Quantum Technology and the Military—Revolution or Hype?

The Impact of Emerging Quantum Technologies on Future Warfare

Captain Daniel Choi, USMC

6 September 2023

https://doi.org/10.36304/ExpwMCUP.2023.11

Abstract: While the fundamental nature of war remains constant, military strategies continue to evolve in response to capabilities enabled by new technologies. Therefore, military leaders must be aware of emerging and disruptive technologies to maintain forces that are relevant. One such technology is quantum technology, which has received a great deal of attention in the past few years due to its potential application in a wide range of areas. Particularly, quantum technology promises breakthroughs in various domains of warfare by significantly enhancing current military technology. This article explores three major defense applications of quantum technology—quantum computing, quantum sensing, and quantum

---

Capt Daniel Choi commissioned into the Marine Corps in 2017 through the Naval Reserve Officers Training Corps at Cornell University in Ithaca, NY, with a bachelor of arts in mathematics. After serving as a Bell Boeing MV-22B Osprey tiltrotor aircraft pilot, he made a lateral move and is currently serving as an intelligence officer with III Marine Expeditionary Force. The views expressed in this article are solely those of the author. They do not necessarily reflect the opinions of Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government.

communication—and their impact on future warfare based on realistic assessment.

Keywords: quantum technology, quantum computing, quantum sensing, quantum communication, modernization, military technology

As the United States' national strategy shifted its focus toward competing with China, questions have been raised about the U.S. Marine Corps' relevance to the needs of the nation. The Service's current force design is optimized for large-scale amphibious Joint forcible entry operations (JFEO) and sustained operations ashore.[1] However, with the global proliferation of long-range precision missiles, advanced early warning radars, unmanned aerial vehicles (UAVs), and cyber capabilities, former U.S. secretary of defense Robert M. Gates and scholars at the Center for a New American Security and the Center for Strategic and Budgetary Assessments challenged the Service's decades-old multi-Marine expeditionary brigade amphibious JFEO organization design and associated investment.[2] In response, General David H. Berger, the 38th Commandant of the Marine Corps, announced *Force Design 2030* in March 2020, outlining the shortfalls of the Marine Corps' current force design and the need for change to maintain the Service's relevance in contested environments against advanced peer competitors.

Force Design 2030 is the epitome of adaptation, a survival mechanism against selective pressures. One of the major selective pressures that is forcing the Marine Corps to change is the advancement of peer competitors' technology at an unprecedented rate. While technology alone does not change the fundamental nature of war, it certainly influences the strategies

that must be employed to win. Due to the importance of technology in national security, the U.S. government continues to invest billions of dollars each year to fund defense laboratories such as the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research, and the Army Research Laboratory.[3] These research agencies develop new defense technologies and keep leaders informed of how they might impact various aspects of warfare. However, it is ultimately the responsibility of the Marine Corps to adopt and tailor these new technologies in such a way to allow it to provide relevant, unique capabilities to the Joint force. An increased understanding of emerging technology across all levels of leadership would accelerate the adoption of new technology as demanded by rapid technological advancements. This article represents the author's attempt to raise awareness of quantum technology, a major emergent and potentially disruptive technology, and its potential impact on the future battlefield so that the Marine Corps can collectively and proactively maintain a force suitable for future requirements.

An Introduction to Quantum Technology

In the first quarter of the twentieth century, a group of brilliant minds—Albert Einstein, Niels Bohr, Max Planck, Werner Heisenberg, Erwin Schrödinger, and Paul A. M. Dirac, among others—revolutionized the world's understanding of microscopic phenomena by developing the theory of quantum mechanics.[4] The discovery of these new fundamental laws of nature marked the first quantum revolution, resulting in the invention of currently established technologies such as nuclear weapons, the global positioning system (GPS), lasers, semiconductors, and modern communication technologies.[5]

Combined, these technologies have had significant impact on modern warfare. Nuclear weapons can cause mass destruction, giving nuclear-armed states unparalleled advantages over non-nuclear-armed states. Radar and GPS allow ballistic missiles to target any place on the globe. Computers equipped with internet permit near-instant global communication, creating an entirely new domain of warfare: cyberspace.

