https://doi.org/10.55972/spectrum.v27i1.449

ORIGINAL PAPER

Spectrum - The Journal of Operational Applications in Defense Areas

Journal homepage: https://spectrum.ita.br

Quantum Technologies: Quantum Computing

Quantum Technologies: Current Outlook, Challenges and Opportunities

André J. Chaves[1,2,*], Denys Derlian C. Brito[1], Rodrigo P. Ferreira[1], and Victor G. M. Duarte[1]

[1] Instituto Tecnológico de Aeronáutica (ITA), 12228-900, São José dos Campos/São Paulo – Brasil

[2] Centro de Física das Universidades do Minho e do Porto (CF-UM-UP) e Departamento de Física da Universidade do Minho, P-4710-057, Braga – Portugal

[*] Corresponding Author: andrejck@ita.br

Keywords

Quantum Technologies
Military Applications
Quantum Sensing
Quantum Communication
Quantum Computing

Article Information

Received	14 July 2026
Revised	01 August 2026
Accepted	02 August 2026
Available	03 August 2026

Abstract

Quantum technologies result from the use of the laws of modern physics in increasingly sophisticated devices, promising enormous advances in computing, communication, and sensing, for both civilian and military use. As a consequence of technological progress that has miniaturized instrumentation down to atomic scales, we are witnessing the nanoscale manipulation of physical systems using intrinsic properties of quantum systems, such as entanglement. Quantum sensors are able to go beyond classical detection limits. Quantum communication offers a security advantage over classical communication. Quantum computing enables the solution of problems considered impossible to solve with classical computers. These technologies emerge as a result of advances in science and engineering, enabling the manipulation of systems at the atomic level. In this article we briefly present the fundamental concepts of quantum mechanics, the main examples of quantum technologies in sensing, communication, and computing. We show military applications and conclude by presenting the challenges and opportunities.

1. Introduction

Quantum mechanics was developed at the beginning of the 20th century to explain atomic phenomena that contradicted classical physics. Throughout that century, the application of quantum theory enabled countless advances in science and technology, such as the development of semiconductors, transistors, and lasers. These advances also depended on a better understanding of what light is, and therefore on the formulation of quantum electrodynamics. This first quantum revolution was based on the wave-like character of quantum mechanics, as, for example, in the understanding of semiconductor theory. The advancement of nanotechnology and instrumentation allowed the manipulation of systems with increasing precision and the exploration of more quantum phenomena at the nanoscopic scale. This gave rise to a second quantum revolution [1], which includes using the challenging concept of measurement in quantum mechanics as a tool, along with properties such as superposition and entanglement.

The peer review process was coordinated, and the final publication approved, by Humberto Baldessarini Pires.

Several instruments enabled the realization of quantum technologies, such as scanning tunneling microscopes, lasers, optical tweezers, superconductors, cryogenic refrigerators, and many others. On the theoretical side, the creation of quantum information theory, uniting information theory with quantum mechanics, enabled advances in the understanding of quantum phenomena arising from entanglement. Already in the 1980s, Richard Feynman envisioned that the physics of quantum systems would need to be simulated by a quantum computer [2]. That decade was also marked by advances in quantum optics, as can be seen from five Nobel Prizes, beginning with experiments with ultracold atoms [3], Bose-Einstein condensation [4], quantum coherence [5], and laser spectroscopy [6], measurement and manipulation of quantum systems, and the experimental study of photon entanglement [7], [8]. These advances enabled the concept of Schrödinger Machines [9], which depend on our ability to manipulate matter at the atomic level. There are many ways to divide quantum technologies, but following the European Union's Quantum Manifesto, we have quantum sensors, quantum simulation, quantum communication, and quantum computing [10]. While the advancement of quantum technologies

presents opportunities, it also brings risks and challenges. The real impact that all these technologies will have in the future is difficult to predict; however, in this article we briefly discuss the current situation and future prospects, with a focus on the defense sector.

