Tecnologias Quânticas: prospecto atual, desafios e oportunidades para as Forças Armadas Brasileiras

André J. C. Chaves[1], Denys Derlian C. Brito[1], Rodrigo P. Ferreira[1] e Victor G. M. Duarte[1]
[1]Instituto Tecnológico de Aeronáutica, São José dos Campos/ São Paulo — Brasil

***Abstract*— As tecnologias quânticas resultam do uso das leis da física moderna em dispositivos cada vez mais sofisticados; prometendo enormes avanços na computação, comunicação e sensores, tanto em uso civil quanto militar. Como consequência do avanço tecnológico que miniaturizou a instrumentação para escalas atômicas, estamos presenciando a manipulação em escala nanométrica de sistemas físicos utilizando propriedades intrínsecas de sistemas quânticos, como o emaranhamento. Sensores quânticos conseguem ir além dos limites clássicos de detecção. Comunicação quântica oferece vantagem sobre segurança em relação à comunicação clássica. Computação quântica permite a solução de problemas considerados impossíveis de serem resolvidos por computadores clássicos. Essas tecnologias aparecem como resultado do avanço da ciência e engenharia, permitindo a manipulação de sistemas em nível atômico. Nesse artigo apresentamos brevemente conceitos fundamentais de mecânica quântica, os principais exemplos de tecnologias quânticas em sensores, comunicação e comunicação. Mostramos as aplicações militares e concluímos apresentando os desafios e oportunidades.**

***Keywords*— Cibersegurança, Tecnologias Quânticas, Computação Quântica.**

I. Introdução

A mecânica quântica foi desenvolvida no começo do século XX visando explicar fenômenos atômicos que contradiziam a física clássica. Ao longo desse século, a aplicação da teoria quântica permitiu inúmeros avanços na ciência e tecnologia, como no desenvolvimento de semicondutores, transistores, lasers. Esses avanços também dependeram do melhor entendimento do que é luz, e, portanto, da formulação da eletrodinâmica quântica. Essa primeira revolução quântica se baseou no carácter ondulatório da mecânica quântica, como, por exemplo, no entendimento da teoria de semicondutores. O avanço da nanotecnologia e instrumentação permitiu a manipulação de sistemas com precisão crescente e explorar mais fenômenos quânticos em escala nanoscópica. Isso deu origem a uma segunda revolução quântica [1], que inclui utilizar como ferramenta o desafiador conceito de medição na mecânica quântica, e propriedades como superposição e emaranhamento.

Diversos instrumentos permitiram a concretização das tecnologias quânticas, como microscópios por corrente de tunelamento, lasers, pinças ópticas, supercondutores, refrigeradores criogênicos, e muitos outros. Do lado teórico, a criação da teoria da informação quântica, unindo a teoria da informação com a mecânica quântica, permitiu avanços na compreensão dos fenômenos quânticos oriundos do emaranhamento. Já na década de 80, Richard Feynmann vislumbrou que a física sistemas quânticos precisariam ser simulados por um computador quântico [2]. Essa década também foi marcada por avanços na óptica quântica, como pode ser visto por cinco premiações Nobel, começando por experimentos com átomos ultrafrios [3], condensação de Bose-Einstein [4], coerência quântica [5] e espectroscopia a laser [6], medição e manipulação de sistemas quânticos, e estudo experimental de emaranhamento de fótons [7], [8]. Esses avanços permitiram o conceito de Máquinas de Schrödinger [9], que dependem da nossa capacidade de manipular a matéria em nível atômico. Há muitas formas de se dividir as tecnologias quânticas, mas seguindo o Quantum Manifesto da União Europeia, temos sensores quânticos, simulação quântica, comunicação quântica e computação quântica [10]. Ao mesmo tempo que o avanço das tecnologias quânticas apresenta oportunidades, também traz riscos e desafios. O real impacto que todas essas tecnologias terão no futuro é difícil de predizer, porém, nesse artigo falamos brevemente a situação atual e perspectivas para o futuro, com um enfoque na área de defesa.

André J. C. Chaves, andrej6@gmail.com; Denys Derlian C. Brito, denysderlian@hotmail.com; Rodrigo P. Ferreira, rodrigo.ferreira@ga.ita.br; Victor G. M. Duarte, vgmduarte@gmail.com;

A. Metodologia

A metodologia adotada incluiu pesquisas e revisões bibliográficas em bases de dados acadêmicas e periódicos especializados em tecnologias quânticas. Além disso, foram analisados documentos oficiais de órgãos governamentais e instituições de pesquisa para obter informações sobre o panorama mundial e sobre as aplicações das tecnologias no futuro. A análise qualitativa das informações coletadas permitiu identificar tendências, desenvolvimentos tecnológicos e casos de aplicação prática de tecnologias quânticas, proporcionando um prospecto atual, principais desafios e oportunidades para aplicações militares.

