http://dx.doi.org/10.21544/2359-3075.30330

# Tecnologias Quânticas: uma questão de soberania nacional

Fernando M. Araújo-Moreira[1]
Vítor G. Andrezo Carneiro[2]
Juraci Ferreira Galdino[3]

## RESUMO

Os fundamentos da física (ou mecânica) quântica foram apresentados pelo cientista alemão Max Planck em 1900. De conteúdo científico revolucionário, esses fundamentos estabeleceram novos paradigmas que lastrearam a chamada Primeira Revolução Quântica, da qual derivaram produtos como o laser, o GPS e os chips semicondutores, essenciais na atualidade. Em 1950, Chien Shiung Wu e Irving Shaknov realizaram o que hoje é conhecido como experimento WS, que se tornou a chave para a manifestação emergente da segunda revolução quântica, que inclui novas tecnologias agrupadas em quatro grandes áreas: dispositivos quânticos (sensores, biossensores, detectores e atuadores); comunicação e teletransporte quânticos e materiais bidimensionais; computação, criptografia e internet quânticas; e tecnologias derivadas de materiais quânticos de aplicação, por exemplo, na área de energia. Este artigo procura investigar indícios de que a área de Tecnologias Quânticas é essencial não apenas para a Segurança e Defesa Nacional, mas também para a conformação do tabuleiro geopolítico. Eles sugerem que, conjuntamente, as Tecnologias Quânticas, a Inteligência Artificial (IA) e a Cibernética promoverão uma grande revolução tecnológica da humanidade e, particularmente, nos assuntos militares. Sendo assim, o artigo apresenta argumentos para que tais áreas do conhecimento e desenvolvimento tecnológico sejam consideradas estratégicas e prioritárias para o país, tendo em vista a centralidade dessas tecnologias no crescimento econômico, no desenvolvimento social, na segurança, na defesa e na soberania de uma nação no contexto da 4ª Revolução Industrial e da Era do Conhecimento.

**Palavras-chave**: tecnologias quânticas; defesa cibernética; soberania nacional.

[1] Exército Brasileiro. Instituto Militar de Engenharia/Seção de Engenharia Nuclear. Rio de Janeiro, RJ, Brasil. https://orcid.org/0000-0002-5423-0405 http://lattes.cnpq.br/1809254923092721

[2] Exército Brasileiro. Instituto Militar de Engenharia/Seção de Engenharia Elétrica. Rio de Janeiro, RJ, Brasil. https://orcid.org/0000-0002-5738-168X http://lattes.cnpq.br/6739848742248437

[3] Exército Brasileiro. Instituto Militar de Engenharia/Comando. Rio de Janeiro, RJ, Brasil. https://orcid.org/0000-0001-7805-0452 http://lattes.cnpq.br/3588063339399737

> "Portanto, digo que é uma política limitada supor que este ou aquele país deva ser marcado como o aliado eterno ou o inimigo perpétuo da Inglaterra. Não temos aliados eternos, nem inimigos perpétuos. Nossos interesses são eternos e perpétuos, e é nosso dever segui-los."
> Henry John Temple, 3º Visconde Palmerston

## INTRODUÇÃO

As tecnologias quânticas exploram fenômenos físicos probabilísticos que ocorrem em escalas atômicas e subatômicas. A natureza probabilística desses fenômenos foi tema do mundialmente famoso debate entre Albert Einstein e Niels Bohr, durante a Quinta Conferência Solvay sobre Física Quântica, realizada em outubro de 1927, em Bruxelas, e cujo principal objetivo era discutir a recém-formulada teoria quântica. Esse evento reuniu 29 (vinte e nove) das pessoas mais proeminentes da época, das quais 17 (dezessete) tornaram-se ganhadoras do Nobel.

Em 1900, no que ficou conhecido como o debate do século, Niels Bohr, um dos pais da teoria quântica (de essência probabilística) apresentada por Max Planck, defendeu a nova teoria formulada por Werner Heisenberg, enquanto Albert Einstein tentava manter um modelo de causa e efeito (ou seja, essencialmente determinístico). Einstein disse "Deus não joga dados" (fenômeno probabilístico), ao que Niels Bohr respondeu: "Einstein, pare de dizer a Deus o que fazer". Hoje, a comunidade científica concorda que Niels Bohr ganhou o debate. Isto significa que o mundo, na escala quântica, não tem um cenário fixo baseado em causa e efeito (determinístico), mas é de fato aleatório. Em outras palavras, pode-se saber tudo sobre o mundo atômico e subatômico sem saber exatamente o que acontecerá a seguir. Esta concepção deu lugar à chamada Primeira Revolução Quântica, que teve como resultados práticos o desenvolvimento de muitos produtos que, ainda hoje, têm grande utilidade, tais como o laser, o GPS e os chips semicondutores.

O paradigma probabilístico propiciou melhor compreensão de algumas das propriedades-chave das partículas atômicas e subatômicas, tais como tunelamento, superposição e emaranhamento, bem como o domínio e o progresso de outras áreas aplicadas como a tecnologia de informação, a nanotecnologia e a mecânica fina. Em 1950, Chien

Shiung Wu e Irving Shaknov realizaram o que hoje é conhecido como experimento WS, muitas vezes chamado de o primeiro experimento capaz de demonstrar o fenômeno conhecido como emaranhamento quântico. Junto com os fenômenos de tunelamento e superposição, esse fenômeno quântico se tornou a chave para o desenvolvimento da segunda revolução quântica, que inclui novas tecnologias agrupadas em quatro grandes áreas: dispositivos quânticos (sensores, biossensores, detectores e atuadores); comunicação e teletransporte quânticos e materiais bidimensionais; computação, criptografia e internet quânticas; e, tecnologias derivadas de materiais quânticos de aplicação, por exemplo, na área de energia.

Sistemas de comunicações com características muito avançadas no que concerne à segurança dos dados e a velocidade de transmissão, vasto rol de sensores com altíssima sensibilidade e dispositivos de processamento de dados com velocidades chegando a Tb/s (terabits por segundo), são algumas das possibilidades vislumbradas por especialistas no tocante às inovações que poderão surgir no curto e médio prazo. As emergentes Tecnologias Quânticas poderão influenciar a Segurança e a Defesa Nacional, impactando fortemente nas vindouras capacidades militares das Forças Armadas em todas as dimensões de um moderno Teatro de Operações, ensejando, segundo alguns autores, a Guerra Quântica, um novo paradigma para as crises e os conflitos armados. Portanto, os países que ficarem a margem desses avanços tecnológicos sofrerão com enormes vulnerabilidades à sua soberania, além de óbices ao crescimento econômico, científico e tecnológico e ao desenvolvimento social.

Com tudo isso, pode-se perceber que os avanços nas tecnologias quânticas têm características disruptivas e deverão influenciar várias expressões do poder nacional, podendo se tornar essenciais para o crescimento econômico, o desenvolvimento social e para a segurança, defesa e soberania de uma nação. Em que pesem a abrangência e a amplitude das inovações decorrentes dessas tecnologias, este artigo concentra-se nos desdobramentos dessas inovações na área de Defesa. Acompanhar tais avanços com um viés mais técnico, particularmente em uma área de difícil compreensão como a Quântica, pode ser uma tarefa bastante problemática, especialmente na área de Defesa, onde a divulgação de informações é sempre feita de forma protegida, quando é feita.

Assim, este artigo busca fazer uma prospecção, com viés qualitativo e exploratório, das principais evoluções na área de Tecnologias

Quânticas, apresentando-as de forma resumida e com base na experiência técnica dos autores na implantação de algumas dessas tecnologias. Em termos de metodologia, foi feita uma extensa pesquisa bibliográfica na área de Tecnologias Quânticas, procurando-se apresentar e organizar as referências relativas ao uso dessas tecnologias para a Segurança e Defesa. Com o foco em tecnologias que estão atualmente em desenvolvimento para uma área tão sensível como a Soberania Nacional, muitas vezes, tais referências só são encontradas em breves notícias de revistas, cabendo ao especialista ter olhos mais aguçados para compreender os aspectos técnicos do que está sendo desenvolvido.

Portanto, este artigo pretende realizar uma abordagem ampla em um mundo que passa por constantes mudanças especialmente relacionadas aos aspectos científicos, técnicos e geopolíticos relacionados com as tecnologias quânticas de segunda geração e a sua influência nas áreas de segurança e defesa nacional no Brasil e no mundo. Além disso, são apresentados alguns dos novos paradigmas essencialmente ligados às áreas de segurança e defesa, bem como discutidas as principais tendências de algumas dessas tecnologias capazes de impulsionar ainda mais a Quarta Revolução Industrial e de desenvolver elementos essenciais das capacidades militares da Guerra do Futuro.

Promover o acúmulo de capacidades tecnológicas, gerar conhecimentos e criar inovações em áreas sensíveis e críticas, como as tecnologias quânticas, é ao mesmo tempo um grande desafio e uma extraordinária oportunidade para o crescimento econômico, o desenvolvimento social e a soberania nacional dos países. As tecnologias quânticas deverão impactar fortemente todos os campos da Expressão do Poder Nacional, entretanto, é na Expressão Militar que são esperados os principais desdobramentos, pelas consequências vislumbradas em todas as dimensões do combate (terrestre, naval, aérea, espacial e cibernética), conforme ilustrado na Figura 1.


Figura 1: Aplicações das Tecnologias Quânticas em Defesa Nacional (adaptado de KRELINA, M., 2021).

Essas tecnologias não apenas potencializam as atuais, mas também podem criar poderosas e inovadoras capacidades militares, promovendo uma Revolução nos Assuntos Militares, ou até mesmo uma Revolução Militar. As expectativas de mudanças são tão grandes que alguns autores até prenunciam o surgimento de uma nova geração da guerra: a Guerra Quântica. Outros consideram a quântica não apenas uma nova geração da guerra, mas também uma nova dimensão do combate.

Segundo Krelina, a Guerra Quântica (do inglês, Quantum Warfare) é aquela que usa as tecnologias quânticas para aplicações militares que afetam as capacidades de inteligência, segurança e defesa de todos os domínios da guerra e isso introduz novas estratégias militares, doutrinas, cenários e questões de paz, assim como questões éticas3.

As Tecnologias Quânticas, dentre outras possibilidades, permitirão medir ou detectar objetos até então indetectáveis para os atuais paradigmas tecnológicos, resolver problemas complexos, atualmente, sem solução e alçar as ações cibernéticas a um patamar acima dos atuais, tanto em termos de segurança, com a criptografia quântica, quanto em termos de processamento dos dados, com a computação e os algoritmos quânticos.

Na área de Segurança e Defesa, algumas aplicações merecem ser detalhadas, pela importância e desdobramentos no curto e médio prazo7. A seguir são abordadas três das muitas Tecnologias Quânticas com possíveis aplicações nas áreas de Segurança e Defesa: dispositivos quânticos; comunicação quântica; e computação quântica.

O presente artigo optou por focar nessas três Tecnologias

Quânticas, por estarem em uma fase mais avançada de desenvolvimento e dado o enorme impacto delas, particularmente na área de Cibernética, considerando a forte dependência atual do mundo em relação aos computadores. No entanto, a área de Quântica possui tantas características disruptivas, que os autores não poderiam se furtar de comentar sobre outros possíveis impactos sobre a Segurança e a Defesa.

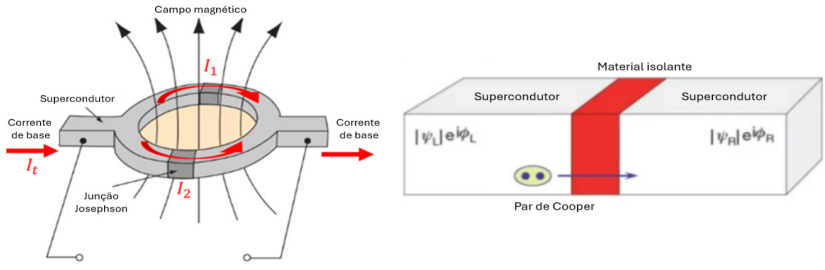
(a) Dispositivos Quânticos.