1.1. Methodology

The methodology adopted included research and literature reviews in academic databases and journals specialized in quantum technologies. In addition, official documents from government agencies and research institutions were analyzed to obtain information on the global landscape and on the future applications of these technologies. Qualitative analysis of the information collected made it possible to identify trends, technological developments, and practical application cases of quantum technologies, providing a current outlook, along with the main challenges and opportunities for military applications.

In Section (2), we present the fundamental concepts of quantum mechanics that will be used in the other sections of the article. In Section (3) we present the areas of quantum sensing, communication, and computing. In Section (4) we present the main military technologies, and in Section (5) we conclude by discussing the opportunities and challenges for the Brazilian armed forces.

2. Fundamental Concepts

Quantum systems are governed by the Schrödinger equation, which, given an initial state, determines its time evolution according to the system's Hamiltonian [11]. The states accessible to a system belong to a vector space called Hilbert space, which has an inner product. Observables are Hermitian linear operators on the Hilbert space, whose eigenvalues are the possible outcomes of a measurement, with the probability of a given measurement given by the Born Rule, corresponding to the square of the inner product between the state and the state vector as it becomes the eigenvector of the operator corresponding to the measured state [11]. This probability is intrinsic to quantum mechanics and is not related to uncertainties arising from the experimental apparatus. This property is used in several quantum technologies, as we will see in Section 3.

Quantum technologies are based on properties of quantum systems, such as quantization, superposition, and entanglement. Quantization, already present in the description of the hydrogen atom, occurs when a quantum particle is confined by a potential and results in a discrete set of energies. The geometry of the confining potential can be engineered, determining the energy levels. This effect is exploited in quantum dots and wells, which have applications ranging from TV screens to infrared radiation sensors for military use.

Superposition, analogous to what happens with classical waves, such as electromagnetic or acoustic waves, refers to the sum of two distinct states. Using Bra-Ket notation, superposition refers to:

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

with $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Superposition in quantum mechanics is a result of the choice of basis. Superposition is used both in quantum computing, since the qubit is written as the superposition of two states, corresponding to logical 0 and logical 1, and in quantum communication, as, for example, in the BB84 protocol.

Entanglement is the main resource of quantum information theory. It is an intrinsic property of quantum systems that correlates measurements of observables. Let us illustrate this with the maximally entangled state of two identical particles. Using $|a,b\rangle$ to denote that particle 1 is in state $|a\rangle$ and particle 2 is in state $|b\rangle$, one of the maximally entangled states is:

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

because, if particle 1 is measured in state a, we can be certain that particle 2 will be measured in state b. The same does not happen for the product state:

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

As a consequence of quantum entanglement, Bell proposed inequalities for expected values which, if violated, would confirm the predictions of quantum mechanics [12], as has already been carried out experimentally [7].

3. Quantum Technologies

In this section we discuss three of the main pillars of quantum technologies: sensing, communication, and computing. This list is not exhaustive, as it could also include items such as atomic clocks and quantum simulation [10]. In common, all these technologies make use of concepts from quantum information theory.

3.1. Quantum Sensors

There are three definitions of quantum sensing [13]: i) quantum objects used to measure physical properties; ii) systems that use quantum coherence; or iii) sensors that make use of quantum entanglement. As examples of i) and ii), we have neutral atoms, ion traps, Rydberg atoms, atomic clocks, nitrogen-vacancy centers in diamond, spin-based sensors, nuclear magnetic resonance, and superconducting circuits. In this section we will comment on some properties and examples of quantum sensors. Most quantum sensors are based on two-level systems. They are controlled by a time-dependent external signal, generally provided by electromagnetic radiation in the visible or infrared range, or by electric or magnetic fields [13].

Considering that the quantum sensor operates through the interaction of a qubit with the external signal, the coupling factor is called the transduction parameter, directly related to sensitivity, which is proportional to the sensor's response to a desired signal and inversely proportional to its response to noise [13]. Depending on the object to be measured, different

measurement protocols can be used. The use of entangled qubits for measurement can increase sensitivity. Quantum sensors are considered the most mature quantum technology for military application [14]. In subsections 4.1 and 4.2 we will discuss the military uses of quantum radar and SQUID magnetometers.