Since the first quantum revolution, further advancement in technology has allowed for the manipulation of quantum systems (such as particles) at the individual level. The second quantum revolution was marked by the discovery that precise control of individual quantum systems enables one to harness quantum phenomena to develop new technologies. *Quantum technology* refers to the class of technologies that emerged from the second quantum revolution and have the potential to spur breakthroughs in a wide range of application areas in both government and private sectors. Global interest in research and innovation in quantum technology has been steadily rising in the past two decades, with many countries—the United States, the United Kingdom, the European Union, Japan, and China, among others—launching research programs to accelerate the development of quantum technology.[6]

This article seeks to answer the following questions: What exactly are these emerging quantum technologies, and how will they affect the conduct of future warfare? In doing so, it will explore major applications of quantum technology and realistic possibilities based on practical challenges associated with developing quantum technology.

Quantum Computing

Underlying Principles

Quantum computers process information in a fundamentally different way than classical computers. In classical computers, the most basic unit of information is called a *bit*. Each bit is stored in a transistor that can turn on or off, often represented as 1 or 0, respectively. A bit can be thought of as a coin on a table with a definite state: either tail-side (1) or head-side (0) up. In quantum computers, the most basic unit of information is called a *qubit* (short for *quantum bit*), which is stored in a quantum system (spin states of an atom, polarization of a photon, etc.). A qubit, unlike a bit, can exist in a superposition state, simultaneously being in a combination of 1 and 0 states with varying probabilities of being 1 or 0. A qubit can be thought of as a spinning coin on a table: it is neither head-side nor tail-side up, but instead in an indefinite state with probabilities of landing head-side or tail-side up. Superposition allows qubits to store an exponential number of states. For example, while 10 bits can represent only one of the 2^{10} (1,024) possible states at one time, 10 qubits can represent all 1,024 states at the same time. Another key distinguishing characteristic of qubits is *entanglement*. When two qubits are entangled, effects on one qubit instantaneously affect the other qubit. By performing various operations on entangled qubits in superposition states, one can control enormous amount of data in parallel. If one could accurately measure and gather all states at the end, quantum computers would have a truly transformative impact on humanity. Unfortunately, the laws of quantum mechanics dictate that the measurement on qubits randomly "selects" only one of the possible states, and the other states disappear.[7] Fortunately, there are clever ways to increase the probability of obtaining certain states.

Quantum computers can therefore outperform classical computers by processing exponentially larger amount of data and yielding the correct solution with high probability. The ability of qubits to exist in multiple states simultaneously (superposition) and nonlocal correlation among qubits (entanglement) are the hallmarks of quantum computers.

Cryptoanalysis

Quantum computers can solve a specific set of problems much faster than classical computers. One example is breaking asymmetric cryptosystems. The most commonly used asymmetric cryptosystem today is the Rivest-Shamir-Adleman (RSA) cryptosystem, which is widely used in email, logins, credit-card payments, and other digital data transmissions to ensure privacy and authenticity of data.[8] The security of the RSA cryptosystem relies on the hardness of prime factorization. Given a set of prime numbers, it is easy to multiply those numbers. Given a large number, on the other hand, it is not so easy to find prime factors that make up the number. As an example, it takes classical computers trillions of years to find prime factors of a 2048-bit number, a typical size of an RSA key. A breakthrough came in the mid-1990s when Peter W. Shor discovered a quantum algorithm (Shor's algorithm named for him) that can break a 2048-bit RSA encryption key in a matter of hours using quantum computers.[9] Shor's algorithm can also solve other asymmetric cryptosystems such as elliptic-curve cryptography, which is considered more secure and efficient than the RSA cryptosystem.[10] This introduces the question: Is it no longer safe to purchase things online using a credit card? The answer is no—at least not yet—as scalable quantum computers required to break asymmetric encryption keys are still decades

away. Nevertheless, current encrypted data is still vulnerable to so-called "harvest now, decrypt later" (HNDL) attacks.[11] HNDL refers to the act of collecting sensitive encrypted data that can be decrypted later once scalable quantum computers are available. This poses serious security concerns, especially for classified information, the disclosure of which can cause damage to national security even decades after the initial classification. Aware of HNDL and future cyber threats posed by the development of quantum computers, the U.S. National Security Agency is currently implementing other encryption systems, known as quantum-resistant (QR) algorithms, that are not vulnerable to known quantum algorithms. The transition to QR algorithms for U.S. national security systems is expected to be complete by 2035.[12] That said, quantum cryptanalysis is an area of extensive research, and whether these QR algorithms will remain unexploitable by other algorithms yet to be discovered remains unanswered.