Neste contexto, serão discutidos os dispositivos de sensoriamento quântico, particularmente sensores, biossensores, detectores e atuadores que utilizam os princípios quânticos de tunelamento, superposição e emaranhamento quânticos, pela possibilidade de medição de grandezas físicas, alcançando sensibilidades muito além do limite clássico. Já existem tecnologias de sensoriamento comerciais que usam fenômenos quânticos para atingir níveis elevados de precisão na medição, incluindo aplicações em relógios atômicos, ressonâncias magnéticas e paramagnéticas nucleares e microscópios eletrônicos.

De acordo com a NSF (National Science Foundation), o equivalente estadunidense do CNPq, nos próximos dez anos várias oportunidades estarão disponíveis em termos de dispositivos quânticos de última geração para aplicação nas áreas de biotecnologia e defesa, posicionamento e navegação, e sistemas de cronometragem úteis tanto para as forças armadas quanto para o setor civil, ao mesmo tempo que oferecerá novas oportunidades para abordar problemas complexos em ciência dos materiais, química e física. Essas aplicações têm implicações abrangentes em áreas importantes como energia e segurança, impactando a rotina diária da população em geral.

Um dos mais importantes dispositivos quânticos para sensoreamento é o denominado S.QU.I.D. (Superconducting QUantum Interference Device), utilizado para medir campos magnéticos (Figura 2a). Ele é formado pela associação de uma ou mais junções Josephson (Figura 2b),. Um dos aspectos mais interessantes desta junção é que ela é a base do quantum bit (abreviado como qubit) utilizado na fabricação de uma das estratégias ou rota tecnológica para desenvolver o computador quântico. O qubit é formado por uma partícula ou propriedade física que assume um estado de superposição, o que significa que ele pode representar os dois estados lógicos 1 e 0, simultaneamente. O estado (1 ou 0) só é

definido no momento da medida e as estatísticas ocorrem com uma certa probabilidade, que depende do tipo de processo que gerou o qubit.




(a) (b)

Figura 2: (a) Esquema de sensor SQUID; (b) esquema de junção Josephson.

Por exemplo, na área de energia, as aplicações em sensoriamento quântico são bem abrangentes, incluindo energia renovável, energia nuclear, gestão de rejeitos nucleares, energia fóssil, energia geotérmica, eletricidade, eletrificação de veículos etc. As aplicações potenciais do sensoriamento quântico em áreas de energia fóssil são mostradas na Tabela 1. Os diferentes tipos de sensores quânticos são mostrados na Tabela 2.

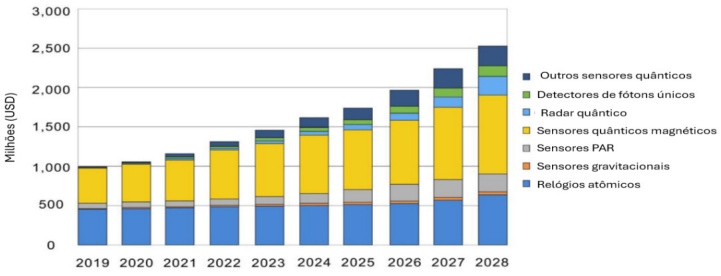
Tabela 1: Aplicações potenciais do sensoriamento quântico em áreas de energia fóssil.

| Área de energia fóssil | Aplicação de sensoreamento |
|---|---|
| Utilização de CO2 e beneficiamento de carvão | Detecção rápida e sensível de emissão e vazamentos de CO2, detecção de metais de alto valor de carvão e subprodutos de utilização de carvão. |
| *Upstream* de Petróleo e gás | Gravímetros quânticos para a detecção de depósitos de petróleo / gás. |
| *Midstream* de Petróleo e gás | Monitoramento da integridade da tubulação durante o transporte e armazenamento. |
| *Downstream* de Petróleo e gás | Monitoramento da emissão de CO2 durante o consumo. |
| Captura e armazenamento de carbono | Detecção rápida e sensível de emissão de CO2 e vazamentos. |
| Extração e recuperação de carvão | Detecção de elementos metálicos críticos de carvão e subprodutos de utilização de carvão, gravímetros para exploração de carvão, segurança de minas de carvão. |
| Geração de eletricidade | Sensores que monitoram campos eletromagnéticos. |
| Transporte e distribuição de eletricidade | Monitoramento de temperatura em transformadores. |
| Física e energia nuclear | Monitoramento da segurança nuclear nacional, dispositivos de interferência quântica supercondutora (SQUIDs). |

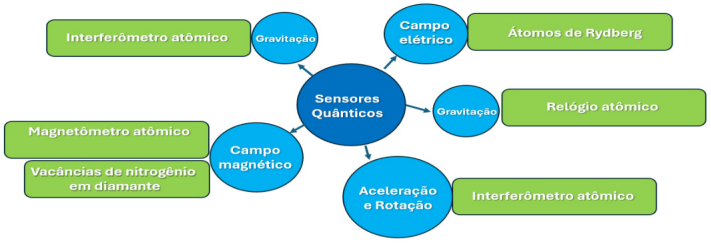
Tabela 2: Diferentes tipos de sensores quânticos e as tecnologias a eles associadas.

| Tecnologia | Características quânticas | Condições experimentais | Vantagens vs. sistemas clássicos | Desafios |
|---|---|---|---|---|
| Sensores quânticos não fotônicos | Spin *qubits*, átomos neutros, íons presos | Medições de múltiplos parâmetros | Alta sensibilidade, baixo ruído | Decoerência, ruído de projeção quântica |
| Detecção remota de alvos | Iluminação quântica, emaranhamento quântico | Interferometria quântica | Relação sinal-ruído aprimorada | Muito frágil em relação à perda óptica |
| Radar quântico | Iluminação quântica de micro-ondas | Interferometria quântica | Expor alvos furtivos | Falta de conversores de fóton-micro-ondas |
| Espectroscopia quântica | Emaranhamento quântico, fótons únicos | Medições de correlação de intensidade | Além do limite de ruído de disparo, aproximando-se do limite quântico final | Decoerência quântica |
| Microscopia quântica | Emaranhamento quântico, | Microscopia e detecção quântica | Super resolução além do limite de Rayleigh | Localização desconhecida do centroide de origem |
| Interferômetros quânticos | Estados emaranhados, luz espremida | Interferômetros de menor escala | Escala de Heisenberg | Muito frágil em relação à perda óptica |
| Detector de ondas gravitacionais | Luz espremida | Interferômetros de tamanho quilômetro | Escala de Heisenberg | Muito frágil em relação à perda óptica |
| Leitura quântica da memória óptica clássica | Discriminação de canal quântico | Interferômetro e fonte de fóton único | Leitores ópticos mais rápidos e sem erros e memórias mais densas | Uso de fontes de fótons e detectores com altíssima eficiência |

A Figura 3 mostra um resumo das previsões de dez anos para o mercado de sensores quânticos por tipo de sensor e as aplicações desses sensores quânticos.




(a)




(b)

Figura 3: (a) Resumo das previsões de dez anos para o mercado de sensores quânticos por tipo de sensor; (b) aplicações de sensores quânticos.

Especificamente, na área de Segurança e Defesa nacional, o sensoriamento quântico deverá ter muitas aplicações nos diferentes teatros de operações e domínios do combate. Podem ser usados, por exemplo, na fabricação de sensores e detectores de explosivos e de agentes de guerra químicos, biológicos, radiológicos e nucleares. Os dispositivos de PNT (do inglês, Position, Navigation and Timing) quânticos podem ser usados como sistemas de navegação inercial confiáveis, permitindo a navegação sem uma referência externa, como, por exemplo, GPS. Quando plenamente desenvolvido, esse recurso poderá ser revolucionário tanto para a navegação subaquática quanto para plataformas terrestres3.

Outra aplicação muito importante do sensoriamento quântico e com grandes desdobramentos no Teatro de Operações e cujas pesquisas já se encontram em estágios intermediários de maturidade tecnológica, é a detecção, identificação e estimação de PNT de submarinos e aeronaves furtivas. Uma pequena amostra da evolução nesse setor é apresentada a seguir.

No final de 2023, o governo canadense anunciou a compra de

88 unidades do avião caça considerado o 2º mais moderno do mundo: o F35 Lightning. Fabricados pela estadunidense Lockheed Martin, o custo da operação foi de aproximadamente 14 bilhões de dólares americanos, ou seja, o preço de cada unidade custou aproximadamente USD 160 milhões (ou R$ 0.96 bilhões cada unidade). Esse custo é justificado pois o F-35 Lightning possui diversas características de última geração, como o motor mais potente do mundo, produzido pela Pratt & Whitney; os modernos sensores que criam imagens amplas do campo de batalha, possibilitando uma melhor consciência situacional, necessária para a realização do C4ISR (sigla do inglês que significa, Comando, Controle, Comunicações, Computação, Inteligência, Vigilância e Reconhecimento); um sistema robótico avançado, chamado VLO Stealth, que tem capacidade incomparável de detectar o inimigo e entrar no espaço aéreo contestado; possui um "Sistema de Guerra Eletrônica", que detecta inimigos e bloqueia radares. Por sua sofisticação multifuncional, ele permite que o piloto opere em qualquer ambiente e contra qualquer ameaça, mas a característica que o diferencia dos outros caças é a sua furtividade (também conhecida como stealth mode, ou simplesmente stealth), ou seja, a sua capacidade de ser invisível aos radares inimigos.

Entretanto, a capacidade de furtividade do F35 e de demais caças tende a se tornar uma tecnologia ultrapassada com o desenvolvimento de um sensor quântico de última geração para atuar como radar, como anunciado pela China. A P&D desse radar foi iniciada na última década[v]. Atualmente, supõe-se que esteja em estágio de maturidade tecnológica (do inglês, Technology Readiness Level – TRL) acima de 6, sugerindo que pode inviabilizar as tecnologias de furtividade em uso. Este é um dos casos demonstrativos de quebra de paradigmas na área de Defesa decorrente da produção de sensores quânticos.

Os avanços chineses no setor são contestados pelos estadunidenses. O físico Jeffrey Shapiro, professor do Instituto de Tecnologia da Massachusetts (MIT) e um pioneiro da ideia de radar quântico, opinou que ainda há muitos desafios tecnológicos a serem superados para que o radar seja eficaz. Por outro lado, a China Electronics Technology Group Corporation (CETC) revelou um protótipo alegando que poderia identificar aeronaves furtivas em voo. Adicionalmente, cientistas chineses explicaram que partículas quânticas de alta energia seriam capazes de adquirir alvos não visíveis aos radares convencionais. Apesar da guerra de narrativas, deve-se levar em conta que pesquisadores chineses afirmam

que já conseguiram demonstrar o efeito de detecção furtiva, com alvos a distâncias significativas e, principalmente, os demonstradores tecnológicos que vem sendo apresentadas pela China.

Figura 4: YIC-8E, o primeiro radar quântico anti-stealth do mundo, criado pela China.

Demonstrando sua capacidade tecnológica no setor, a China apresentou, recentemente, um radar revolucionário no Zhuhai Airshow: o YLC-8E. Esse radar quântico, que vem sendo desenvolvido pela China (Figura 4), utiliza fótons de micro-ondas emaranhados como método de detecção e, pelo menos em princípio, poderá anular a tecnologia stealth dos chamados aviões invisíveis. Esse desenvolvimento é visto como um grande desafio para os jatos de combate F-35 e F-22 altamente avançados dos EUA.

Figura 5: Imagens do novo drone furtivo russo S-70.