3.2. Quantum Communication

A concept of hacker-proof quantum communication, grounded in the "no-cloning theorem" formulated in 1982, allows the secure transmission of data without the risk of eavesdropping. This technology promises more secure and comprehensive communication, offering practical solutions to protect sensitive information across various domains [15].

Quantum communication encompasses various technologies and applications, ranging from laboratory experiments to commercially available technologies, the main ones being Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG) [16]. The basis of quantum communication is quantum entanglement, in which two users share pairs of particles with linked properties. This property is compared and used to create a kind of "secret phrase" that encrypts the data transmission. Quantum communication offers a unique form of security and encryption, but technical and practical challenges still need to be overcome to make it a widely used reality.

Despite significant advances, challenges still remain in the development of global quantum communication networks, with current efforts still in early stages [17]. Although it is difficult to determine precisely when this will occur, experts estimate that the technology may reach solid maturity within a period of 10 to 15 years [18]. To achieve this, it is necessary to develop other essential technologies, such as quantum processors and a complete set of protocols and applications specific to the quantum internet. The ultimate goal of quantum communication is to create a "quantum internet" — a network of quantum computers interconnected by highly secure quantum communication [19].

3.3. Quantum Computing

Quantum computing can be understood as an alternative way of storing and processing information. Just as classical computing is based on the fundamental unit of information, the *bit*, quantum computing is based on the *quantum bit*, also known as the *qubit* [20].

Because of specific properties of quantum mechanics, such as the superposition of quantum states, algorithms developed for quantum computing — known as quantum algorithms — can, in principle, perform certain tasks in far fewer steps than classical algorithms [21]. This ability to perform tasks more quickly is commonly referred to as "quantum advantage" [22].

One of the most notable examples of quantum advantage occurred in October 2019, when Google researchers used the 53-qubit Sycamore quantum processor for random number generation (RNG), which was done about 20 million times faster than the best classical supercomputer [23]. Although limited, RNG applications are essential in crucial areas such as cryptography [24], severely impacting the security of digital communication.

In addition to Google's experiment, there are several other quantum algorithms that have been proven superior to their classical counterparts. Among these, Shor's algorithm stands out — capable of factoring integers exponentially faster than the best available classical approach [25]. Since much of current cryptography is based on the difficulty of factoring very large numbers, the implementation of Shor's algorithm renders virtually all currently encrypted data vulnerable [26].

The impact of quantum computing, however, is not restricted to cryptography and digital security. The primary motivation for quantum computing — more accurate simulation of quantum systems — is probably the one that will be realized in the shortest time frame [27]. There are several algorithms, such as the variational quantum eigensolver (VQE), that allow the calculation of the lowest energy of a given quantum system, with important applications in quantum chemistry and materials science [28].

Beyond the more immediate applications in simulating quantum systems, there are several other proposed quantum algorithms for optimization problems [29] and machine learning [30], which could have impacts ranging from the pharmaceutical industry [31] to the design of more aerodynamic structures in turbulent regimes [32], for example. Implementing such applications, however, requires quantum processors [33] or quantum error correction (QEC) techniques [34] that are not yet available today. Based on this, one can outline maturity horizons for quantum computing depending on the estimated time to reach these applications, as shown in Figure 1.

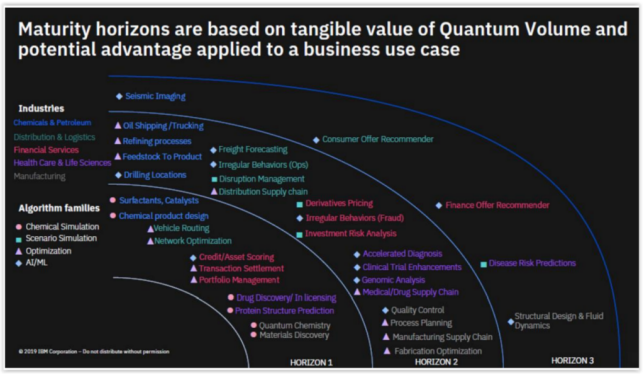

Fig. 1. Estimate of different maturity horizons for quantum computing applications, ranging from horizon 1 (most immediate) to 3 (most distant) [35].