Optimization

Cryptoanalysis is perhaps the most widely known application of quantum computers. Nevertheless, there are many other application areas, such as optimization and simulation, in which quantum computers can outperform classical computers. The field of quantum optimization algorithms has been an extensive area of research due to the ubiquity of optimization problems. While there are various optimization problem types, all can be stated broadly as: find the best option in a set of all possible options, given a desired outcome and constraints. There is a surprisingly large number of optimization problems relating to the military, such as transportation and logistics, emergency response, sensor deployment, target detection, cyberdefense,

multiship/multiaircraft mission planning for large combat operations, UAV planning and assignment, theater ballistic missile defense, and more.[13] Most currently known quantum optimization algorithms, however, only provide up to polynomial speedup.[14] If, for example, a classical computer requires 100 hours to complete an optimization task, a quantum computer could reduce the number of hours to 10—or from 10,000 hours to 100 hours, from n hours to $\sqrt{n}$ hours, and so on. A polynomial speedup is not trivial, but the improvement is not as significant as an exponential speedup. It does not reduce trillions of years of required computational time to a few hours like Shor's algorithm; rather, it reduces trillions of years to something more like a million years. This is certainly an improvement, but not a breakthrough. Meanwhile, advances in quantum computing inspire more efficient classical computing methods. For example, DARPA launched the Quantum-Inspired Classical Computing program in 2021 in an attempt to develop a quantum-inspired classical computing method to solve complex optimization problems relevant to the U.S. Department of Defense and reported that such a method has the potential to outperform quantum computers by more than a factor of 10,000.[15] Quantum computers provide only a moderate speedup in solving optimization problems against continuously advancing classical algorithms and computational methods. While a near polynomial speedup is not insignificant, another breakthrough in quantum optimization algorithm would be required for quantum computers to achieve a more significant exponential speedup.

Simulation

Quantum simulation is probably the most practical near-term application of quantum computers. Computer simulation of physical systems is nothing new and, in fact, has become an indispensable tool in the past half-century in advancing various fields of science and technology, including material science, molecular biology, chemistry, astronomy, and many others. However, due to the inherent limitation of classical computers, certain physical systems—namely quantum systems greater than approximately 50 qubits in size—generally cannot be simulated even by the world's fastest supercomputer in a reasonable amount of time.[16] In contrast, quantum computers use qubits, which are a quantum system and have the very properties suitable for the efficient simulation of quantum systems. This is precisely what Richard P. Feynman, one of the pioneers in the field of quantum computing, envisioned in 1981: simulation of quantum models using a quantum device.[17] Although some clever methods, such as density functional theory or Quantum Monte Carlo, allow classical computers to simulate a quantum system in a reasonable amount of time at the expense of some errors, these approximation techniques fail at problems in which even a small error leads to significant changes in simulation results. One example of such problems is the simulation of superconductors, materials with zero electrical resistance below a certain critical temperature. These materials could have far-reaching applications in the military realm, such as in efficient electrical power distribution, mine detection, naval vessel propulsion, and levitated trains.[18] Superconductors discovered thus far, however, require extremely low temperatures (-470° Fahrenheit to -160° Fahrenheit) or extremely high pressure (150 gigapascals to 250 gigapascals),

or a combination of both, to work.[19] Considering that the lowest temperature ever reported at ground level on Earth is -128.6° Fahrenheit and that the Earth's inner core pressure is 365 gigapascals, large-scale practical application of superconductors requires a discovery of a new material that superconducts at ambient temperature and pressure.[20] The challenge in studying superconductors is that there is no universally accepted theory that accurately describes high-temperature superconductivity. Additionally, because superconductivity depends sensitively on individual electron-electron interaction, current approximation methods are insufficient to qualitatively predict the accurate structure of superconductors. Quantum computers, in contrast, have the potential to exactly simulate the quantum structures and behaviors of superconducting materials. In addition to material science, other applications of quantum simulation include the discovery of new drugs that cure diseases and catalysis that facilitates important chemical reactions such as nitrogen fixation, all of which are important and probably impactful enough to win a Nobel Prize.[21]