Outro exemplo demonstrativo dos avanços da aplicação de dispositivos quânticos na área de defesa é o drone de ataque superpesado russo (S-70 da Sukhoi-MIG), chamado de Okhotnik (ou Caçador), visto na Figura 5. Ele já foi empregado experimentalmente em 2019, possui 20 toneladas de peso e autonomia de 6.000 km, podendo alcançar a velocidade máxima de 1.000 km/h . Suas características operacionais de invisibilidade (grau de furtividade) e elevada capacidade de sensoreamento indicam o possível uso de sensores quânticos, dada a sua alta sensibilidade e precisão.

Figura 6: Bombardeiro supersônico Stealth chines, H20.

O H-20, o novo bombardeiro supersônico chinês (Figura 6), apresentado durante as duas sessões do Congresso Nacional do Povo, é outra inovação importante que sugere a elevada capacidade tecnológica dos chineses em tecnologias quânticas, particularmente em dispositivos quânticos. Em uma entrevista concedida ao Hong Kong Commercial Daily, em março de 2024, Wang Wei, subcomandante da Força Aérea do Exército de Libertação Popular, revelou que o H-20 será anunciado oficialmente em breve ao público, e negou que haja gargalos técnicos, dizendo que o H-20 "é algo para se orgulhar e empolgar". O significado é grande. Uma das características do H20 é o número de dispositivos quânticos de sensoriamento e detecção tanto a bordo quanto nos equipamentos de ataque.

(b) Comunicação Quântica

Atualmente, busca-se conferir segurança dos dados das comunicações civis e militares por meio técnicas como criptografia e salto em frequência, esta última afeta mais as comunicações militares, isso ocorre tanto nas comunicações confinadas, via fibra óptica, por exemplo, quanto nas não confinadas, como as comunicações sem fio comumente praticadas em Teatros de Operações usando rádios militares de comunicações táticas. Em ambiente de rede, usa-se também a troca de chaves criptográficas para tornar as comunicações mais seguras.

Entretanto, esses sistemas de comunicações convencionais, exploram fenômenos eletromagnéticos que são vulneráveis a interferências, interceptações e a ações de hackers, os quais podem copiar bits em trânsito sem deixar rastros. O novo paradigma de comunicações quânticas permite preservar a confidencialidade na transmissão.

A comunicação quântica, por outro lado, tira proveito das leis da física quântica para proteger a informação. Essas leis permitem que as partículas – normalmente fótons de luz – assumam um estado de superposição, formando o qubit de comunicação. Do ponto de vista da cibersegurança, quando um hacker tenta invadir o sistema, enquanto esses dados estão em trânsito, o estado do qubit é alterado deixando um rasto da sua invasão. Assim, um hacker não pode mexer nos qubits sem abandonar um sinal revelador de sua atividade.

Em consequência disso, muitas pesquisas vêm sendo realizadas no sentido de serem criadas redes de transmissão de dados altamente sensíveis com base em um processo chamado de distribuição de chaves quânticas (do inglês, Quantum Key Distribution – QKD) que, na teoria, são ultra seguras. Nesse processo, as propriedades quânticas de certas partículas são usadas para gerar uma chave secreta, que é conhecida somente pelas duas partes interessadas em se comunicar. O fóton foi a partícula física que se tornou a candidata natural para a implementação dos qubits em comunicações quânticas. Como ele é normalmente transportado por fibras ópticas ou enlaces FSO (Free-Space Optics), aumentou a importância dos grupos de pesquisa de todo o mundo que trabalham com fotônica ou óptica quântica.

O segredo do QKD está nas chaves criptográficas, que são criadas e transmitidas na forma de qubits, portanto com grande segurança28. No entanto, as chaves criadas são usadas para criptografar os dados de forma clássica. Em uma das abordagens de QKD, o Protocolo BB84, cujo nome vem dos seus criadores (Charles H. Bennett e Gilles Brassard) e do ano de proposição (1984), uma das pontas cria a chave e a envia por um canal óptico. Em seguida, as duas extremidades comparam uma parte de suas chaves, o que é conhecido como refinamento da chave, para saber se possuem a mesma chave. Além disso, um outro processo, conhecido como destilação da chave, consegue detectar se a chave foi interceptada ou não por um hacker. Caso isso ocorra, essa chave é descartada e novas são geradas até que se tenha certeza de que uma chave segura foi compartilhada.

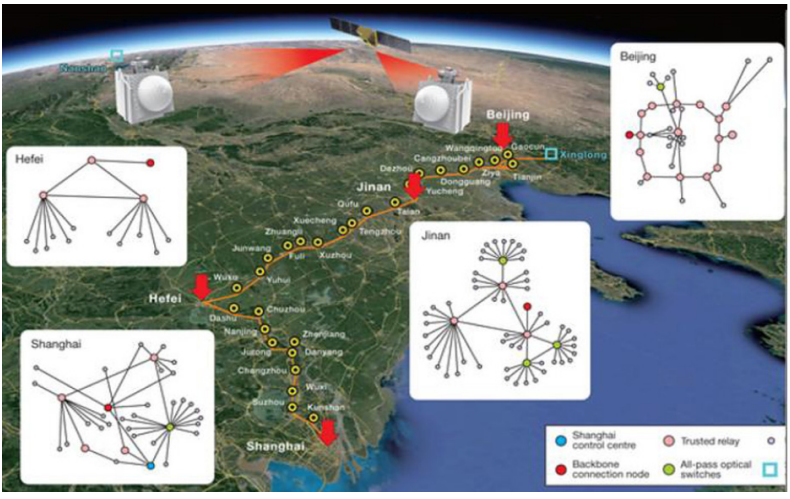



Figura 7: Rede de comunicação QKD entre Pequim e Xangai.

A China vem demonstrando sucessivos avanços no desenvolvimento das comunicações quânticas. Em 2016, a China lançou os primeiros satélites de comunicação quântica, que usavam enlaces FSO para estabelecer uma comunicação QKD entre duas estações terrestres separadas por 2.600 km. Em 2017, já havia uma rede de comunicação quântica, com mais de 2.000 km, entre Pequim e Xangai, via enlaces de fibra óptica, com diversos repetidores e dois satélites para o apoio na geração e transmissão das chaves quânticas (Figura 7). Em 2021, os pesquisadores já haviam aumentado o alcance máximo de um enlace de QKD puramente terrestre para além de 500 km, usando uma tecnologia conhecida como QKD de campo duplo (TF-QKD)30.

Apesar desses avanços, ainda há muito espaço para a pesquisa em redes de comunicação quântica. Por exemplo, o canal de comunicação quântico pode ser ruidoso ou possuir imperfeições que geram erros. Tais erros podem ser confundidos como sendo devidos à presença de um espião e fazerem com que as chaves geradas sejam descartadas.

Um outro problema a ser estudado são os repetidores quânticos, necessários para redes de longa distância. A rede Pequim-Xangai usa cerca de 30 repetidores, chamados de nós confiáveis (trusted nodes), onde as chaves quânticas são descriptografadas em bits para depois serem retransmitidas quanticamente. Um hacker que invada esses nós pode

copiar os bits sem ser detectado.

Visando mitigar esses riscos, alguns pesquisadores trabalham com outro tipo de abordagem, conhecida como teletransporte quântico. Essa tecnologia se baseia na criação de pares de fótons emaranhados, que são transmitidos para as duas extremidades do canal. Sempre que uma interação posterior muda o estado do fóton emaranhado de uma das extremidades, o estado do fóton da outra extremidade também é alterado, por conta do emaranhamento quântico. Para isso, nenhum canal quântico é necessário. Somente um canal clássico que transmita o resultado da medição feita pelo transmissor. Porém, criar uma rede de teletransporte com muitos nós ainda é um grande desafio. Pesquisadores de todo o mundo estão buscando formas confiáveis de produzir fótons emaranhados, em escala, sob demanda e mantendo seu emaranhamento por grandes distâncias.

Em 2015, um estudo publicado demonstrou o teletransporte de dois estados quânticos do fóton, o seu spin e o seu momento angular. Ambos foram usados como qubits. Em 2017, o satélite Micius, da China, foi usado para teletransportar dois fótons entre a Áustria e a China, em um experimento de comunicação quântica de 7.600 km. Notadamente, a China é o país mais avançado nessa tecnologia (Figura 8). Em 2022, esse país estabeleceu um canal de *Comunicação Direta com Segurança Quântica* (QSDC) de 102,2 km, alcançando o novo recorde para esse tipo de comunicação. O recorde anterior para esse tipo de canal era de 18 km. Um canal QSDC realiza tarefas diferentes de um sistema QKD, no sentido em que é criado um canal quântico para a transmissão segura e confiável, tanto em relação a ruídos quanto a escutas. Usualmente, a criação desse canal seguro envolve a geração de fótons emaranhados.

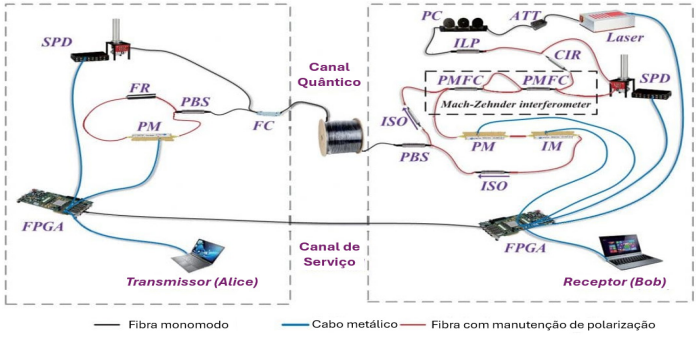



Figura 8: Rede criada pela China quebrando recorde de distância de

QSDC (adaptado de ZHANG, H. et al., 2022).

No âmbito da área de Defesa no Brasil, destaca-se o empreendimento liderado pelo Instituto Militar de Engenharia (IME), cuja execução conta com a parceria de outros centros de pesquisa do Brasil, para também propor um modelo de comunicação quântica, baseada na geração e distribuição de fótons emaranhados. Denominado Rede Hermes Quântica (RHQ), o projeto pretende, inicialmente, estabelecer uma rede de três nós entre o IME, a ECEME (Escola de Comando e Estado Maior do Exército) e o CBPF (Centro Brasileiro de Pesquisas Físicas) (Figura 9a). Nesta rede, será estabelecido um protocolo QKD, baseado em emaranhamento e enlaces FSO.


(a) (b)

Figura 9: (a) Rede Hermes Quântica (RHQ): as linhas vermelhas representam os links do IME para a Escola de Comando e Estado-Maior do Exército, ECEME, e para o Pão de Açúcar; a linha azul mostra o link do IME até o Centro Brasileiro de Pesquisas Físicas (CBPF); (b) Rede Rio Quântica (RRQ) com sua extensão.

Este projeto estratégico para as Forças Armadas, conta em sua execução com o apoio do CBPF, da UFF (Universidade Federal Fluminense), da PUC-Rio (Pontifícia Universidade Católica do Rio de Janeiro) e da UFRJ (Universidade Federal do Rio de Janeiro). Outro parceiro importante é a UFPE (Universidade Federal de Pernambuco), cujo Departamento de Física vem atuando no desenvolvimento de dispositivos quânticos necessários para a computação e comunicação quântica fim-a-fim, sem a necessidade de repetidores de sinais que empregam o paradigma convencional. Os resultados das pesquisas da UFPE são essenciais para as próximas fases

da RHQ, nas quais são previstos enlaces de fibra óptica de longa distância. O IME assinou em março de 2024 um Acordo de Cooperação Técnica com a UFPE e esta instituição figura como uma das parceiras na RHQ.

A RHQ é sinérgica e complementar a outro importante projeto que vem sendo realizado pelas mesmas instituições: a Rede Rio Quântica (RRQ), um empreendimento liderado pela UFF. O objetivo principal deste projeto é estabelecer uma rede metropolitana de comunicação quântica, conectando essas instituições e o IME. Alguns dos enlaces se estendem por dezenas de quilômetros, via fibra óptica. Existe também a previsão de um enlace aéreo de cerca de 7 km atravessando a Baía de Guanabara (Figura 9b).

