núcleo de competência em Redes Quânticas, por meio da implementação de uma rede de comunicações

¹³ Este projeto envolve recursos da ordem de 68 milhões de reais, sendo aproximadamente 48 milhões de reais para uso do IME e o restante para o IDQBRN, subordinado ao CTEx, e o IBEx, subordinado ao Departamento-Geral do Pessoal (DGP).

¹⁴ Informações cedidas pelo IME.

¹⁵ Esses dispositivos não vão se limitar a substituir os existentes, os quais são todos importados, mas deverão ter características diferentes daqueles que hoje se encontram em uso, no sentido de representar um real avanço em termos das capacidades operacional e de Defesa do EB, incorporando neles novos conceitos, materiais, *softwares* e *hardwares*.

¹⁶ Cabe aqui destacar os planos do CBPF na área de Tecnologias Quânticas, incluindo um laboratório para construção dos dispositivos supercondutores para *chips* quânticos.

Quântica dentro da região metropolitana do Rio de Janeiro, abrindo o caminho para a integração do Brasil à *Internet Quântica*”.

Por fim, o CDS propõe a criação de um ecossistema produtivo de Tecnologias Quânticas por meio do projeto intitulado “Soberania Quântica”, envolvendo a sociedade brasileira, o Congresso Nacional, o MD, o MCTI, as empresas da Base Industrial de Defesa (BID), ICT e empresas brasileiras. A proposta de criação desse ecossistema é que o MCTI e o MD assumam a liderança do projeto e que ICTMD e nichos tecnológicos participem em toda a sua cadeia produtiva, desde a pesquisa básica e aplicada até a comercialização e exportação de produtos quânticos.

4. Conclusão

Conclui-se sobre a importância para as Forças Armadas de investimento em recursos humanos (civis e militares) capacitados em tecnologias quânticas. Nesse sentido, a participação de pesquisadores em redes quânticas internacionais e a submissão de projetos de PD&I de ICTMD semelhante ao modelo chinês parece um bom exemplo.

Nessa direção, sugere-se o estabelecimento relações de pesquisa colaborativa entre ICTMD da Força e instituições que estão na vanguarda na pesquisa e no desenvolvimento de tecnologias quânticas, como a *Heidelberg University*, a *Louisiana State University*, a *University of Calgary*, a *Trento University*, o *Max Planck Institute of Optics*, a *Cambridge University* e a *University of New South Wales*. Merecem atenção, também, as convocatórias realizadas pelo EuroHPC e pelo Horizonte Europa da Comissão Europeia, além das convocatórias públicas internacionais do Conselho Europeu de Pesquisa, do Sétimo Programa-Quadro, da *Deutsche Forschungsgemeinschaft*, das Ações Marie Curie, da *Landstiftung* e *Alexander Von Humboldt Stiftung* e da *Konrad-Adenauer Stiftung*.

Conclui-se neste artigo sobre a pertinência

de se pensar a criação de um programa estratégico de computação quântica no âmbito da Força, o que pode vir a ser indutor da criação de redes empresariais, como consórcios, *clusters* produtivos e/ou SPE. Dentre as vantagens de fomentar a criação de redes empresariais, encontram-se: o apoio entre empresas, manifestado em relações verticais e horizontais; a rivalidade entre concorrentes que promovem as abordagens de PD&I e facilitam a introdução de novas estratégias e técnicas; a fluidez; e a rápida difusão da informação e das inovações por meio de canais de fornecedores ou de compradores que têm contato com vários concorrentes.

Portanto, o MD e o EB podem potencializar nichos tecnológicos, fomentando o surgimento de *startups* em universidades, parques e polos tecnológicos nacionais, a criação de *hubs* de inovação e a atração de programas internacionais de aceleração tecnológica, fundos de *Venture Capital (VC)*, *equity crowdfunding* e *corporate venturing*. Podem também fomentar o surgimento de redes empresariais, como *clusters*, consórcios e SPE. A EU, por exemplo, deu origem ao OPEN QKD, que, de fato, tem contribuído para posicionar a Europa na vanguarda das tecnologias quânticas. A Tabela 8 destaca as mais recentes publicações em Tecnologias Quânticas no âmbito do OPEN QKD. Imperativo que pesquisadores das ICTMD envolvidos com a área quântica conheçam estas publicações, estabeleçam contatos e interajam com autores e/ou suas respectivas instituições.

Semelhante à China, o MCTI e o MD podem enviar pesquisadores para nichos tecnológicos no exterior focados em tecnologias quânticas por meio da criação de programas específicos em CT&I que promovam a absorção de conhecimentos estratégicos em tecnologias quânticas, aumentem os índices de inovação e competitividade de nichos tecnológicos brasileiros em *rankings* internacionais de inovação e posicionem a curto e médio prazo o Brasil na vanguarda de tecnologias quânticas.

Dentre as tecnologias usadas no SISFRON que podem ser substituídas por tecnologias quânticas, encontram-se satélites, sensores, radares e redes definidas por *softwares*. Tanto o SISFRON quanto o projeto de Defesa Cibernética podem ser impactados com a criptografia quântica, em especial, QKD, sensores quânticos, como magnetômetros de alta precisão, e comunicação quântica, como *Internet* quântica. *Chips* e computadores quânticos também terão profundo impacto no projeto de Defesa Cibernética.