Artificial Intelligence

From predicting protein structures to autonomously controlling plasma inside a nuclear fusion reactor, artificial intelligence is transforming various industries, and the defense sector is no exception.[22] Artificial intelligence can provide a wide range of defense applications, including but not limited to target recognition, text analysis, self-driving vehicles, swarm intelligence for drone operations, data processing, and intelligence fusion, which could dramatically increase operational efficiencies.[23] Current artificial intelligence training methods rely heavily on machine learning, a subfield of artificial

intelligence that enables systems to recognize patterns in data, make predictions, and extract insights through the use of statistical methods. Training artificial intelligence with machine learning techniques requires tremendous amounts of data and computing power. For example, ChatGPT, one of the most popular large language models to date, was trained on more than 1,000 high-end graphics processing units and 570 gigabytes of text data and cost $4.6 million.[24]

Recent studies show that quantum algorithms could, in theory, provide polynomial and exponential speedup for some machine learning tasks and requires much less data.[25] Use of quantum algorithms and quantum computers to perform machine learning tasks is called *quantum machine learning* (QML) and could significantly reduce the cost, amount of training data, and time associated with training an artificial intelligence model. However, QML still remains theoretical because the quantum advantage is based on certain assumptions about the data and hardware. For example, some QML algorithms assume that classical data is encoded in the amplitudes of a quantum state, but it is unclear whether this encoding scheme is practically feasible in a realistic device.[26] Furthermore, hardware noise can corrupt the dataset preparation scheme and prevent QML algorithms from finding optimal solutions due to the phenomenon known as noise-induced barren plateaus.[27] Despite the current challenges associated with the application of QML, the future development of standardized quantum data sets, new efficient data encoding schemes, and low-noise scalable quantum hardware could provide a cost-effective artificial intelligence training solution.

Building Quantum Computers

Despite tremendous potential for applications of quantum computers, physical realization of practical quantum computers presents immense challenges. One of the major challenges in building a quantum computer is the extreme fragility of qubits. Interaction between qubits and the environment causes information stored in the qubits to leak out and can lead to inadvertent measurement of the qubits. The qubits then become classical bits; the superposition reduces to either 1 or 0.[28] This loss of quantum information is called *decoherence*. For this reason, qubits must be well-isolated from the environment. But this introduces several issues: that complete isolation of qubits is practically impossible; that as the number of qubits increases, it becomes more difficult to isolate them; and that one must interact with qubits to control them and perform computations.[29] Imperfect isolation and manipulation of qubits inevitably lead to decoherence, which in turn results in errors. Hence, *quantum error correction*, an algorithm that encodes a qubit into a collection of qubits (or *logical qubit*), has been proposed as the solution to this problem.[30] Each logical qubit needs dozens or even thousands of ancillary qubits to identify and correct errors. In other words, storing and processing 10 logical qubits of information with a sufficiently low error rate may actually require anywhere between about 100 to 10,000 physical qubits, depending on the type of qubits. Worse yet, as the number of qubits increases, the quantum computer becomes more susceptible to *crosstalk*, unwanted interaction between qubits, which can cause even more errors.[31] Since the first proposal of theoretical quantum error correction methods in 1985, several experimental realizations of quantum error

correction have been demonstrated.[32] Nevertheless, these were limited to only a few or a dozen qubits and the correction of only specific types of errors.

Another challenge is the physical realization of qubits. There are several approaches to building quantum computers, each with substantial obstacles to be overcome. Superconducting qubits, the method most widely used, must be kept at an extremely low temperature between 10 and 20 milli-Kelvins (0.001–0.002 Kelvin above the lowest temperature possible) and decohere (lose quantum properties) in 1.48 milliseconds.[33] Trapped ions, another popular approach, also operate at a low temperature below 10 Kelvin. Although trapped ions have a much longer coherence time compared to superconducting qubits and can be controlled with high fidelity, their processing speed is still too slow to provide any meaningful advantage over a classical computer.[34] Photonic qubits are stable and can operate at room temperature; however, significant improvement is still needed in reliably generating and detecting photons and manipulating multiple photons simultaneously.[35] Other methods have been pursued by scientists, such as quantum dots and nitrogen-vacancy centers, but these are still in their infancy.