(c) Computação Quântica

Os primeiros passos visando ao desenvolvimento da computação quântica iniciou-se na década de 1950. Em 1981, durante uma conferência no MIT, um dos pais da mecânica quântica moderna, o físico Richard Feynman, apresentou uma proposta para utilização de sistemas quânticos em computadores, que teriam então uma capacidade de processamento superior aos computadores comuns. Em 1985, David Deutsch, da Universidade de Oxford, descreveu o primeiro computador quântico como uma Máquina de Turing Quântica.

Depois de Deutsch, apenas em 1994, houve notícias da computação quântica, quando em Nova Jersey, no Bell Labs da AT&T, o professor de matemática aplicada Peter Shor desenvolveu um algoritmo *(Algoritmo de Shor),* capaz de fatorar grandes números numa velocidade muito superior àquela dos computadores convencionais (clássicos). Em 1996, Lov Grover, também da Bell Labs, desenvolveu o Speedup, o primeiro algoritmo para pesquisa de base de dados quânticos. Em 1999, foram construídos no MIT os primeiros protótipos de computadores quânticos baseados em princípios térmicos. A Fig. 10 mostra o elemento principal de um computador quântico: o chip que armazena os *qubits.*

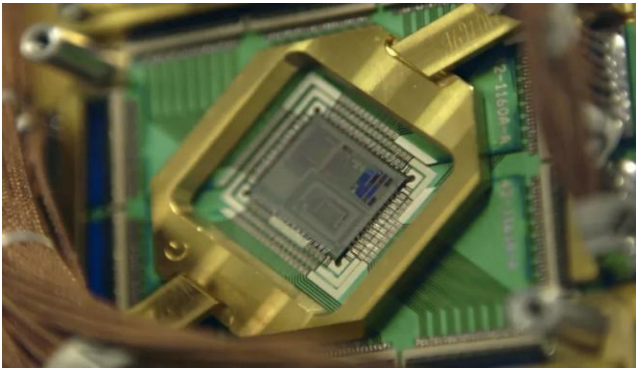


Figura 10: Elemento principal de um computador quântico: o chip que armazena a estrutura de *qubits*.

No ano de 2007, surge o Orion, um processador quântico de 16 qubits que realiza tarefas práticas. Ele foi desenvolvido pela empresa canadense D-Wave Systems, com base em princípios de supercondutividade. Em 2011, essa empresa lançou o primeiro computador quântico comercial chamado D-Wave One, com processador de 128 qubits. Porém, o D-Wave One ainda não era totalmente independente e precisava ser usado em conjunto com computadores convencionais. Em 2017, a mesma empresa lançou comercialmente o D-Wave 2000Q, um computador quântico de 2000 qubits com preço de US$ 15 milhões. Atualmente, a D-Wave já possui computadores quânticos com mais de 5000 qubits. Em que pese a quantidade de qubits não ser mais um fator determinante da evolução de um computador, pois os chips mais modernos estão investindo na qualidade e no maior controle dos qubits, 5000 qubits representam um marco de desenvolvimento.

A Figura 11 mostra os principais players mundiais na área de fabricação de computadores quânticos e o tipo de qubit utilizado para o seu desenvolvimento.

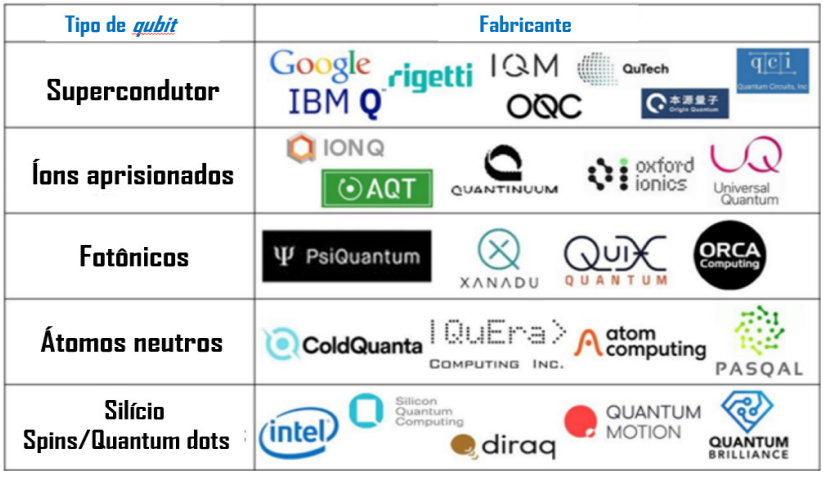



Figura 11: Principais players mundiais na área de fabricação de computadores quânticos e o tipo de *qubit* utilizado para o seu desenvolvimento.

Dentre as inúmeras possibilidades vislumbradas para aplicação da computação quântica, uma merece destaque: a fatoração de números inteiros. Essa é uma classe de problema matemático que os computadores clássicos demoram um tempo extremamente longo para solucionar (da ordem de milhares de bilhões de séculos), enquanto os quânticos podem resolver com eficiência em questão de algumas poucas horas.

Na teoria dos números, a fatoração de inteiros é a decomposição de um número composto em um produto de números inteiros menores. Se esses fatores forem restritos aos números primos, por exemplo, o processo é denominado fatoração prima. Apesar de muito antigo, o problema da fatoração de grandes números inteiros ainda não foi solucionado de forma eficiente. O interesse de se encontrar uma solução para este problema aumenta cada vez mais, pois a segurança dos atuais métodos de criptografia de chave pública, como o RSA (acrônimo composto pelas letras iniciais dos sobrenomes de Ron Rivest, Adi Shamir e Leonard Adleman), depende da atual eficiência dos métodos de fatoração. Quando os números são suficientemente grandes, nenhum algoritmo de fatoração de números inteiros não quântico eficiente é conhecido. Muitas áreas da matemática e da ciência da computação se envolvem com esse problema, inicialmente a

teoria algébrica dos números e, mais recentemente, a computação quântica.

Adicionalmente, já existem algoritmos quânticos para resolver estes problemas e decifrar comunicações digitais, como o Algoritmo de Shor, citado anteriormente35, que só pode ser executado num computador quântico. Esse algoritmo é capaz de analisar e fatorar números inteiros de qualquer tamanho. Por exemplo, Gidney e Ekera indicam que é possível fatorar um inteiro de 2048 bits em apenas 8 horas, usando um computador com 20 milhões de qubits. Com a tecnologia atual, são necessários milhares de anos.

Dessa maneira, a computação quântica terá muita aplicação na análise de grandes quantidades de dados. Entretanto, esta nova tecnologia não apenas acelera a computação convencional, mas também oferece maior capacidade de processamento para certos tipos de problemas, além da fatoração de números muito grandes, como: sequenciamento de DNA, inteligência artificial e previsão do tempo, entre outras áreas.

A transmissão segura de dados através da comunicação quântica e a computação quântica aplicada à cibernética são de fundamental importância. Em termos de segurança e defesa nacional, a computação quântica deverá ser crucial, principalmente quando aplicada à cibernética já que a maior parte da infraestrutura digital planetária e quase todas as atividades realizadas online, como videoconferências, envio de e-mails e acesso remoto de contas bancárias, são baseadas na criptografia realizada através de protocolos que usufruem da incapacidade de recursos computacionais existentes resolverem a fatoração de números inteiros grandes.

Embora os computadores quânticos não tenham o poder de processamento de decifrar a maioria dos métodos de criptografia, deve-se encontrar maneiras de proteção dessa ameaça, pois os avanços na capacidade desses computadores têm sido expressivos e como os investimentos nessa área em pesquisa científica e desenvolvimento tecnológico estão aumentando, a tendência é de que o ritmo desse aumento não arrefeça. Como dito antes, estima-se que um computador quântico precisaria ter cerca de 20 milhões de qubits para quebrar a criptografia RSA atual – usada para enviar dados confidenciais pela Internet. Levando em consideração que o maior computador quântico atualmente tem 5000 qubits (D-Wave), pode-se afirmar que ainda falta muito tempo para quebrar essa criptografia37.

Em síntese, apesar de ainda não existirem computadores

quânticos comerciais para a população em geral (apenas dispositivos com fins educacionais com baixo número de qubits), os desenvolvimentos nesta área já se encontram numa fase intermédia de maturidade tecnológica. Com a perspectiva do desenvolvimento de computadores quânticos comerciais, é factível imaginar que informações criptografadas dos sistemas de comunicações em utilização estão sendo armazenadas para serem utilizadas na decifragem quando a nova tecnologia estiver disponível.

De fato, a computação quântica é uma ameaça urgente à segurança cibernética da sociedade, em geral, e dos sistemas empregados na área de Segurança e Defesa nacional, em particular. Para combatê-la, deve-se atualizar completamente toda a infraestrutura digital. Nesse sentido, merecem destaque algumas abordagens discutidas a seguir.

Uma possibilidade para proteger as informações atuais contra os computadores do futuro é implementar o que é conhecido como criptografia pós-quântica (do inglês, Post-Quantum Cryptography – PQC). Apesar do nome, trata-se de novos algoritmos criptográficos clássicos (ou seja, não são quânticos), cuja solução por computadores quânticos seria tão demorada quanto o dos algoritmos clássicos atuais.

O órgão dos EUA equivalente ao INMETRO brasileiro, o NIST (Instituto Nacional de Padrões e Tecnologia), realizou uma competição/consulta internacional, na qual selecionou três algoritmos PQC para padronização e adoção global. O processo começou em 2016 e, em agosto de 2023, foram solicitados comentários públicos a respeito dos três finalistas. O período de comentários foi finalizado em novembro de 2023 e a decisão final do NIST foi tomada em agosto deste ano. Um dos objetivos do NIST é de que os algoritmos selecionados possam interoperar com os protocolos e redes de comunicações existentes. Com os algoritmos padronizados, espera-se que o IETF (Internet Engineering Task Force), responsável pelo desenvolvimento e promoção de padrões da Internet, incorpore-os em novas versões de protocolos como IPSec (sigla em inglês para IP Security protocol) e TLS (Transport Layer Security), já em 2025.

Uma outra opção seria esperar que a comunicação quântica, via criptografia quântica, teletransporte quântico ou outra implementação mais moderna, amadureça a ponto de usar esse tipo de comunicação para se proteger de ataques de descriptografia realizados por computadores quânticos. A implementação mais conhecida de criptografia quântica são os protocolos QKD.

Investir na comunicação quântica (QKD ou teletransporte quântico), promovendo o seu amadurecimento na expectativa de que ela venha a oferecer resiliência à ameaça quântica, é uma abordagem que está sendo adotada por vários grupos de pesquisa brasileiros, como as iniciativas promovidas pelo IME e pelas universidades do projeto RRQ. Os formuladores de políticas públicas e líderes de todas as esferas, devem ficar atentos e preparados para a necessidade de atualizações na área de segurança cibernética.

(d) Corrida mundial pelo domínio das Tecnologias Quânticas

As Tecnologias Quânticas são transversais e possuem amplo espectro de aplicação em Segurança e Defesa nacional, sendo fundamentais ao desenvolvimento de novas capacidades militares essenciais para a Guerra do Futuro.

Os avanços nas áreas associadas com as Tecnologias Quânticas estão sendo surpreendentes, particularmente pelos grandes interesses governamentais e privados que mobilizam cifras extraordinárias de recursos financeiros para fomentar as pesquisas básicas, pesquisas aplicadas e as pesquisas e desenvolvimentos, bem como para formar recursos humanos altamente qualificados para explorar todas as facetas ainda não descobertas das tecnologias quânticas.