Na seção (II), apresentamos os conceitos fundamentais de mecânica quântica que serão utilizados nas outras seções do artigo. Na seção (III) apresentamos as áreas de sensores, comunicação e computação quânticas. Na seção (IV apresentamos as principais tecnologias militares e na seção (V) concluímos discutindo as oportunidades e desafios para as forças armadas brasileiras.

II. Conceitos Fundamentais

Sistemas quânticos são governados pela equação de Schrödinger, que, dado um estado inicial, determina a sua evolução temporal conforme a Hamiltoniana do sistema [11]. Os estados acessíveis a um sistema pertencem a um espaço vetorial, chamado de espaço de Hilbert, que possui um produto interno. Observáveis são operadores lineares hermitianos do espaço de Hilbert, cujos autovalores são os resultados possíveis de uma medição, com a probabilidade de uma

certa medição dada pela Regra de Born, correspondente ao quadrado do produto interno entre o estado e o vetor de estado se torna o autovetor do operador correspondente ao estado medido [11]. Essa probabilidade é intrínseca à mecânica quântica e não está relacionada com incertezas vindas do aparato experimental. Essa propriedade é utilizada em diversas tecnologias quânticas, como perceberemos na seção III.

As tecnologias quânticas se baseiam em propriedades dos sistemas quânticos, como quantização, superposição e emaranhamento. A quantização, presente já na descrição do átomo de hidrogênio, acontece quando uma partícula quântica está confinada por um potencial e resulta em um conjunto discreto de energias. A geometria do potencial confinante pode ser projetada, determinando os níveis de energia. Esse efeito é explorado em pontos e poços quânticos, que possuem aplicação desde tela de TVs quanto em sensores de radiação infravermelha para uso militar.

A superposição, analogamente ao que acontece para ondas clássicas, como eletromagnéticas ou acústicas, se refere a soma de dois estados distintos. Utilizando a notação de Bra-Ket, a superposição se refere à:

$$|\psi\rangle = \alpha|u\rangle + \beta|v\rangle, \tag{1}$$

com $\alpha, \beta \in \mathbb{C}$ tal que $|\alpha|^2 + |\beta|^2 = 1$. A superposição na mecânica quântica é um resultado da escolha de base. A superposição é utilizada tanto na computação quântica, pois o qubit é escrito como a superposição de dois estados, correspondentes ao 0 lógico e 1 lógico, quanto na comunicação quântica, como, por exemplo, no protocolo BB84.

O emaranhamento é o principal recurso da teoria da informação quântica. É uma propriedade intrínseca de sistemas quânticos, que correlaciona medições de observáveis. Exemplifiquemos com o estado máximo de emaranhamento de duas partículas idênticas. Usando $|a, b\rangle$ para simbolizar que uma partícula 1 está no estado $|a\rangle$ e a partícula 2 no estado $|b\rangle$, um dos estados de máximo emaranhamento é:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|a, b\rangle + \frac{1}{\sqrt{2}}|b, a\rangle, \tag{2}$$

pois, caso a partícula 1 seja medida no estado a, podemos ter certeza que a partícula 2 será medida no estado b. O mesmo não acontece no estado produto:

$$|\psi_{\text{prod}}\rangle = \frac{1}{\sqrt{4}}|a, a\rangle + \frac{1}{\sqrt{4}}|a, b\rangle + \frac{1}{\sqrt{4}}|b, a\rangle + \frac{1}{\sqrt{4}}|b, b\rangle. \tag{3}$$

Como consequência do emaranhamento quântico, Bell propôs desigualdades para valores esperados que, caso violadas, confirmariam as predições da mecânica quântica [12], como já realizado experimentalmente [7].

III. Tecnologias Quânticas

Nessa seção discutiremos três dos principais eixos das tecnologias quânticas: sensores, comunicação e computação. Essa lista não é extensiva, que pode incluir itens como relógios atômicos e simulação quântica [10]. Em comum, todas essas tecnologias utilizam conceitos da teoria da informação quântica.