Many other challenges remain, such as scalability and cost, to allow for the realization of a practical quantum computer. However, based on IBM roadmaps, the projected progress rate in both algorithms and hardware, and the majority expert prediction, it seems reasonable to expect practical, scalable quantum computers that can solve relevant problems within the next 20–30 years.[36]

Quantum Sensing

Interestingly, quantum systems' strong sensitivity to external disturbances—the very characteristic that makes building a quantum computer such a difficult task—can be used to our advantage in improving the accuracy of sensors. *Quantum sensing* describes the employment of quantum mechanical systems to measure various physical quantities such as electric field, magnetic field, gravity, acceleration, and rotation by capitalizing on the weakness of quantum systems.[37] Sensors from the first quantum revolution are already in prolific use. For example, magnetometers have widely been used in archeology, environmental surveys, and ordnance and weapons detection.[38] Atomic clocks have been incorporated into GPS satellites for synchronization for nearly half a century.[39] With the ability to control individual quantum systems from the second quantum revolution, one can enhance measurement precision even further, up to several orders of magnitude.

Quantum Inertial Navigation

One major quantum sensing application in the defense sector is quantum inertial navigation. Both Russia and China are proliferating counterspace capabilities to engage in GPS jamming and physically degrade or damage U.S. satellites. Yet, the U.S. military still relies heavily on its GPS for surface, ground, and air navigation.[40] In a GPS-degraded or -denied environment, national positioning, navigation, and timing capabilities will be impacted. Furthermore, GPS is not available in underground or underwater environments. To compensate, most military aircraft, precision missiles, land vehicles, and naval vessels are equipped with inertial navigation systems (INS)

that can determine their position by continuously calculating rotation and acceleration. Because INS drifts over time due to accumulation of measurement errors, this necessitates frequent recalibration, typically by satellites, for a long-period or high-accuracy navigation. To put this into context, high-end INS drifts approximately 1.8 kilometers per day for ships, submarines, and spacecraft and 1.5 kilometers per hour for aircraft, though exact figures may vary based on the specific platform and speed.[41]

Quantum sensors offer a solution to this problem with unprecedented measurement accuracy. A recent study showed that a hybrid quantum accelerometer can reliably measure the acceleration of 6 $x10^{-8}$ gravity for an extended period of time—that is, 0.0000006 percent of Earth's gravity, a 50-fold improvement in measurement stability over classical accelerometers.[42] Accurate accelerometers can reduce INS drift and permit accurate, prolonged navigation without communicating with external entities and disclosing the user's position. While fast, robust, and compact inertial sensors with required performance in relevant environments are yet to be fully developed, quantum inertial navigation promises passive, undeniable navigation capability in the future.

Quantum Radio Frequency Sensing

Communication is crucial for command and control in an increasingly complex operating environment. One major trend in military communication is transitioning from voice-only systems to datalink to enable delivery of maps, images, and videos. This transition requires wider bandwidths, which in turn increases the size, weight, and power of communication systems.[43] Rydberg atom-based sensors have the potential to act as a compact,

wideband radio-frequency receiver. Rydberg atoms are highly excited atoms with high sensitivity to electric fields with frequencies ranging from 100 megahertz to 1 terahertz.[44] Moreover, Rydberg atom-based antennas are only approximately 1 millimeter in size, much smaller than that of traditional antennas, which range from 10 centimeters to 3 meters. There still remains technical hurdles that must be overcome to make Rydberg atom-based sensors more affordable and deployable.[45] The biggest challenge is the cryogenics required for cooling Rydberg atoms. With further advances in laser-cooling techniques, Rydberg atom-based sensors could provide a smaller and more capable passive radio-frequency receiver.