A Figura 12 mostra os investimentos realizados no mundo em 2022 que somaram aproximadamente 30 bilhões de dólares (aproximadamente R$ 160 bilhões). Em 2023, essa quantia ultrapassou os USD 38 bilhões (cerca de R$ 228 bilhões) e a previsão é que em 2040 ultrapasse USD 106 bilhões, mais de meio trilhão de reais,. A China aparece como o maior investidor na área (USD 15 bilhões). O Brasil aparece com tímidos USD 12 milhões de investimentos em 2023.

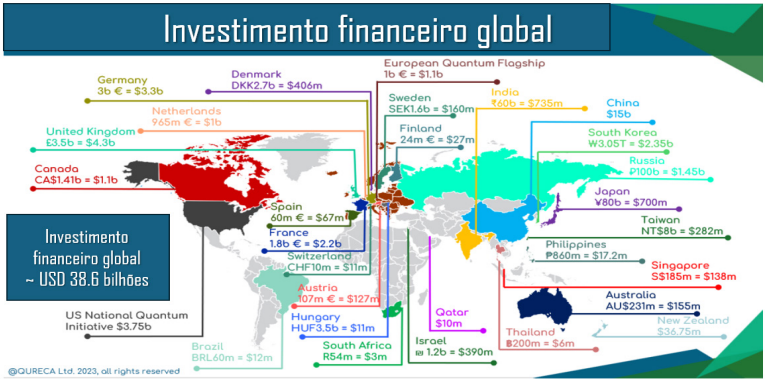



Figura 12: Investimentos realizados no mundo em 2023.

Além da questão financeira, há que se considerar também a infraestrutura nacional para armazenamento e tratamento dos dados. O que é comumente conhecido como a "nuvem", nada mais são do que servidores distribuídos em enormes datacenters, responsáveis pelo armazenamento e processamento dos sistemas na internet. Trata-se de uma questão da soberania de dados: países que não possuem soberania sobre sua infraestrutura e bases de dados físicos locais correm o risco de ter seus dados utilizados por outros países para o desenvolvimento de tecnologias quânticas. Além disso, as tecnologias quânticas, particularmente a computação e a comunicação quântica, também necessitarão de datacenters preparados para receberem os hardwares quânticos.

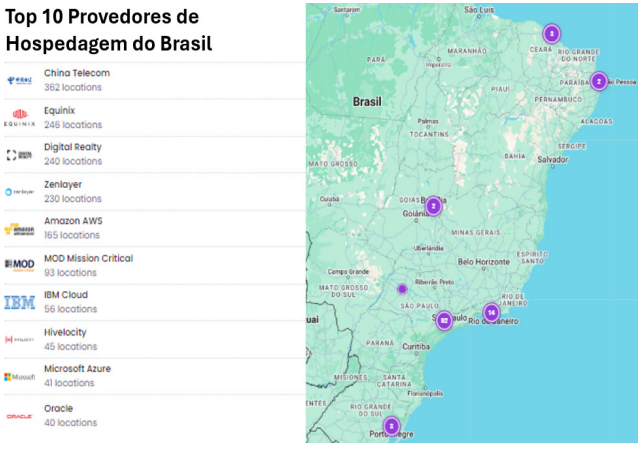



Figura 13: Distribuição dos principais provedores de hospedagem

no Brasil

O Brasil possui uma rede de datacenters ainda pequena, mal distribuída e controlada por grandes corporações estrangeiras, como pode ser visto na Figura 1346. São 117 datacenters no território nacional, distribuídos em somente em 6 estados e controlados por 26 fornecedores, a maioria deles estrangeiros. São esses datacenters que armazenam as principais informações dos sistemas brasileiros. Portanto, trata-se de uma questão de soberania que o software e o hardware quântico não tenham que ser hospedados em locais controlados por estrangeiros.

## REFLEXOS DAS TECNOLOGIAS QUÂNTICAS E DA 4ª REVOLUÇÃO INDUSTRIAL NA DEFESA NACIONAL

A quarta revolução industrial é caracterizada pela fusão das esferas físicas, digitais e biológicas, com tecnologias sendo desenvolvidas nessas três esferas para um desenvolvimento mais acelerado do setor produtivo. Nessa revolução, obtém-se uma sinergia de avanços e inovações disruptivas em diversos setores da ciência e tecnologia, que quando combinadas impactam as mais diversificadas áreas da sociedade, o crescimento e o desenvolvimento econômico, a segurança e a soberania nacional, as relações internacionais e, particularmente, a natureza dos conflitos e das guerras. No bojo dessa revolução são identificadas algumas tendências, que serão analisadas com maior foco no presente texto, como a hiperconectividade, a digitalização e a convergência digital, assim como o compartilhamento de informações, por exemplo, armazenadas em "nuvem". Essas tendências têm um grande impacto na Segurança e Defesa Cibernética, área que será fortemente afetada pelas Tecnologias Quânticas.

Como consequência desse avanço vertiginoso, é possível identificar hoje uma internet móvel omnipresente e eficaz; redução no tamanho e no custo e aumento na capacidade dos sensores que surgem para monitorar os mais variados fenômenos e objetos; além de robôs; internet das coisas (IoT), internet das coisas no campo de batalha (IoBT), cidades inteligentes, veículos autônomos, manufatura aditiva, tecnologias vestíveis, enxames de drones, armas inteligentes dentre muitas outras. Face à imensidão de tecnologias que permeiam essa revolução, aqui, foca-se nas discussões e interdependências entre IA, Cibernética e Tecnologias Quânticas e algumas possíveis tendências advindas do emprego conjunto

dessas tecnologias na área de Defesa.

Apesar de suas bases teóricas e das primeiras provas do conceito terem surgido na década de 1950, a IA vem proporcionado um volume cada vez maior de inovações importantes nos últimos anos, graças ao fácil acesso a grandes quantidades de dados, o que é necessário para que algoritmos "inteligentes" possam convergir e aprender com o ambiente; do aumento exponencial do poder de processamento (Lei de Moore) e da capacidade de armazenamento, essenciais para permitir a execução de algoritmos de IA em tempo real; dos avanços no desenvolvimento dos algoritmos de busca e de técnicas de aprendizagem profunda; da disponibilidade de sensores que coletam grandes quantidades de dados em tempo real; e dos avanços em atuadores, em muitos casos indispensáveis para realizar ações originadas de dispositivos dotados de IA. À medida que as novas tecnologias quânticas se tornarem passíveis de serem embarcadas, a IA poderá ser impulsionada ainda mais e poderá ocorrer um salto extraordinário no desempenho desses dispositivos e sistemas, como veículos autônomos, enxames de drones e em robótica.

Do ponto de vista da indústria de defesa, destacam-se usos de IA em Cibernética, Redes de Sensores sem Fio, Simulação, Detecção de Objetos, Veículos Aéreos Não Tripulados (VANT), Sistemas de Comando e Controle e Sistemas Mecatrônicos. Assim, a seleção, detecção e engajamento de alvos, bem como o uso automatizado de enxames de drones são algumas das possibilidades do emprego da IA na Guerra do Futuro. A IA é uma tecnologia que já existia anteriormente em um formato diferente, tendo sido criada para obter maior eficiência em tarefas específicas e não generativas. Mais recentemente, a inteligência artificial, tendo como principal representante na população em geral o ChatGPT (ou GPT-3, Generative Pre-Trained Transformer), da empresa Open IA, deu indícios da revolução científica, tecnológica e social pela qual passa a área de IA.

O GTP-4 deverá usar 100 trilhões de parâmetros. Muito maior do que os 175 bilhões de parâmetros da versão GPT-3. Alguns cientistas consideram que a nova versão, o GTP-5, poderá se tornar uma Inteligência Artificial Geral (IAG) . Para que isso seja possível, ainda devemos aguardar os próximos resultados. As versões ChatGPT-3.5 e 4 são conhecidas por se degradarem quando usadas extensivamente por vários usuários, fenômeno chamado de desvio comportamental ou "model drift". Superando tais obstáculos, a IA, associada com a capacidade de

processamento e armazenamento das Tecnologias Quânticas, deverá apresentar capacidades muito maiores do que as conhecidas atualmente.

A eletrônica embarcada e os componentes baseados em software estão começando a desempenhar um papel importante em artefatos e vetores aéreos, marítimos e terrestres. O advento das redes cognitivas, da computação em nuvem e dos avanços nas comunicações digitais através de canais sem fio estão aumentando a conectividade. As tecnologias-chave que sustentam estas questões permitem que as Forças Armadas desenvolvam princípios de guerra cibernética, empreguem sistemas complexos de comando e controle e percebam situações de campo de batalha de uma forma intuitiva e com detalhes sem precedentes. A segurança – apoiada por protocolos baseados em tecnologias quânticas – estará na vanguarda da concepção e operação de sistemas de guerra inteligentes e das suas redes de apoio. O progresso é grande para quem dominar as tecnologias críticas, mas representará um grande retrocesso e grandes ameaças para países com baixa capacidade tecnológica acumulada em áreas-chave.

No contexto da 4ª Revolução Industrial, desponta a Guerra Cibernética, cuja vulnerabilidade de segurança aumenta com a dependência da tecnologia, sobretudo com o advento das tecnologias quânticas. A primeira definição formal de Guerra Cibernética é frequentemente atribuída aos pesquisadores John Arquilla e David Ronfeldt, em um relatório publicado em 1993 pelo think tank RAND Corporation. Eles definiram Guerra Cibernética como: "Conduzir e preparar-se para conduzir, operações militares de acordo com princípios relacionados à informação. Isso significa ataques que têm como objetivo desativar, interromper ou destruir sistemas de informação e comunicação adversários, enquanto protege os próprios sistemas." Com a 4ª Revolução Industrial, as infraestruturas críticas se tornam conectadas em rede e ao ciberespaço, tornando os impactos deste tipo de guerra ainda maiores. As Tecnologias Quânticas impulsionarão este impacto.

Entre os meses de junho e outubro de 1999, Jonathan – um adolescente estadunidense de apenas 15 anos de idade – hackeou a NASA e o Pentágono, além de outros alvos menores. Ele se tornou a primeira pessoa no mundo a entrar no sistema do Defense Threat Reduction Agency (DTRA), uma divisão do DoD (Department of Defense) encarregada de analisar possíveis ameaças aos Estados Unidos. A mesma façanha em relação ao Pentágono foi alcançada por outros hackers, como Gary McKinnon, acusado de ter invadido, entre fevereiro de 2001

e março de 2002, os computadores da Nasa, do Pentágono, do Exército (USARMY), da Força Aérea (USAF) e da Marinha (USNAVY) dos Estados Unidos. Promotores estadunidenses acusaram McKinnon de desligar completamente uma rede de mais de 2 mil computadores, por 24 horas. Os ataques de hackers russos têm sido notícia desde as últimas eleições para presidente dos Estados Unidos da América até mais recentemente, durante a Guerra Rússia-Ucrânia.

Em 2016, uma simples foto (Figura 14), compartilhada por Mark Zuckerberg para celebrar os 500 milhões de usuários do Instagram, colocou de volta o assunto dos *hackers*. Na imagem é possível ver que o criador do Facebook cobriu com fita adesiva a *webcam* e o microfone do seu notebook. Definitivamente, ninguém no mundo está livre dos *hackers.*

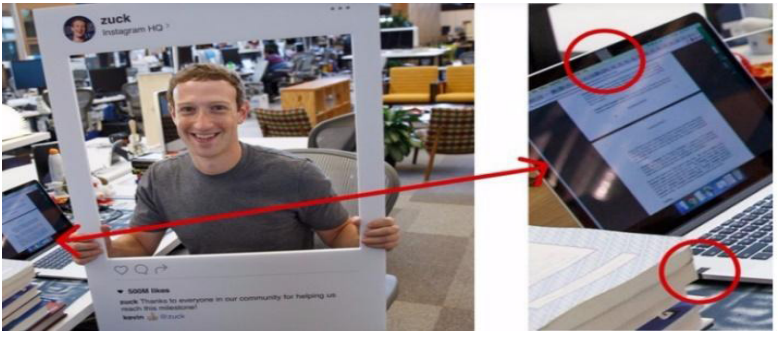



Figura 14: Foto compartilhada por Mark Zuckerberg para celebrar os 500 milhões de usuários do Instagram colocou de volta o assunto dos *hackers*

Em 2018, a China foi acusada de invadir os sistemas da Marinha dos EUA. Segundo informações obtidas pelo jornal The Washington Post a partir de funcionários não identificados das Forças Armadas norte-americanas, hackers chineses teriam invadido os sistemas de uma empresa terceirizada que presta serviços para as Forças Armadas estadunidenses e acessado cerca de 614 GB de dados sigilosos.