A. Sensores Quânticos

Há três definições de sensoriamento quântico [13]: i) objetos quânticos usados para medir propriedades físicas; ii) sistemas que usam coerência quântica; ou iii) sensores que utilizam do emaranhamento quântico. Temos como exemplos em i) e ii), átomos neutros, armadilha de íons, átomos de Rydberg, relógios atômicos, centro de vacância do nitrogênio em diamante, sensores baseados em spin, ressonância nuclear magnética e circuitos supercondutores. Vamos nessa seção comentar algumas propriedades e exemplos de sensores quânticos. A maioria dos sensores quânticos se baseiam em sistemas de dois níveis. São controlados por um sinal externo dependente do tempo, que de forma geral é realizada por radiação eletromagnética no visível ou infravermelho, ou por campos elétricos, ou magnéticos [13].

Considerando que o sensor quântico atua pela interação de um qubit com o sinal externo, o fator de acoplamento é chamado de parâmetro de transdução, relacionado diretamente com a sensividade, que é proporcional a resposta do sensor a um sinal desejado e inversamente proporcional a resposta em relação ao ruído [13]. Dependendo do objeto a ser medido, diferentes protocolos de medição podem ser usados. O uso de qubits emaranhados para se fazer a medição pode aumentar a sensividade. Sensores quânticos são considerados a tecnologia quântica mais madura para aplicação militar [14]. Nas subseções IV-B e IV-D comentaremos os usos militares de radares quânticos e magnetômetros SQUID.

B. Comunicação Quântica

Um conceito de comunicação quântica à prova de hackers, fundamentado no "teorema de não clonagem" formulado em 1982, a qual permite a transmissão segura de dados sem o risco de espionagem. Tal tecnologia promete uma comunicação mais segura e abrangente, oferecendo soluções práticas para proteger informações sensíveis em diversos domínios [15].

A comunicação quântica engloba diversas tecnologias e aplicações, desde experimentos de laboratório até tecnologias comercializáveis, sendo as principais a Distribuição de Chaves Quânticas (QKD) e os Geradores de Números Aleatórios Quânticos (QRNG) [16]. A base da comunicação quântica é o emaranhamento quântico, onde dois usuários compartilham pares de partículas com propriedades interligadas. Essa propriedade é comparada, sendo usada para criar uma espécie de "frase secreta" que criptografa a transmissão de dados. A comunicação quântica oferece uma forma única de segurança e criptografia, mas desafios técnicos e práticos ainda precisam ser superados para torná-la uma realidade amplamente utilizada.

Apesar dos avanços significativos, ainda existem desafios no desenvolvimento de redes globais de comunicação quântica, com os esforços atuais em estágios iniciais [17]. Embora seja difícil determinar com precisão quando isso ocorrerá, os especialistas estimam que a tecnologia possa amadurecer consolidadamente num período de 10 a 15 anos [18]. Para alcançar isso, é necessário desenvolver outras tecnologias essenciais, como processadores quânticos e um conjunto completo de protocolos e aplicativos específicos para a internet quântica. O objetivo final na comunicação quântica é criar uma rede de "internet quântica" — uma

rede de computadores quânticos interligados por comunicação quântica altamente segura [19].

C. Computação Quântica

Computação quântica pode ser entendida como uma forma alternativa de armazenar e processar informação. Assim como a computação clássica é baseada na unidade fundamental de informação *bit*, a computação quântica baseia-se no *quantum bit*, também conhecido como *qubit* [20].

Por conta de propriedades específicas da Mecânica Quântica, como a superposição de estados quânticos, algoritmos desenvolvidos em computação quântica – conhecidos como algoritmos quânticos – conseguem, em princípio, realizar determinadas tarefas em muito menos etapas do que os algoritmos clássicos [21]. Tal capacidade de executar tarefas mais rapidamente é comumente denominada "vantagem quântica" [22].

Um dos exemplos mais notáveis de vantagem quântica ocorreu em outubro de 2019, quando pesquisadores da Google utilizaram o processador quântico Sycamore de 53 qubits para geração de números aleatórios (*random number generation* ou RNG), o que foi feito cerca de 20 milhões de vezes mais rapidamente do que o melhor supercomputador clássico [23]. Apesar de limitadas, as aplicações de RNG são essenciais em áreas cruciais, como a criptografia [24], severamente impactando a segurança da comunicação digital.