Quantum Communication

Quantum Key Distribution

From African talking drums and Samuel Morse's telegraph to the relatively recent inventions of fiber optic cable and satellite, long-distance communication has revolutionized the world. Nearly all financial, agricultural, energy, and governmental organizations and industries rely heavily on their digital infrastructures for transmitting and receiving data. Due to this exclusive reliance on digital communication and increasing complexity of critical infrastructure networks, communication failure or cyberattack on a single node can result in a catastrophic chain reaction. In this context, communication security is of paramount importance.

Current communication security primarily uses asymmetric cryptosystems. However, as previously discussed, the security of asymmetric cryptosystems relies on computational assumptions that may not be valid in the future due to rapid advancements in computation hardware and

algorithms, such as quantum computers and Shor's algorithm. One alternative to the asymmetric cryptosystem is a symmetric cryptosystem, in which one key is used to both encrypt and decrypt data and proper exchange of the key between users is required. The problem is that this transmission of the secret key is not fundamentally secure because the key can be copied by a third party during the transmission. In other words, symmetric cryptosystems are vulnerable to eavesdroppers.[46] In 1984, Charles H. Bennett and Gilles Brassard proposed a novel way of exchanging a secret key called *quantum key distribution* (QKD), which promises information-theoretic security—unconditional security owing only to the laws of physics—by using quantum systems to encode information and exploiting the no-cloning theorem, another key property of quantum systems.[47] The no-cloning theorem states that it is impossible to copy a quantum state, preventing eavesdroppers from cloning quantum states in transmission without altering the states. A change in states causes errors, which can be detected by the sender and receiver after the transmission. If the error rate is above a certain threshold, the sender and receiver can reasonably assume that someone is eavesdropping and discard the key. If the error rate is below the threshold, the sender and receiver can be sure that nobody has extracted sufficient information about the key by the laws of physics and that they have securely exchanged the key. To put it succinctly, eavesdroppers cannot gain enough information about the secret key without being detected by the sender and receiver. For this reason, QKD is a promising security protocol for future communication.

Turning a theoretical QKD protocol into practical hardware involves several challenges. First, information is lost at an exponential or quadratic

rate as photons travel through and interact with fiber optic cable or free space.[48] Second, the currently achieved key generation rate of QKD is about 100 megabytes per second, which limits the amount of data that can be securely transmitted.[49] Third, achieving unconditional security in practice requires rigorous security proof for the underlying protocol because the imperfections of realistic devices introduce vulnerabilities such as a side-channel attack.[50]

In the past two decades, progress has been made in developing practical QKD. In terms of performance, China is taking the lead with the largest demonstrated QKD network of more than 4,600 kilometers and the highest key generation rate of more than 100 megabytes per second.[51] In terms of security, a handful of new QKD protocols have been proposed to achieve practical security.[52] However, each protocol is considered under different security assumptions and may still be vulnerable to various attacks. Currently, the National Security Agency does not yet consider QKD a viable security protocol due to the limitations associated with implementation.[53] Further progress in distance, key generation rate, and practical security is still needed before QKD can be used to protect critical infrastructures.

Quantum Network

A *quantum network* refers to the connection of quantum computers and sensors that enables the distribution of quantum information. But why would a quantum network be needed when the internet already provides near-instant communication across the globe? The answer is that a quantum network would have many applications unattainable by classical internet, including QKD that could provide information-theoretic security, blind

quantum computing that could provide private computation, and global timekeeping that could improve GPS.[54] Perhaps the most important application is quantum internet. As discussed above, building a scalable quantum computer is extremely challenging, and the number of qubits will limit the problems it can solve. A network of quantum computers that can share qubits could potentially perform computations that are beyond the reach of individual quantum computers.[55]

One of the key challenges in the practical implementation of a quantum network is decoherence—the decay of quantum information—over long distances. This requires a series of intermediate systems called *quantum repeaters* that regenerate an incoming signal but still need to satisfy the no-cloning theorem, as the incoming quantum signal cannot simply be copied. Entanglement swapping could, in theory, resolve this issue and create entanglement over long distances to serve as a quantum repeater. However, this process requires reliable and practical quantum memory, which is not yet available.[56] Although a group of researchers from China demonstrated an all-photonic quantum repeater that does not need a quantum memory, other challenges remain, such as the creation of graph states.[57] If these challenges are overcome and a quantum network is established, it would accelerate the research in QKD and quantum computing applications.