Em meados de junho de 2023, a Marinha dos EUA foi novamente invadida por hackers chineses. A Microsoft emitiu um aviso de alerta, assim como o fizeram as agências de inteligência, incluindo a Agência de Segurança Nacional, a Agência de Segurança Cibernética e Infraestrutura e as agências de segurança cibernética de outras quatro nações. Os avisos alertaram empresas corporativas e públicas de que um sofisticado grupo de hackers, apoiado pelo governo chinês, explorou com sucesso uma

vulnerabilidade em um popular pacote de segurança cibernética. Com o Volt Typhoon, esse suposto grupo chinês afetou a infraestrutura cibernética crítica em vários setores. Segundo ela, os hackers chineses tinham como alvo as comunicações e os setores marítimos na ilha de Guam, no Oceano Pacífico, que abriga uma importante base militar dos EUA.

Recentemente, foi noticiado pelo jornal The New York Times que os Estados Unidos trabalham para identificar e eliminar um código de informática malicioso que, segundo a matéria, foi instalado pela China no coração de redes que controlam a infraestrutura crítica do Exército americano, havendo a possibilidade dele ser acionado à distância em caso de conflito armado (como por exemplo, numa guerra entre China e Taiwan) e interromper as redes de eletricidade, água potável e comunicação que abastecem as bases militares americanas, dificultando o emprego dessas tropas. Isso mostra as possíveis consequências desastrosas que uma defesa cibernética ineficiente poderia causar à segurança de qualquer país.

Com as tendências advindas da quarta revolução tecnológica e suas consequências como digitalização e hiperconectividade, inclusive dos sistemas e materiais de emprego militares, a superfície de ataque cibernético irá aumentar ainda mais. Os ciberataques e a espionagem digital se intensificarão e suas consequências se tornarão mais graves.

O estudo da quarta revolução industrial e da guerra cibernética tornou-se central para o desenvolvimento da arte e do pensamento militares. Nesta nova era, a dependência da tecnologia será extremamente grave para um país devido ao aumento das vulnerabilidades cibernéticas. Evidências sugerem que as tecnologias quânticas serão fulcrais no balanço entre maior proteção ou maior vulnerabilidade cibernética, pois os avanços tecnológicos impulsionam tanto inovações para a defesa quanto para violação da segurança dos sistemas de comunicações de dados. Pode-se inferir que um sistema de proteção baseado no emprego de comunicação quântica, computação quântica, criptografia, bem como através do uso de dispositivos (sensores, detectores e atuadores) baseados nestas tecnologias será eficiente. Dessa forma, alcançar a chamada supremacia quântica é um objetivo essencial para um país que almeje assumir um papel relevante no concerto das nações, bem como, promover pelos seus próprios meios a Soberania nacional,.

Analisando-se os diferentes teatros de operações dos últimos conflitos ou crises, como a que ocorre entre China e Taiwan, observaremos fortes sinais de surpreendente avanço tecnológico. Exemplo disso é o

desenvolvimento do drone russo chamado Joker, que pode permanecer adormecido (ou em modo de hibernação) durante semanas.

Projetado para se esconder de contramedidas eletrônicas, o drone poderia ser colocado em preparação para o ataque horas, dias ou semanas antes de seu operador acordá-lo para desencadear a missão. Os avanços não param sugerindo o uso intensivo das Tecnologias Quânticas pelas grandes potências em médio prazo e em um futuro não muito distante, a guerra poderá ser dominada pelo uso das tecnologias quânticas, configurando a denominada Quantum Warfare (Figura 01) ou Guerra Quântica.

As discussões apresentadas na Seção 3, trazem à tona a famosa frase proferida em 1915 pelo Almirante britânico John Fisher. Em plena Primeira Guerra Mundial (1914-1918), ele declarou que a Guerra será ganha pelas invenções. As características dos conflitos atuais e as tendências de evolução no campo científico-tecnológico, sobretudo na área das tecnologias quânticas, sugerem que essa assertiva é clarividente.

Mas apesar dos avanços tecnológicos, a denominada Guerra do Futuro ainda não chegou, pois esses novos conceitos ainda estão sendo incorporados às diferentes forças. As máquinas com IA de última geração deverão ser, em breve, uma realidade. Já há inúmeros estados americanos que estão começando a utilizar robôs da Boston Dynamics no policiamento ostensivo das cidades (dentre elas, Los Angeles, Nova Iorque e São Francisco).

Figura 15: Arma anti-blindagem de ombro, denomiando Javelin, dispara um míssil autoguiado contra o seu alvo.

Em que pese as táticas de emboscada e o fato de a Rússia não estar utilizando seus tanques mais modernos, a atual guerra entre a Ucrânia e a Rússia mostrou que a tecnologia de lançadores de mísseis Javelin (Figura 15) pode representar um risco, em termos de poder de fogo, à frota de veículos

blindados russos. Essa arma anti-blindagem de ombro foi desenvolvida e fabricada para o Marine Corps/US Army pela Lockheed Martin (Flórida) e a Raytheon (Arizona)61, mas ainda não incorpora quaisquer conceitos relacionados à tecnologia quântica, por ainda não serem embarcáveis. Quando isso acontecer, avanços extraordinários poderão ocorrer nas áreas de inteligência artificial, robótica, cibernética, comunicações e sistemas de comando e controle, com inúmeras consequências na capacidade de defesa e poder de combate das forças.

Diante dessa efervescência de inovações tecnológicas, em 2021 se consolidou uma mudança fundamental na política de defesa de muitos países considerados potências militares, caracterizada pelo crescimento do orçamento para a tecnologia digital, inteligência artificial, cibernética e tecnologias quânticas, e pela diminuição das verbas tanto para equipamentos convencionais quanto para o sustento de grandes tropas

## CONSIDERAÇÕES FINAIS

Neste artigo, abordou-se, de maneira geral, a influência das tecnologias derivadas da Segunda Revolução Quântica, sobretudo, nas áreas de Segurança e Defesa nacional. As evidências aqui apresentadas sugerem que a adoção de programa estratégico do Exército Brasileiro nessa área é uma questão de soberania. Os países desenvolvidos ou que desejam adquirir proeminência no concerto das nações investem pesadamente em PD&I para obter variadas aplicações militares em Tecnologias Quânticas. A computação, a comunicação, o sensoreamento e a criptografia quânticas representam a única maneira de se dispor de comunicação segura a prova de hackers, consciência situacional e o desenvolvimento de forma eficiente de capacidades militares centrais para a Guerra do Futuro.

Dada o enorme impacto das tecnologias quânticas na área de cibernética, e dada a forte dependência atual do mundo em relação aos computadores, o presente estudo abordou muitos aspectos relacionados à Guerra Cibernética. Num conflito bélico, financeiro etc., é comum que as infraestruturas críticas sejam atacadas logo no início, para desestabilizar uma nação. Atualmente, todas as infraestruturas críticas dependem de uma rede computacional sofisticada que se torna cada vez mais alvo de agressores. Em todo os casos, vislumbra-se que a melhor estrutura de Segurança e Defesa Cibernética usará as Tecnologias Quânticas.

A possibilidade de se obter informações indevidamente,

dentro de uma rede de comunicação, em tempos extremamente curtos, com o algoritmo de Shor, por exemplo, é preocupante. Assim, o conjunto de tecnologias quânticas aplicáveis à cibernética, junto com a área de dispositivos (sensores, biossensores e detectores) quânticos, são essenciais para que as Forças Armadas possam cumprir suas missões constitucionais. No futuro, a associação destas tecnologias com outras, como IA será determinante em robótica, sistemas autônomos, VANTS, missilística e lastrearão a chamada Guerra Quântica.

Dada esta grande importância estratégica e os objetivos marcadamente diferentes dos três principais atores – o meio acadêmico, as empresas e o governo, notadamente as Forças Armadas – é seguro afirmar que o desenvolvimento e a implementação das Tecnologias Quânticas devam ser gerenciados e liderados pelas Forças Armadas, em particular pelo Exército Brasileiro, focado na área de cibernética. Isso, porque cabe às outras forças cuidar das outras duas grandes áreas estratégicas: a Nuclear e a Aeroespacial, conforme estabelecido na Estratégia Nacional de Defesa.

As Tecnologia Quânticas enfrentam diversos desafios tecnológicos atualmente, tais como: a frequente necessidade de operar em temperaturas extremamente baixas; decoerência; ruído quântico; escalabilidade; materiais adequados; e custos ainda elevados. Apesar desse fato poder ser visto como um problema, tais desafios também representam uma oportunidade, pois isso significa que a tecnologia ainda não está pronta e existe espaço para um desenvolvimento nacional. É importante destacar que investir em tal tecnologia implica em concorrer com outras políticas públicas brasileiras.

No entanto, frente ao tamanho esforço global, em termos de investimentos em Tecnologias Quânticas, o Brasil e, particularmente, as suas Forças Armadas não pode ficar indiferente. Os investimentos mundiais indicam basicamente uma coisa: quem não dominar as Tecnologias Quânticas pagará um alto preço estratégico em Segurança e Defesa Nacional, além de crescimento e desenvolvimento econômico e tecnológico. Integrado ao Programa de Defesa Cibernética na Defesa Nacional (PDCDN), o Exército Brasileiro desenvolve o seu Programa Estratégico de Defesa Cibernética, que tem por finalidade coordenar e integrar os projetos e processos do Setor Cibernético, bem como desenvolver as capacidades cibernéticas das Forças Armadas, por meio de integração, coordenação e atuação conjuntas. O PDCDN tem buscado, desde 2023, fornecer recursos para o desenvolvimento de Tecnologias

Quânticas nacionais.

Dessa maneira, o Brasil não pode ignorar a importância estratégica do desenvolvimento nacional destas tecnologias e simplesmente optar pela sua importação, tanto de produtos (sistemas de comunicação, internet e criptografia quântica e sensores quânticos) quanto de serviços (computadores quânticos). É inconcebível que dados estratégicos e confidenciais sobre as operações das nossas Forças Armadas devam ser analisados por computadores quânticos estrangeiros como o Sycamore (da Google) ou o Osprey (da IBM) devido à inexistência de equipamento nacional.

Não há muitas dúvidas quanto à necessidade premente e essencial do desenvolvimento local das Tecnologias Quânticas de aplicação em segurança e defesa nacional. Entretanto, em razão dos enormes desafios científicos e tecnológicos e da dualidade das tecnologias a serem desenvolvidas, com forte impacto em todas as Expressões do Poder Nacional, para atingir o resultado almejado nessas tecnologias disruptivas, há de se promover esforço nacional na destinação dos recursos financeiros necessários para se atingir autonomia em área estratégica para o país.

Os políticos, estrategas e decisores políticos que defendem os valores da liberdade, democracia e soberania, reconhecem que a preservação delas depende de uma vigilância constante, ou seja, de um sistema de Defesa Nacional que possa repelir ameaças atuais e futuras. A manutenção de um sistema de vigilância permanente é o preço a pagar por algo tão precioso. Como resumiu Rui Barbosa: "Um exército pode passar 100 anos sem uso, mas nem um minuto sem preparação". Esta maneira de pensar dá as bases para o sentido de autopreservação e coesão nacional que orientará os investimentos na área de Defesa.