Além do experimento da Google, há diversos outros algoritmos quânticos que são comprovadamente superiores aos correspondentes clássicos. Dentre estes, destaca-se o algoritmo de Shor – capaz de fatorar números inteiros exponencialmente mais rápido do que a melhor abordagem clássica disponível [25]. Uma vez que grande parte da criptografia atual é baseada na dificuldade de fatoração de números muito grandes, a implementação do algoritmo de Shor torna vulneráveis virtualmente todos os dados encriptados atualmente [26].

O impacto da computação quântica, no entanto, não está restrito à criptografia e segurança digital. A motivação primária da computação quântica – simulação mais acurada de sistemas quânticos – é, provavelmente, aquela que será concretizada em menor prazo [27]. Existem diversos algoritmos, como o *variational quantum eigensolver* (VQE), que permitem o cálculo da menor energia de um dado sistema quântico, apresentando importantes aplicações em química quântica e ciência de materiais [28].

Além das aplicações mais imediatas em simulações de sistemas quânticos, há diversas outras propostas de algoritmos quânticos em problemas de otimização [29] e *machine learning* [30], podendo ter impactos desde a indústria farmacêutica [31] ao *design* de estruturas mais aerodinâmicas em regime turbulento [32], por exemplo. A implementação de tais aplicações, contudo, requer processadores quânticos [33] ou técnicas de *quantum error correction* (QEC) [34] ainda não disponíveis atualmente. Com base nisso, pode-se traçar horizontes de maturidade de computação quântica dependendo do tempo estimado para alcançar as aplicações, conforme indicado na Figura 1.

Do ponto de vista do *hardware* quântico, há fundamentalmente duas vertentes sendo desenvolvidas na academia e na indústria. A primeira diz respeito à escalabilidade dos processadores quânticos atuais [33]. Dado que a maioria dos

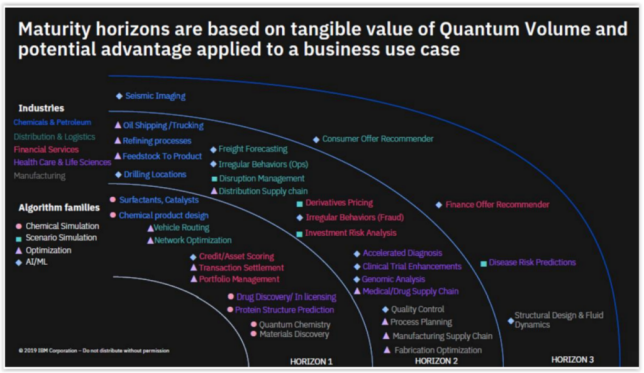

Fig. 1. Estimativa de diferentes horizontes de maturidade de aplicações de computação quântica, indo do horizonte 1 (mais imediato) ao 3 (mais longínquo) [35].

algoritmos quânticos requer milhões de qubits físicos [36] para atingir vantagem quântica frente aos métodos clássicos, tem-se um vasto espaço de melhoria nesse aspecto, partindo dos 433 qubits supercondutores atuais. A Figura 2 ilustra o plano de escalabilidade de *hardware* quântico supercondutor elaborado pela IBM. A segunda vertente, por sua vez, trata da melhoria da qualidade do qubit em si por meio do aumento do tempo de coerência, redução da taxa de erro das leituras dos qubits e melhorando a conectividade entre qubits [37].

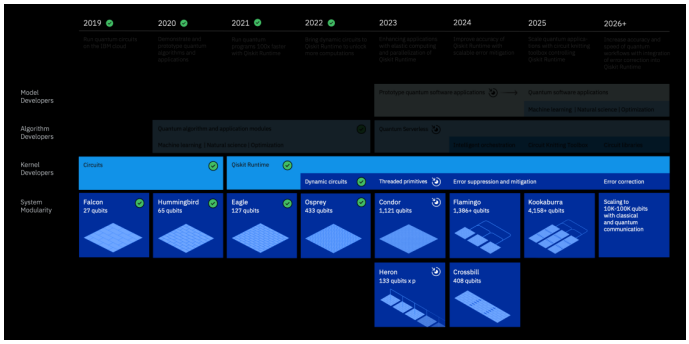

Fig. 2. Planejamento estipulado pela IBM de desenvolvimento de computadores quânticos supercondutores [38].

IV. Aplicações Militares

Nesta seção, mencionamos algumas das principais aplicações militares para tecnologias quânticas. Devido ao caráter sensível, essa análise é prejudicada ao utilizar apenas as informações já publicadas.