From the point of view of quantum hardware, there are fundamentally two directions being developed in academia and industry. The first concerns the scalability of current quantum processors [33]. Given that most quantum algorithms require millions of physical qubits [36] to achieve quantum advantage over classical methods, there is a vast room for improvement in this respect, starting from the current 433 superconducting qubits. Figure 2 illustrates the scalability roadmap for superconducting quantum hardware developed by IBM. The second direction, in turn, deals

with improving the quality of the qubit itself by increasing coherence time, reducing the error rate of qubit readouts, and improving connectivity between qubits [37].

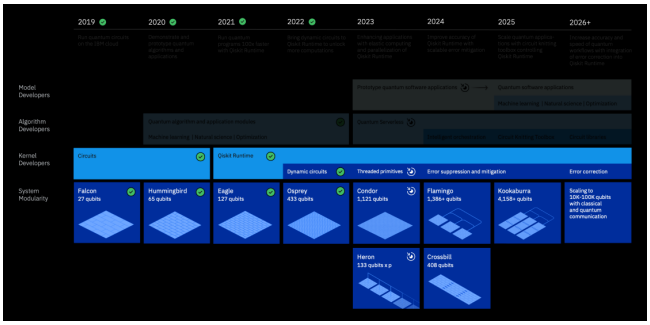

Fig. 2. Roadmap set out by IBM for the development of superconducting quantum computers [38].

4. Military Applications

In this section, we mention some of the main military applications for quantum technologies. Due to the sensitive nature of the subject, this analysis is limited by relying only on already published information.

4.1. Quantum Radar

Quantum radar is based on photon entanglement to gain a measurement advantage over classical radars [39], [40]. It is a direct result of quantum metrology, a set of procedures to increase measurement precision [41]. The quantum radar protocol is based on quantum illumination [42]. A pair of entangled photons is generated; while one is sent into space, the other is stored in a quantum memory. The photon sent out, if it hits a target, may be reflected back to the quantum radar. In principle, it is not possible to distinguish photons reflected by a target from mere environmental noise. However, the presence of entanglement makes it possible, probabilistically, to determine whether the measured photon was reflected by the target or is just noise [40]. In this sense, quantum radars have a better signal-to-noise ratio than classical radars. Both China and the United States are already working on quantum radar research [43].

4.2. SQUID Magnetometer

Magnetometers, sensors capable of detecting magnetic fields, have several applications, ranging from metrology, archaeology, natural resource exploration, to aerospace, and the detection of submarines and mines. One of the most precise magnetometers is based on superconducting quantum interference (SQUID) [44]. Magnetometers can be used to detect ships or submarines by detecting anomalies in the magnetic field caused by the metal hull [45]. The use of SQUID magnetometers allows the detection of submarines at a distance of kilometers, as already demonstrated by the Chinese [46], who already have a collaboration between academia and industry in the development of SQUIDs [47]. We also note that other types of quantum magnetometers as alternatives to SQUIDs are also being developed, such as, for example, using atomic magnetometers [48].

4.3. Quantum Computing

The area most vulnerable to the development of quantum computing is cryptography. To address this situation, numerous investments are being made in post-quantum cryptography (PQC) [49]. This consists of the design and implementation of classical algorithms that are resilient even to attacks from future quantum computers. Instead of relying on integer factorization, PQC algorithms use more complex structures, such as lattices [50] and elliptic curves [51], to encrypt transmitted information.

In 2016, the National Institute of Standards and Technology (NIST) of the United States launched a competition for PQC algorithms to define the standard that will be adopted in the future to protect information against quantum attacks [52]. After 6 years and many rounds of analysis by cryptography experts, NIST announced the 4 algorithms selected as the PQC standard: CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium, SPHINCS+, and Falcon for digital signatures [53].

4.4. Quantum Cryptography

The importance of implementing quantum cryptography in military applications lies within the context of cyber warfare and relates to ensuring the security and agility of systems [54]. The risk of hostile intelligence collecting encrypted data with the expectation of future decryption using the power of quantum computers is real, high, and present [55]. In this context, the need arises for quantum advantage in cyber warfare, which allows one to think in terms of attack and defense in contrast to current cryptographic algorithms.