Conclusion

Quantum technology will not replace existing technology—rather, it will enhance existing technology. Quantum cryptoanalysis could diversify cyber operations for the U.S. military in general and the Marine Corps in particular in both offensive and defensive domains. The invention and implementation

of quantum-resistant algorithms would be one example of cyber defense. Quantum optimization algorithms could solve various optimization problems, including but not limited to route planning, supply chain, multi-UAV employment, and missile defense, increasing operational efficiency while reducing the resources required. Quantum simulation could lead to the development of lighter, robust, and more energy-efficient materials, enabling Marines to sustain longer with a lighter footprint in a distributed environment. Quantum sensors could enable extended navigation and wideband radio-frequency reception with a smaller footprint and little to no electromagnetic signature. A quantum network could provide a high level of communication security and enable the distribution of quantum information.

It is important to note that these applications are still theoretical due to the engineering challenges associated with implementation. Most technologies from the second quantum revolution are still decades away from practical application. The Marine Corps should not be too farsighted, as it must be able to fight at a moment's notice—but at the same time, it should not be too myopic to become outdated and lose relevance in the future. The rapidly advancing technology of the United States' peer competitors demands that the Marine Corps adopt new technology quickly. One precursor to the timely and sound acquisition, doctrinal development, and tactical employment of new technology is to maintain collective awareness of emerging disruptive technologies across all levels of leadership so that the Marine Corps can properly organize, equip, and train Marines to serve as the nation's stand-in force for the future.

---

[1] Gen David H. Berger, *Force Design 2030* (Washington, DC: Headquarters Marine Corps, 2020).
[2] LtCol Scott Cuomo et al., "Not Yet Openly at War, but Still Mostly at Peace," *Marine Corps Gazette* 103, no. 2 (February 2019): 6–22.

[3] Eric Chewning et al., "How Will U.S. Funding for Defense Technology Innovation Evolve?," McKinsey & Company, 4 November 2022; and "Department of Defense Release the President's Fiscal Year 2024 Defense Budget," U.S. Department of Defense, 13 March 2023.
[4] Jun John Sakurai and Jim Napolitano, *Modern Quantum Mechanics*, 3d ed. (Cambridge, UK: Cambridge University Press, 2022), v, https://doi.org/10.1017/9781108587280.
[5] Michal Krelina, "Quantum Technology for Military Applications," *European Physical Journal Quantum Technology* 8, no. 24 (December 2021): 1, 15, https://doi.org/10.1140/epjqt/s40507-021-00113-y.
[6] "Overview on Quantum Initiatives Worldwide: Update 2022," Quantum Resources and Careers, 10 March 2022.
[7] Scott Aaronson, "The Limits of Quantum Computers," *Scientific American*, 1 March 2008.
[8] Dan Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," *Notices of the American Mathematical Society* 46 (February 1999): 203–12; and Ron L. Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1978): 120–26, https://doi.org/10.1145/359340.359342.
[9] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* 26, no. 5 (1997), https://doi.org/10.1137/S0097539795293172; and Craig Gidney and Martin Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," *Quantum* 5 (2021): 433, https://doi.org/10.48550/arXiv.1905.09749.
[10] Dindayal Mahto, Danish Ali Khan, and Dilip Kumar Yadav, "Security Analysis of Elliptic Curve Cryptography and RSA," *Proceedings of the World Congress on Engineering* 1 (2016).
[11] Vikram Sharma, "Quantum and the Cybersecurity Imperative," *Digital Debates: CyFy Journal* 9 (2022): 15–22.
[12] "Announcing the Commercial National Security Algorithm Suite 2.0," National Security Agency, 7 September 2022.
[13] Vladimir Boginski, Eduardo Pasiliao, and Sigian Shen, "Special Issue on Optimization in Military Applications," *Optimization Letters* 9 (2015): 1475–76, https://doi.org/10.1007/s11590-015-0966-4; and William M. Carlyle, "Military Applications of Optimization," Naval Post Graduate School, 19 April 2018.
[14] Fernando G. S. L. Brandao and Krysta M. Svore. "Quantum Speed-ups for Solving Semidefinite Programs," *IEEE 58th Annual Symposium on Foundations of Computer Science* (2017): 415–26, https://doi.org/10.1109/FOCS.2017.45.
[15] "Solving Defense Optimization Problems with Increased Computational Efficiency," Defense Advanced Research Projects Agency, 4 October 2021.
[16] Sergio Boixo et al., "Characterizing Quantum Supremacy in Near-Term Devices," *Nature Physics* 14, no. 6 (2018): 595–600, https://doi.org/10.1038/s41567-018-0124-x.
[17] Richard P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics* 21, no. 6/7 (1982): 467–88, https://doi.org/10.1007/BF02650179.
[18] Isabelle Dumé, "Quantum Microscopy Sheds Light on High-temperature Superconductivity," Physics World, 9 November 2022; and Sajid Saleem, "Military Applications of Superconductivity and Future Perspectives," *International Conference on Electrical Engineering* 9, no. 9 (2014), https://doi.org/10.21608/ICEENG.2014.30474.
[19] Lilia Boeri et al., "The 2021 Room-Temperature Superconductivity Roadmap," *Journal of Physics: Condensed Matter* 34, no. 18 (2021): 183002, https://doi.org/10.1088/1361-648X/ac2864.