A. Relógios Atômicos

Relógios atômicos são considerados uma das primeiras tecnologias quânticas [39], sendo fundamentais no funcionamento de sistemas de posicionamento globais, como GPS, Galileo, GLONASS e BeiDou [40]. Esses sistemas são usados para fornecer localização e tempo com grande acurácia para sistemas militares [41]–[43]. O avanço na tecnologia de relógios atômicos, como os relógios lógicos quânticos e relógios de redes ópticas pode permitir o uso de sistemas de alta precisão em ambientes onde um sistema de posicionamento global é negado [44].

B. Radar Quântico

O radar quântico se baseia no emaranhamento de fótons para ter uma vantagem em medições sobre os radares clássicos [45], [46]. São um resultado direto da metrologia quântica, uma série de procedimentos para aumentar a precisão de medições [47]. O protocolo do radar quântico se baseia na iluminação quântica [48]. Um par de fótons emaranhado é gerado, enquanto um é enviado para o espaço, outro é armazenado em uma memória quântica. O fóton enviado, caso atinja algum alvo, pode ser refletido para o radar quântico. A princípio, não é possível distinguir fótons refletidos por um alvo ou apenas ruído do ambiente. Porém, a presença de emaranhamento permite, de forma probabilística, dizer se o fóton medido foi refletido pelo alvo ou se é apenas ruído [46]. Nesse sentido, radares quânticos possuem uma relação sinal-ruído melhor do que radares clássicos. Tanto a China quanto os Estados Unidos já estão trabalhando em pesquisa sobre radares quânticos [49].

C. Imageamento Fantasma Quântico

O imageamento fantasma (*ghost imaging*) [50], se refere a técnicas ópticas onde um objeto é identificado por um feixe de radiação eletromagnética que não atingiu o objeto, tendo por princípio o uso de correlações (clássicas ou quânticas) com outro feixe que atingiu o objeto. Uma das vantagens do imageamento fantasma é que, o objeto pode ser iluminado com uma dada frequência, enquanto o feixe correlacionado estar em outra frequência, por exemplo, uma frequência melhor adaptada para o detector, o que pode permitir resoluções melhores. Outra vantagem do imageamento fantasma é a possibilidade de utilizar protocolos similares à criptografia quântica para impedir manipulação de imagens por terceiros [51].

D. Magnetômetro SQUID

Magnetômetros, sensores capazes de detectar campos magnéticos, possuem diversas aplicações, desde metrologia, arqueologia, exploração de recursos naturais até aeroespaço, detecção de submarinos e minas. Um dos magnetômetros mais precisos se baseia em interferência quântica em supercondutores (SQUID) [52]. Magnetômetros podem ser usados para a detecção de navios ou submarinos através da detecção em anomalias do campo magnético devido à fuselagem metálica [53]. O uso de magnetômetros SQUID permite a detecção de submarinos a uma distância de quilômetros, como já demonstrado por chineses [54], que possuem já uma colaboração entre academia e indústria no desenvolvimento de SQUID's [55]. Também citamos que outros tipos de magnetômetros quânticos como alternativas a SQUID's também estão sendo desenvolvidos, como, por exemplo, usando magnetômetros atômicos [56].

E. Computação Quântica

A área mais vulnerável ao desenvolvimento da computação quântica é a criptografia. Para endereçar esta situação, numerosos investimentos estão sendo realizados em criptografia pós-quântica (*post-quantum cryptography* ou PQC) [57]. Esta consiste na elaboração e implementação de algoritmos clássicos que são resilientes até mesmo ao ataque de computadores quânticos futuros. Ao invés de se basearem na fatoração de números, os algoritmos de PQC usam estruturas mais complexas, como reticulados [58] e curvas elípticas [59], para encriptar a informação transmitida.

Em 2016, o *National Institute of Standards and Technology* (NIST) dos Estados Unidos iniciou uma competição de algoritmos de PQC para definir o padrão que será adotado futuramente para proteger a informação contra-ataques quânticos [60]. Após 6 anos e muitas rodadas de análise de especialistas em criptografia, o NIST anunciou os 4 algoritmos selecionados como padrão em PQC: CRYSTALS-Kyber para encapsulamento de chaves e CRYSTALS-Dilithium, SPHINCS+ e Falcon para assinatura digital [61].