Por fim, conclui-se que o EB pode avançar no desenvolvimento de tecnologias quânticas sem desprestigiar o desenvolvimento de tecnologias que sejam capazes de resistir a ataques ciberquânticos, ou seja, ataques cibernéticos realizados a partir de computadores quânticos. Daí o esforço duplo e necessário das ICTMD subordinadas ao EB em avançar no desenvolvimento de tecnologias quânticas e pós-quânticas.

Referências

- [AUSTRALIA] *Army Quantum Technology Roadmap*. Australian Army Research Centre. Australian Army, April 2021. Disponível em <https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf> Acesso em 12 jan. 2023.
- [BRASIL] *Plano Estratégico do Exército 2020-2023*. Exército Brasileiro, 2019. Disponível em <http://www.ceadex.eb.mil.br/images/legislacao/XI/plano_estrategico_do_exercito_2020-2023.pdf> Acesso em 12 jan. 2023.
- AMERONGEN, Michael van. Quantum technologies in defence & security. *NATO Review*, 03 June 2021. Disponível em <<https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>> Acesso em 12 jan. 2023.
- CORRÊA, Fernanda das Graças. Gestão de pessoas no planejamento estratégico do Exército Brasileiro na área da computação quântica. *Revista Análise Estratégica*. Vol 27 (5), Setembro/ Novembro de 2022. Disponível em <<http://www.ebrevistas.eb.mil.br/CEEEExAE/article/view/11160/8954>> Acesso em 12 jan. 2023.
- CORRÊA, Fernanda das Graças. Guerra russo-ucraniana: grande laboratório para ensaios destrutivos e não destrutivos de tecnologias emergentes e disruptivas. *Revista Análise Estratégica*. Vol 28 (1) Dez/Fev 2023. Disponível em <<http://ebrevistas.eb.mil.br/CEEEExAE/article/view/11454/9174>>
- CORRÊA, Fernanda das Graças. Nichos em inovação disruptiva de interesse da Defesa no Brasil: oportunidades e desafios. *Revista Análise Estratégica*. Vol 25 (3) Junho/ Agosto de 2022. Disponível em <<http://www.ebrevistas.eb.mil.br/CEEEExAE/article/view/10649/8596>> Acesso em 12 jan. 2023.
- DINIZ, Eugenio; COSTA, Isabela Simões Martins; SANTIAGO, Marcello; DIAS, Marina Peixoto; PINTO, Sabrina Santos; MENDONÇA, Victor Braga de Andrade. SISFRON: Um sistema de Defesa Nacional e Regional. *Anais do XVI Congresso Acadêmico sobre Defesa Nacional*. Escola Naval, Rio de Janeiro, RJ – Brasil. 2019. Disponível em <https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/sisfrona_uma_sistemaa_dea_defesaa_nacionala_ea_regional.pdf> Acesso em 12 jan. 2023.
- JABOUR NETO, Filipe Cury; DUARTE, Otto Carlos Muniz Bandeira. *Criptografia Quântica para Distribuição de Chaves*. COPPE-POLI/GTA - Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro - RJ – Brasil, 2016. Disponível em <<https://www.gta.ufrj.br/seminarios/CPE825/tutoriais/jabour/o19.pdf>> Acesso em 12 jan. 2023.
- JULIENNE, Marc. Le rêve quantique chinois: les aspirations d'un géant dans l'infiniment petit. *Études de l'Ifri*, février 2022. Disponível em <https://www.ifri.org/sites/default/files/atoms/files/julienne_reve_quantique_chinois_2022.pdf> Acesso em 12 jan. 2023.
- KANIA, Elsa; ARMITAGE, Stephen. Disruption Under the Radar: Chinese Advances in Quantum Sensing. *China Brief Volume: 17 Issue: 11*. Disponível em <<https://jamestown.org/program/disruption-under-the-radar-chinese-advances-in-quantum-sensing/>> Acesso em 12 jan. 2023.
- PFEIFFER, Gustavo; PAIM, Rodrigo; MOTTA, Vinicius. *Criptografia Quântica*. COPPE-POLI/GTA - Universidade Federal do Rio de Janeiro (UFRJ),

Rio de Janeiro - RJ – Brasil,2017. Disponível em <https://www.gta.ufrj.br/grad/11_1/quantica/index.html> Acesso em 12 jan. 2023.

STRIDER. *Quantum Dragon*. Strider Global Intelligence Team. November 2019. Disponível em <<https://www.striderintel.com/resources/quantum-dragon-report/>> Acesso em 12 jan. 2023.

SOUSA, Moniele S., PAULO, Alex F. de; SILVA, Flávio de; O. PEREIRA, João H. de S. Caracterização das pesquisas sobre a próxima rede global de comunicação: a Internet Quântica. *Anais do I Workshop de Comunicação e Computação Quântica*. 2021. Disponível em <<https://sol.sbc.org.br/index.php/wquantum/article/view/17220>> Acesso em 12 jan. 2023.

VIANNA, Eduardo Wallier; CAMELO, José Ricardo Souza. Defesa Cibernética no Brasil: primícias de uma história de sucesso. *Revista da Escola Superior de Guerra*. v. 35 n. 75 (2020). Disponível em <<https://revista.esg.br/index.php/revistadaesg/article/view/1144/941>> Acesso em 12 jan. 2023.