Within the scope of defensive capabilities, considering that quantum information cannot be copied [56], a potential application of quantum cryptography, in terms of military applications, would be to replace conventional cryptographic schemes (mainly asymmetric ones) involved in the exchange of sensitive information between military entities with algorithms resistant to quantum attacks, using QKD [57].

In addition, there arises the need to implement post-quantum cryptography as soon as it is certified and standardized, making it essential to prepare the infrastructure to implement it [58]. This applies both to military, intelligence, and government sectors, as well as to industry or academia, where secrets and confidential data are exchanged or stored. It is worth noting that post-quantum cryptography should be implemented in the Internet of Things (IoT) or the Internet of Military Things (IoMT) [59], as a rapidly growing sector with many potential security breaches. Finally, it is worth highlighting the growing global trend of using machine learning or artificial intelligence for cyber warfare [60].

5. Perspectives and Opportunities

Quantum technologies have the potential to revolutionize both the civilian and military spheres, offering significant

advances in computing, communication, and sensing. These technologies are based on intrinsic properties of quantum mechanics, such as superposition and entanglement, which allow tasks to be performed faster and more precisely than with classical systems.

In terms of potential military application, the applications of quantum technologies are promising. However, despite the enormous potential, there are still technical and practical challenges to be overcome for the full deployment of these technologies. In this context, the development of quantum technologies depends on high-precision instruments, requiring sophisticated engineering. Most quantum technologies are based on systems manipulated at the atomic level. This requires state-of-the-art technology in microelectronics, low-noise microwave amplifiers, photonics, and nanofabrication. The development of quantum algorithms has the lowest barrier to entry, but at the cost of creating technological dependence on the countries that hold the quantum hardware.

Furthermore, the path to maturity and effective application of quantum technologies is still uncertain, but continued progress in research and development may lead to significant advances in military capabilities in the future. Careful development, monitoring, and strategic adoption of quantum technologies will be essential to ensure that the benefits are realized while risks are mitigated, and that global security and stability are preserved.

Author Contributions

Chaves, A. J.: Conceptualization, Methodology, Supervision, Investigation, Formal Analysis, Writing – Original Draft, Visualization. **Brito, D. D. C.**: Investigation, Writing – Review & Editing. **Ferreira, R. P.**: Investigation, Writing – Review & Editing. **Duarte, V. G. M.**: Investigation, Writing – Review & Editing.

All authors have read and approved the final version of the manuscript and assume full responsibility for its accuracy, integrity, and originality.

Conflict of Interest Statement

The authors declare that there are no financial, commercial, political, academic, or personal conflicts of interest related to the conduct and publication of this research.

References

[1] J. P. Dowling 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, 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, 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, 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, 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 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, 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. Sayler, "Defense primer: Quantum technology," Congressional Research Service, CRS Report for Congress IF11836, 2021. [Online]. Available: https://www.congress.gov/crs-product/IF11836

[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*, ser. Advanced Sciences and Technologies for Security Applications. Cham, Switzerland: Springer Cham, 04 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, 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, 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, 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 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, 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, S. Brierley, "Accelerated variational quantum eigensolver," *Physical review letters*, vol. 122, no. 14, p. 140504, 2019.

[29] A. Ajagekar 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, 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, 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, D. W. Steuerman, "Materials challenges and opportunities for quantum computing hardware," *Science*, vol. 372, no. 6539, p. eabb2823, 2021.

[34] D. A. Lidar 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. Lanzagorta, *Quantum radar*. Morgan & Claypool Publishers, 2012, vol. 5.

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

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

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

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

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

[45] 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.

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

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

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

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

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

[51] B. Koziel, R. Azarderakhsh, M. M. Kermani, 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.

[52] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko, 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.

[53] A. Fregly, J. Harvey, B. S. Kaliski Jr, 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.

[54] 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

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

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

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

[58] M. J. D. Vermeer 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

[59] 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

[60] K. Kline, M. Salvo, 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).