F. Criptografia Quântica

A importância da implementação da criptografia quântica em aplicações militares está inserida no cenário da guerra cibernética e relaciona-se com a garantia da segurança e agilidade dos sistemas [62]. O risco de inteligência hostil coletar dados criptografados com a expectativa de futura decodificação usando o poder dos computadores quânticos é real, alto e presente [63]. Nesse contexto, surge a necessidade da vantagem quântica na guerra cibernética, o que permite se pensar em termos de ataque e defesa em contraposição aos algoritmos de criptografia atuais.

No escopo das capacidades defensivas, considerando que a informação quântica não pode ser copiada [64], uma potencial aplicação da criptografia quântica, pensando em aplicações militares, seria de substituir os esquemas convencionais de criptografia (principalmente assimétricos) envolvidos na troca de informações sensíveis entre entidades militares por algoritmos resistentes a ataques quânticos, utilizando a QKD [65].

Além disso, surge a necessidade da implementação da criptografia pós-quântica assim que ela for certificada e padronizada, fazendo-se mister a preparação da infraestrutura para implementá-la [66]. Isso se aplica tanto aos setores militares, de inteligência e governamentais, quanto à indústria ou academia, onde segredos e dados confidenciais são trocados ou armazenados. Observa-se que a criptografia pós-quântica deve ser implementada na Internet das Coisas (IoT) ou na Internet das Coisas Militares (IoMT) [67], como um setor em rápido crescimento com muitas potenciais violações de segurança. Por fim, vale ressaltar a tendência crescente mundial do uso de aprendizado de máquina ou inteligência artificial para a guerra cibernética [68].

V. Perspectivas e Oportunidades

As tecnologias quânticas têm o potencial de revolucionar tanto a esfera civil quanto a militar, oferecendo avanços significativos em computação, comunicação e sensores. Essas tecnologias são baseadas em propriedades intrínsecas da mecânica quântica, como a superposição e o emaranhamento, que permitem realizar tarefas de forma mais rápida e precisa do que os sistemas clássicos.

Em termos de potencial aplicação militar, as aplicações das tecnologias quânticas são promissoras. Contudo, apesar do enorme potencial, ainda existem desafios técnicos e práticos a serem superados para a implantação completa dessas tecnologias. Nesse contexto, o desenvolvimento de tecnologias

quânticas depende de instrumentos de alta-precisão, demandando uma engenharia sofisticada. A maioria das tecnologias quânticas se baseia em sistemas manipulados em nível atômico. Isso requer o estado tecnologia de estado da arte de microeletrônica, amplificadores micro-ondas de baixo ruído, fotônico e nanofabricação. O desenvolvimento de algoritmos quânticos possui a menor barreira de entrada, porém ao custo de se criar dependência tecnológica em relação aos países detentores dos *hardwares* quânticos.

Outrossim, o caminho para a maturidade e aplicação efetiva das tecnologias quânticas ainda é incerto, mas o progresso contínuo na pesquisa e no desenvolvimento pode levar a avanços significativos nas capacidades militares no futuro. O cuidado no desenvolvimento, monitoramento e adoção estratégica das tecnologias quânticas será essencial para garantir que os benefícios sejam aproveitados enquanto os riscos são mitigados, e que a segurança e a estabilidade global sejam preservadas.

REFERÊNCIAS

[1] J. P. Dowling and G. J. Milburn, "Quantum technology: the second quantum revolution," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[2] R. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, 1982.

[3] P. D. Lett, R. N. Watts, C. I. Westbrook, W. D. Phillips, P. L. Gould, and H. J. Metcalf, "Observation of atoms laser cooled below the doppler limit," *Phys. Rev. Lett.*, vol. 61, pp. 169–172, Jul 1988. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.61.169

[4] K. B. Davis, M.-O. Mewes, M. R. Andrews, N. J. van Druten, D. S. Durfee, D. Kurn, and W. Ketterle, "Bose-einstein condensation in a gas of sodium atoms," *Physical review letters*, vol. 75, no. 22, p. 3969, 1995.

[5] R. J. Glauber, *Quantum theory of optical coherence: selected papers and lectures*. John Wiley & Sons, 2007.

[6] T. W. Hänsch, "Repetitively pulsed tunable dye laser for high resolution spectroscopy," *Applied Optics*, vol. 11, no. 4, pp. 895–898, 1972.

[7] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities," *Physical review letters*, vol. 49, no. 2, p. 91, 1982.

[8] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of bell's inequalities using time-varying analyzers," *Phys. Rev. Lett.*, vol. 49, pp. 1804–1807, Dec 1982. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.49.1804

[9] G. J. Milburn and P. Davies, "Schroedinger's machines: The quantum technology reshaping everyday life," *(No Title)*, 1997.