Embora diversas áreas do Poder Nacional possam ser mobilizadas para atuar pela soberania de uma nação, o Estado deve coordenar, coletar e integrar Sistemas e Materiais de Emprego Militar (SMEM) para fortalecer as capacidades do seu sistema militar. Esta robustez requer necessariamente autonomia tecnológica. Em termos de tecnologia de Defesa, nada é mais moderno e fundamental do que as Tecnologias Quânticas. Elas têm potencial para afetar quase todos os aspectos do ambiente militar, desde aqueles que possuem pouco conteúdo científico-tecnológico até os mais complexos.

Apoiando-se em inovações tecnológicas autóctones de alto valor agregado, essenciais à sobrevivência do Estado e à concretização

dos chamados Objetivos Nacionais Permanentes, de forma geral o setor da Defesa é o motor propulsor do desenvolvimento científico e tecnológico e eleva o mercado multimilionário das empresas que compõem a Base Industrial de Defesa (BID). Indispensáveis para o incentivo a projetos inovadores, especialmente aqueles diretamente relacionados com a Defesa Nacional, os mecanismos adoptados pelo Estado para apoiar a BID dispõem de poucos estudos que caracterizem os fatores relacionados com a sua origem ou desenvolvimento. No entanto, sabe-se que os principais intervenientes neste domínio, como os Estados Unidos, a União Europeia, a Grã-Bretanha e a Rússia, venceram as grandes guerras do século XX graças a uma próspera indústria de Defesa e de um permanente e importante apoio financeiro nas áreas de educação, ciência e tecnologia, demonstrando assim a importância deste trio para os seus povos na resolução de conflitos.

É essencial definir os objetivos de curto, médio e longo prazos; coordenar e avaliar os avanços na comunidade acadêmica e das ICTs, bem como contribuir com pesquisas no setor, por meio de suas ICTs em parceria com a comunidade acadêmica, empresas e outros setores governamentais. Isto inclui não só parcerias com grandes empresas tecnológicas, mas sobretudo com startups, universidades e institutos de pesquisa, pois são essenciais para a inovação neste tipo de tecnologia. Porém, como o conteúdo é sensível e de vital importância para a Segurança e Defesa do país, esse processo deve envolver a participação significativa das Forças Armadas, especialmente do Exército Brasileiro, em particular, das suas organizações de ensino, pesquisa, desenvolvimento e inovação. Uma iniciativa nesse sentido foi recentemente aprovada pela CAPES (PRO-DEFESA-V) e, com coordenação do IME, que envolve aproximadamente 100 pesquisadores de 43 instituições civis e militares e 23 programas de pós-graduação.

Para que às Forças Armadas possam realmente usufruir dos benefícios destas novas Tecnologias Quânticas é fundamental que elas participem ativamente nesta área e forneçam tanto as bases do desenvolvimento quanto a adoção de aplicações dos possíveis usos na área militar. Um forte envolvimento no ecossistema quântico melhorará a compreensão das Forças Armadas sobre os riscos potenciais associados com estas novas tecnologias, especialmente na área de cibernética. Tal risco fica evidente quando se leva em conta a importância do desenvolvimento da internet quântica, baseada na comunicação quântica.

É difícil imaginar uma frase mais atual e relevante do que aquela proferida em 1915 pelo Almirante britânico John Fisher quando ele declarou que "a Guerra será ganha pelas invenções". Analisando, à luz do texto anterior, o dito pelo 3º Visconde Palmerston – "Não temos aliados eternos, nem inimigos perpétuos. Nossos interesses são eternos e perpétuos" – fica cristalina a necessidade premente de desenvolvermos as nossas próprias Tecnologias Quânticas relacionadas com Segurança e Defesa. As tecnologias quânticas são essenciais para o crescimento econômico, o desenvolvimento e a soberania de um país. Ao se perder a oportunidade de explorar adequadamente algumas revoluções tecnológicas, como a microeletrônica e a nanotecnologia, o Brasil sofreu incalculáveis e irreversíveis prejuízos. Os países que não tenham domínio das Tecnologias Quânticas poderão vir a sofrer uma verdadeira catástrofe, em termos socioeconômicos e de soberania.

Em 2025, o mundo celebra o Ano Internacional da Ciência e Tecnologia Quântica, uma iniciativa da ONU. O Brasil tem todas as condições para acelerar o passo e usufruir dos recursos políticos e financeiros que devem advir dessa comemoração. No Brasil, o Ministério da Ciência, Tecnologia e Inovação (MCTI) também criou um grupo de trabalho para criar propostas na área de Quântica. Espera-se que essa iniciativa dê início à criação da Estratégia Brasileira de Quântica, nos mesmos moldes da EBIA (Estratégia Brasileira de Inteligência Artificial). Ou seja, a esfera política nacional já vem se convencendo da importância do assunto.

Ou desenvolvemos internamente as Tecnologias Quânticas necessárias ou os nossos setores de Segurança e Defesa nacional tornar-se-ão obsoletos em pouco tempo, com consequências desastrosas e irreversíveis. Ninguém fará o dever de casa por nós.

# Quantum Technologies: a matter of national sovereignty

**RESUMO**

The foundations of quantum physics (or mechanics) were presented by German scientist Max Planck in 1900. With revolutionary scientific content, these foundations established new paradigms that supported the so-called First Quantum Revolution, from which products such as lasers, GPS and semiconductor chips, which are essential today, were derived. In 1950, Chien Shiung Wu and Irving Shaknov conducted what is now known as the WS experiment, which became the key to the emerging manifestation of the second quantum revolution, which includes new technologies grouped into four broad areas: quantum devices (sensors, biosensors, detectors, and actuators); quantum communication and teleportation, and two-dimensional materials; quantum computing, cryptography, and the quantum internet; and technologies derived from quantum materials of application, for example, in the area of energy. This article aims to search for evidence that the field of Quantum Technologies is essential not only for National Security and Defense, but also for shaping the geopolitical landscape. They suggest that, together, Quantum Technologies, Artificial Intelligence (AI) and Cybernetics will promote a great technological revolution of humanity, and particularly in military affairs. Thus, the article presents arguments for these areas of knowledge and technological development to be considered strategic and priority for the country, in view of the centrality of these technologies in economic growth, social development, security, defense and sovereignty of a nation in the context of the 4th Industrial Revolution and the Knowledge Age.

**Keywords**: quantum technologies; cyber defense; national sovereignty.

## REFERÊNCIAS

ADVANTAGE: The most connected and powerful quantum computer built for business. **D-Wave Systems**. Disponível em: https://www.dwavesys.com/solutions-and-products/systems/. Acesso em: jun. 2024.

ALVAREZ, Raúl. Jonathan James, el joven que con sólo 15 años hackeó y puso de cabeza a la NASA y al Pentágono. **Xataka**, 18 fev. 2020. Disponível em: https://www.xataka.com/historia-tecnologica/joven-que-solo-15-anos-hackeo-puso-c abeza-a-nasa-al-pentagono. Acesso em: jun. 2024.

ARAÚJO-MOREIRA, Fernando M. et al. Tecnologias quânticas: a inovação disruptiva como diferencial estratégico para a Defesa Nacional. **Seven Editora**, [S. l.], 2023. Disponível em: https://sevenpublicacoes.com.br/editora/article/view/1561. Acesso em: jun. 2024. DOI: 10.56238/tecavanaborda-042.

ARAUJO-MOREIRA, F. M.; Supremacia quântica e Defesa nacional: a nova realidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 245–247, 2023. ISBN 978-65-87080-44-4.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming!. **RAND Corporation**, 1993. Disponível em: https://www.rand.org/pubs/reprints/RP223.html. Acesso em: nov. 2024.

BARONE, A.; PATERNÒ, G. **Physics and applications of the josephson effect.** New York: John Wiley & Sons, 1982. DOI:10.1002/352760278X.

BARZANJEH, S. et al. Microwave quantum illumination using a digital receiver. **Science Advances**, v. 6, n. 19, p. 1-9, 8 mai. 2020. DOI:10.1126/sciadv.abb0451.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. **International Conference on Computers, Systems & Signal Processing**, Bangalore, vol. 1, p. 175–179, 1984. Disponível em: https://www.karlin.mff.cuni.cz/~holub/soubory/BB84original.pdf. Acesso em: jun. 2024.

BERENDSEN, René G. **The Weaponization of Quantum Mechanics: Quantum Technology in Future Warfare**. 2019. 60f. School of Advanced Military Studies, US Army Command and General Staff College. Dissertação de Mestrado, mai. 2019. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1083173.pdf. Acesso em: jun. 2024.

BOTHNER, Daniel; RODRIGUES, Ines C.; FRANSE, Jasper; STEELE, Gary. TN2953-P The Josephson junction: Quantum tunnelling and interference in an electrical circuit. **NS Web**. Disponível em: https://nsweb.tn.tudelft.nl/~gsteele/SQUID_practicum/TN2513-P%20SQUID%20Prac ticum%20 Manual.html. Acesso em: jun. 2024.

BOUTIN, Chad. NIST releases first 3 finalized post-quantum encryption standards. **NIST**, 13 ago. 2024. Disponível em: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-q uantum-encryption-standards. Acesso em: outubro de 2024.

BRANDOM, Russell. Google's quantum computer just flunked its first big test. **The Verge**, 19 jun. 2014. Disponível em: https://www.theverge.com/2014/6/19/5824336/google-s-quantum-computer-just-flunk ed-its-first-big-test. Acesso em: jun. de 2024.

BRASIL. Ministério da Defesa. **IME se destaca em Programa de Ensino e Pesquisa em Defesa**. Exército Brasileiro, 26 ago. 2024. Disponível em: https://www.eb.mil.br/web/noticias/w/ime-se-destaca-no-pro-defesa-v-principal-edital -da-capes-destinado-a-area-da-defesa. Acesso em: junho de 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 8.194, de 19 de maio de 2024**. Institui grupo de trabalho com o objetivo de debater e propor as bases e diretrizes para o estabelecimento de uma Iniciativa Brasileira para Tecnologias Quânticas. Diário Oficial da União: seção 1, Brasília, DF, n. 97, p. 87, 21 mai. 2024. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mcti-n-8.194-de-19-de-maio-de-2024-56075 5075. Acesso em: out. 2024.

BRAZIL data centers locations. **Datacenters.com**, 2024. Disponível em

https://www.datacenters.com/locations/brazil. Acesso em: nov. 2024.

CHEN, Stephen. The end of stealth? New chinese radar capable of detecting 'invisible' targets 100km away. **South China Morning Post**, Beijing, 21 set. 2016. Disponível em: https://www.scmp.com/news/china/article/2021235/end-stealth-new-chinese-radar-capable-detecting-invisible-targets-100km. Acesso em: jun. 2024.

CLARKE, John. SQUIDs. **Scientific American**, v. 271, n. 2, p. 46–53, ago. 1994. DOI: 10.1038/scientificamerican0894-46.

CORREIA, Flávia. China quebra recorde de distância de comunicação direta com segurança quântica. **Olhar Digital**, 20 abr. 2022. Disponível em: https://olhardigital.com.br/2022/04/20/ciencia-e-espaco/china-quebra-recorde-de-dist ancia-de-comunicacao-direta-com-seguranca-quantica/. Acesso em: jun. 2024.

COWING, Keith. The world's first integrated quantum communication network. **SpaceRef**, 7 jan. 2021. Disponível em: https://spaceref.com/newspace-and-tech/the-worlds-first-integrated-quantum-commu nication-network/. Acesso em: jun. 2024.

CRAWFORD, Scott E. et al. Quantum sensing for energy applications: review and perspective. **Advanced Quantum Technologies**, v. 4, n. 8, ago. 2021. DOI: 10.1002/qute.202100049.