[10] Q. Flagship, "Quantum manifesto," https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf, 2016, accessed: 2022-07-05.

[11] A. F. R. de Toledo Piza, *Mecânica quântica*. Edusp São Paulo, 2003.

[12] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[13] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, p. 035002, Jul 2017. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.89.035002

[14] K. M. Slayer and C. R. Service, "Defense primer: quantum technology," 2021.

[15] M. Giles. (2019, February 14) Explainer: What is quantum communication? Archive page. [Online]. Available: https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

[16] Q. Flagship, "Quantum communication," https://qt.eu/applications/quantum-communication, this website is developed with funding from the European Union's Horizon Europe Programme under Grant Agreement ID 101070193 © Quantum Flagship.

[17] A. Lele, *Quantum Technologies and Military Strategy*, 01 2021.

[18] M. van Amerongen, "Quantum technologies in defence & security," *NATO Review*, June 2021. [Online]. Available: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

[19] J. S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, M. Krutzik, S. Mohapatra, D. Dequal, G. Vallone, P. Villoresi, A. Ling, T. Jennewein, M. Mohageg, J. G. Rarity, I. Fuentes, S. Pirandola, and D. K. L. Oi, "Advances in space quantum communications," *IET Quantum Communication*, vol. 2, no. 1, pp. 37–45, 2021.

[20] R. P. Feynman, *Feynman lectures on computation*. CRC Press, 2018.

[21] S. Bravyi, D. Gosset, and R. König, "Quantum advantage with shallow circuits," *Science*, vol. 362, no. 6412, pp. 308–311, 2018.

[22] A. J. Daley, I. Bloch, C. Kokail, S. Flannigan, N. Pearson, M. Troyer, and P. Zoller, "Practical quantum advantage in quantum simulation," *Nature*, vol. 607, no. 7920, pp. 667–676, 2022.

[23] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[24] C. S. Petrie and J. A. Connelly, "A noise-based ic random number generator for applications in cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615–621, 2000.

[25] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[26] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, 2017.

[27] T. Hoefler, T. Häner, and M. Troyer, "Disentangling hype from practicality: on realistically achieving quantum advantage," *Communications of the ACM*, vol. 66, no. 5, pp. 82–87, 2023.

[28] D. Wang, O. Higgott, and S. Brierley, "Accelerated variational quantum eigensolver," *Physical review letters*, vol. 122, no. 14, p. 140504, 2019.

[29] A. Ajagekar and F. You, "Quantum computing for energy systems optimization: Challenges and opportunities," *Energy*, vol. 179, pp. 76–89, 2019.

[30] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[31] M. Zinner, F. Dahlhausen, P. Boehme, J. Ehlers, L. Bieske, and L. Fehring, "Quantum computing's potential for drug discovery: Early stage industry dynamics," *Drug Discovery Today*, vol. 26, no. 7, pp. 1680–1688, 2021.

[32] R. Steijl, "Quantum algorithms for fluid simulations," *Advances in quantum communication and information*, p. 31, 2019.

[33] N. P. De Leon, K. M. Itoh, D. Kim, K. K. Mehta, T. E. Northup, H. Paik, B. Palmer, N. Samarth, S. Sangtawesin, and D. W. Steuerman, "Materials challenges and opportunities for quantum computing hardware," *Science*, vol. 372, no. 6539, p. eabb2823, 2021.

[34] D. A. Lidar and T. A. Brun, *Quantum error correction*. Cambridge university press, 2013.

[35] IBM, "Quantum maturity horizons," *IBM Quantum Experience*, June 2019. [Online]. Available: https://formtek.com/blog/quantum-computing-future-paths-to-commercialization/

[36] J. Gambetta, "Ibm's roadmap for scaling quantum technology," *IBM Research Blog (September 2020)*, 2020.

[37] D. Rosenberg, D. Kim, R. Das, D. Yost, S. Gustavsson, D. Hover, P. Krantz, A. Melville, L. Racz, G. Samach *et al.*, "3d integrated superconducting qubits," *npj quantum information*, vol. 3, no. 1, p. 42, 2017.

[38] IBM, "The ibm quantum development roadmap," *IBM Quantum Experience*, November 2022. [Online]. Available: https://www.ibm.com/quantum/roadmap

[39] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technology*, vol. 8, 12 2021.

[40] Q. Ai, K. Maciuk, P. Lewinska, and L. Borowski, "Characteristics of onefold clocks of gps, galileo, beidou and glonass systems," *Sensors*, vol. 21, no. 7, p. 2396, 2021.

[41] J. R. Vig, "Military applications of high accuracy frequency standards and clocks," *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, vol. 40, no. 5, pp. 522–527, 1993.

[42] J. W. Betz, *GLONASS*, 2016, pp. 212–225.

[43] Y. Wu, H. Meng, and H. Yan, "Adaptive positioning and tracking system for military equipment based on beidou satellites," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2022, pp. 724–727.

[44] S. J. Gamberini and L. Rubin, "Quantum sensing's potential impacts on strategic deterrence and modern warfare," *Orbis*, vol. 65, no. 2, pp. 354–368, 2021.

[45] M. Lanzagorta, *Quantum radar*. Morgan & Claypool Publishers, 2012, vol. 5.

[46] M. Lanzagorta and J. Uhlmann, "Opportunities and challenges of quantum radar," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 11, pp. 38–56, 2020.

[47] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum metrology," *Physical review letters*, vol. 96, no. 1, p. 010401, 2006.

[48] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave quantum illumination," *Physical review letters*, vol. 114, no. 8, p. 080503, 2015.

[49] H. Vella, "Quantum radars: Expose stealth planes," *Engineering & Technology*, vol. 14, no. 4, pp. 42–45, 2019.

[50] M. J. Padgett and R. W. Boyd, "An introduction to ghost imaging: quantum and classical," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 375, no. 2099, p. 20160233, 2017.

[51] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, "Quantum-secured imaging," *Applied physics letters*, vol. 101, no. 24, 2012.

[52] K. Gramm, L. Lundgren, and O. Beckman, "Squid magnetometer for mangetization measurements," *Physica Scripta*, vol. 13, no. 2, p. 93, 1976.

[53] G. Ioannidis, "Identification of a ship or submarine from its magnetic signature," *IEEE Transactions on Aerospace and Electronic Systems*, no. 3, pp. 327–329, 1977.

[54] K. Kubiak, *Quantum technology and submarine near-invulnerability*. JSTOR, 2020.

[55] J. Lin, M. Wang, and J. Zhao, "Review: Progress in squid-based geophysical precision measurement technology," *J. Harbin Inst. Technol*, vol. 27, no. 03, pp. 101–115, 2020.

[56] S. Y. Hussain, "Application of quantum magnetometers to security and defence screening," Ph.D. dissertation, UCL (University College London), 2018.

[57] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[58] J. Buchmann, R. Lindner, M. Rückert, and M. Schneider, "Post-quantum cryptography: lattice signatures," *Computing*, vol. 85, pp. 105–125, 2009.

[59] B. Koziel, R. Azarderakhsh, M. M. Kermani, and D. Jao, "Post-quantum cryptography on fpga based on isogenies on elliptic curves," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 1, pp. 86–99, 2016.

[60] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko, and S. Kavun, "Code-based cryptosystems from nist pqc," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, 2018, pp. 282–287.

[61] A. Fregly, J. Harvey, B. S. Kaliski Jr, and S. Sheth, "Merkle tree ladder mode: Reducing the size impact of nist pqc signature algorithms in practice," in *Cryptographers' Track at the RSA Conference*. Springer, 2023, pp. 415–441.

[62] G. Alagic *et al.*, "Status report on the second round of the nist post-quantum cryptography standardization process," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR 8309, 2020. [Online]. Available: https://doi.org/10.6028/nist.ir.8309

[63] S. A. Wolf *et al.*, "The changing face of data security: 2020 thales data threat report," Thales, 2020.

[64] J. Park, "The concept of transition in quantum mechanics," *Foundations of physics*, pp. 23–33, 1970.

[65] N. Gisin and R. Thew, "Quantum communication," *Nat Photonics*, vol. 1, no. 3, pp. 165–171, 2007.

[66] M. J. D. Vermeer and E. D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*. RAND Corporation, 2020. [Online]. Available: https://doi.org/10.7249/RR3102

[67] L. Cameron. Internet of things meets the military and battlefield. IEEE Computer Society. [Online]. Available: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

[68] K. Kline, M. Salvo, and D. Johnson, "How artificial intelligence and quantum computing are evolving cyber warfare," Cyber Intelligence Initiative, The Institute of World Politics, 2019, https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/ (visited on 02/24/2021).