DÓLAR cotado a R$ 6,00 em novembro de 2024. **Banco Central do Brasil**, 2024. Disponível em: https://www.bcb.gov.br. Acesso em: nov. 2024

EMMERT-STREIB, Frank. Is ChatGPT the way toward artificial general intelligence. **Discover Artificial Intelligence**, v. 4, n. 32, 2024. DOI: 10.1007/s44163-024-00126-3.

FACEBOOK: esta simple foto ha revelado que Mark Zuckerberg es muy paranoico. **RPP Noticias**, 21 jun. 2016. Disponível em: https://rpp.pe/virales/facebook/facebook-esta-simple-foto-ha-revelado-que-mark-zuc kerberg-es-muy-paranoico-noticia-973116. Acesso em: jun. 2024.

FRANÇA JUNIOR, J. A.; GALDINO, J. F. Gestão de sistemas de material de emprego militar: o papel dos níveis de prontidão tecnológica. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 13, n. 47, p. 155-176, 23 jul. 2019.

FANCHINI, Felipe. Brasil precisa acelerar o passo para se beneficiar da segunda onda de inovação quântica. **The Conversation**, 23 jul. 2024. Disponível em: https://theconversation.com/brasil-precisa-acelerar-o-passo-para-se-beneficiar-da-se gunda-onda-de-inovacao-quantica-226799. Acesso em: out. 2024.

GALANTE, Alexandre. Radar quântico – fim do stealth?. **Poder Aéreo**, 7 mai. 2018. Disponível em: https://www.aereo.jor.br/2018/05/07/radar-quantico-fim-do-stealth/. Acesso em: jun. 2024.

GALDINO, J. F.; SCHONS, D. L. Maquiavel e a Importância do Poder Militar Nacional. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 56, p. 353-368, 2022.

GALDINO, J. F. Base industrial de Defesa: ambivalência e sustentabilidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 397–400, 2023. ISBN 978-65-87080-44-4.

GALDINO, J. F. Lições sobre os desafios enfrentados pela indústria de Defesa do Brasil no período de 1950 a 1990. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 393–396, 2023. ISBN 978-65-87080-44-4.

GARDNER, Frank. As armas de guerra do futuro que já são realidade. **BBC News Brasil**, 7 jan. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-59904239. Acesso em: jun. 2024.

GIDNEY, Craig; EKERA, Martin. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **Quantum**, v. 5, p. 433, 2021. Disponível em: https://quantum-journal.org/papers/q-2021-04-15-433/. Acesso em: out. 2024. DOI: 10.22331/q-2021-04-15-433.

GIRARDI, Romullo; FRANÇA JUNIOR, J. A.; GALDINO, J. F. Criticidade tecnológica na área de defesa em países em desenvolvimento: conceitos e critérios. **Revista de Gestão e Secretariado**, v. 15, n. 4, p. 3618, 2024. ISSN: 2178-9010.

GIRARDI, R.; FRANÇA JUNIOR, J. A.; FERREIRA GALDINO, J. A customização de processos de avaliação de prontidão tecnológica baseados na escala TRL: desenvolvimento de uma metodologia para o Exército Brasileiro. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 57, p. 491-527, 28 set. 2022.

HACKERS patrocinados pelo estado chinês se infiltraram na infraestrutura naval dos EUA, diz secretário da Marinha. **Poder Naval**, 26 mai. 2023. Disponível em: https://www.naval.com.br/blog/2023/05/26/hackers-patrocinados-pelo-estado-chines se-infiltraram-na-infraestrutura-naval-dos-eua-diz-secretario-da-marinha/. Acesso em: jun. 2024.

HACKER que invadiu Pentágono perde novo recurso para evitar extradição. **Globo.com**, 31 jul. 2009. Disponível em: https://g1.globo.com/Noticias/Tecnologia/0,,MUL1249916-6174,00.html. Acesso em: jun. 2024.

IYER, Kaanita. Autoridades dos EUA procuram software chinês invasor que pode afetar operações militares. **CNN Brasil**, 30 jul. 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/autoridades-dos-eua-procuram-software chines-invasor-que-pode-afetar-operacoes-militares/. Acesso em: jun. 2024.

JAVELIN Weapon System. **Lockheed Martin**. Disponível em: https://www.lockheedmartin.com/en-us/products/javelin.html. Acesso em: jun. 2024.

KRATIUK, Anton. Russian stealth drone S-70 uses high-tech components of Western manufacture: ukrainian experts present evidence. **Gagadget**.com, 8 nov. 2024. Disponível em: https://gagadget.com/en/528077-russian-stealth-drone-s-70-uses-high-tech-components-of-western-manufacture-ukrainian-experts-present-evidence/. Acesso em: nov. 2024.

KRELINA, M. Quantum technology for military applications. **EPJ Quantum** Technology. v. 8, n. 24, 2021. DOI: 10.1140/epjqt/s40507-021-00113-y.

LANÇADA a pedra fundamental da Rede Rio Quântica. **Portal Gov.br**, 11 mai. 2023. Disponível em: https://www.gov.br/cbpf/pt-br/assuntos/noticias/lancada-a-pedra-fundamental-da-red e-rio-quantica. Acesso em: jun. 2024.

LEFFER, Lauren. Yes, AI models can get worse over time. **Scientific American**, 2 ago. 2023. Disponível em: https://www.scientificamerican.com/article/yes-ai-models-can-get-worse-over-time/. Acesso em: nov. 2024.

MALIK, Mehul; MAGAÑA-LOAIZA Omar S.; BOYD, Robert W. Quantum-secured imaging. **Applied Physics Letters**, v. 101, n. 24, 10 dez. 2012. DOI: 10.1063/1.4770298.

MCFADDEN, Christopher. Russia has developed a new kind of 'sleeper' drone called the 'Joker'. **Interesting Engineering**, 26 jul. 2023. Disponível em: https://interestingengineering.com/innovation/russia-sleeper-drone-the-joker. Acesso em: jun. 2024.

MONTEIRO, Luís N. C. S. Guerras de 4a geração. **Revista Militar**, Lisboa, v. 2591, p. 1001-1014, dez. 2017. Disponível em: https://www.revistamilitar.pt/artigo/1288. Acesso em: jun. 2024.

MÜLLER, Léo. China é acusada de hackear marinha dos EUA e roubar projeto bélico. **Tecmundo**, 8 jun. 2016. Disponível em: https://www.tecmundo.com.br/seguranca/131129-china-acusada-hackear-marinha-eua-roubar-projeto-belico.htm. Acesso em: jun. 2024.

MURRAY, W.; KNOX, M. A. **Evolução da arte da guerra**: das guerras medievais aos ataques relâmpagos 1300 - 2050. Rio de Janeiro: BIBLIEx, 2022, 292 p.

NEWDICK, Thomas. Russia's S-70 hunter drone was armed when shot down by friendly fighter over Ukraine. **The Warzone**, 7 out. 2024.

Disponível em: https://www.twz.com/air/russias-s-70-hunter-drone-was-armed-when-shot-down-by-fr iendly-fighter-over-ukraine. Acesso em: nov. 2024.

O QUE é comunicação quântica?. **Mit Technology Review**, [s. l.], 1 set. 2020. Disponível em: https://mittechreview.com.br/o-que-e-comunicacao-quantica/. Acesso em: jun. 2024.

PADILHA, Luiz. YlC-8E: o primeiro radar anti-stealth do mundo. **Defesa Aérea & Naval**, 8 out. 2021. Disponível em: https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/ylc-8e-o-primeiro-radar-a nti-stealth-do-mundo. Acesso em: jun. de 2024.

PADILLA CRUZ, A. M. **Quantum Technology and its influence in Global Power Politics**. 2020. 101f. Dissertação (Mestrado Internacional em Segurança, Inteligência e Estudos Estratégicos) - Charles University. 16 set. 2020. Disponível em: https://dspace.cuni.cz/bitstream/handle/20.500.11956/177264/120370453.pdf?seque nce=1&isAllowed=y. Acesso em: nov. 2024.

PANASOVSKIY, Maksim. Chinas Tarnkappenbomber H-20 wird Atomwaffen tragen und konventionelle Einsätze fliegen. **Gagadget.com**, [s. l.], 27 out. 2023. Disponível em: https://gagadget.com/de/342722-chinas-tarnkappenbomber-h-20-wird-atomwaffen-tr agen-und-konventionelle-einsatze-fliegen/. Acesso em: jun. 2024.

PAYÃO, Felipe. China cria radar quântico que revela qualquer caça stealth no mundo. **Tecmundo**, 26 set. 2016. Disponível em: https://www.tecmundo.com.br/tecmundo-auto/109884-china-cria-radar-quantico-revela-qualquer-caca-stealth-mundo.htm. Acesso em: jun. 2024.

PICCHI, Aimee. Los Angeles approves $278,000 robot police dog despite "grave concerns". **CBS News**, 24 mai. 2023. Disponível em: https://www.cbsnews.com/news/los-angeles-robot-police-dog-approved-despite-grave-concerns/. Acesso em: jun. 2024.

PRESKILL, John. Quantum computing 40 years later. **Quantum Physics**, 19 jun. 2021. DOI: 10.48550/arXiv.2106.10522.

POST-QUANTUM Cryptography. **NIST**, 2017. Disponível em: https://www.nist.gov/pqcrypto. Acesso em: jun. 2024.

QUANTUM Manifesto - A new era of technology. **TNO**, 2016. Disponível em: https://www.tno.nl/media/7638/quantum_manifesto.pdf. Acesso em: jun. 2024.

QUANTUM RESOURCES AND CAREERS. Quantum Initiatives Worldwide 2023. **QURECA**. Disponível em: https://www.qureca.com/quantum-initiatives-worldwide/. Acesso em: out. 2024.

RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard M. A method for obtaining digital signatures and public key signatures. **ACM Digital Library**, vol. 21, n. 2, 1 fev. 1978. DOI: https://doi.org/10.1145/359340.359342.

RUSSIAN combat UAV Sukhoi S-70 Okhotnik made first flight. **Army Recognition Group**, 5 ago. 2019. Disponível em: https://www.armyrecognition.com/news/army-news/2019/russian-combat-uav-sukhoi s-70-okhotnik-made-first-flight. Acesso em: nov. de 2024.

SHOR, Peter W. Algorithms for quantum computation: discrete logarithms and factoring. **35th Annual Symposium on Foundations of Computer Science**, Santa Fé, p. 124-134, 1994. DOI: 10.1109/SFCS.1994.365700.

TECHNOLOGY Readiness Level of Quantum Computing Technology (QTRL). **Jülich Forschungszentrum**, 19 jul. 2022. Disponível em: https://www.fz-juelich.de/en/ias/jsc/about-us/structure/research-groups/qip/technolog y-readiness-level-of-quantum-computing-technology-qtrl. Acesso em: jun. 2024.

TREATY of Adrianople - Charges Against Viscount Palmerston. **UK Parliament [Hansard, House of Commons Debate]**, vol. 97, p. 66-123, 01 mar. 1848. Disponível em: https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople -charges-against. Acesso em: nov. de 2024.

VAN AMERONGEN, Michiel. Quantum technologies in defence &

security. **NATO Review**, 3 jun. 2021. Disponível em: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html. Acesso em: jun. 2024.

WU, Chien Shiung; SHAKNOV, Irving. The angular correlation of scattered annihilation radiation. **Physical Review**, v. 77, n. 1, 1950. DOI: 10.1103/PhysRev.77.136.

XUANZUN, Liu. China's in-development H-20 bomber worth the excitement: PLA Air Force deputy commander. **Global Times**, 11 mar. 2024. Disponível em: https://www.globaltimes.cn/page/202403/1308604.shtml. Acesso em: nov. 2024.

ZHANG, H.; SUN, Z.; QI, R. et al. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. **Light Science & Applications**, v. 11, n. 83, 2022. DOI: 10.1038/s41377-022-00769-w.

*** Recebido em 30 de junho de 2024, e aprovado para publicação em 13 de maio de 2025.**