[20] "World: Lowest Temperature," World Meteorological Organization's World Weather and Climate Extremes, Arizona State University, accessed 31 December 2022; and "Core," National Geographic, accessed 31 December 2022.
[21] Gabriel Popkin, "Waiting for the Quantum Simulation Revolution," American Physical Society, 21 October 2019.
[22] "AlphaFold Protein Structure Database," AlphaFold, accessed 10 August 2023; Rob Toews, "AlphaFold Is the Most Important Achievement in AI—Ever," *Forbes*, 3 October 2021; and Jonas Degrave et al., "Magnetic Control of Tokamak Plasmas through Deep Reinforcement Learning," *Nature* 602, no. 7897 (2022): 414–19, https://doi.org/10.1038/s41586-021-04301-9.
[23] Forrest E. Morgan et al., *Military Applications of Artificial Intelligence* (Santa Monica, CA: Rand, 2020), https://doi.org/10.7249/RR3139-1; and "The Most Useful Military Applications of AI in 2023 and Beyond," Sentient Digital, February 2023.
[24] Charmaine Lai et al., "AI Is Harming Our Planet: Addressing AI's Staggering Energy Cost," Numenta, 24 May 2022.
[25] Yunchao Liu, Srinivasan Arunachalam, and Kristan Temme, "A Rigorous and Robust Quantum Speed-up in Supervised Machine Learning," *Nature Physics* 17, no. 9 (September 2021): 1013–17, https://doi.org/10.1038/s41567-021-01287-z; and Matthias C. Caro et al., "Generalization in Quantum Machine Learning from Few Training Data," *Nature Communications* 13, no. 1 (2022): 4919, https://doi.org/10.1038/s41467-022-32550-3.
[26] Marco Cerezo et al., "Challenges and Opportunities in Quantum Machine Learning," *Nature Computational Science* 2, no. 9 (September 2022): 567–76, https://doi.org/10.1038/s43588-022-00311-3.
[27] Samson Wang et al., "Noise-Induced Barren Plateaus in Variational Quantum Algorithms," *Nature Communications* 12, no. 1 (2021): 6961, https://doi.org/10.1038/s41467-021-27045-6.
[28] Scott Aaronson, "What Makes Quantum Computing So Hard to Explain?," *Quanta Magazine*, 8 June 2021.
[29] Philip Ball, "Major Quantum Computing Strategy Suffers Serious Setbacks," *Quanta Magazine*, 29 September 2021.
[30] Peter W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," *Physical Review A* 52, no. 4 (1995): R2493, https://doi.org/10.1103/PhysRevA.52.R2493; Raymond Laflamme et al., "Perfect Quantum Error Correcting Code," *Physical Review Letters* 77, no. 1 (1996): 198, https://doi.org/10.1103/PhysRevLett.77.198; and Daniel Gottesman, "Theory of Fault-Tolerant Quantum Computation," *Physical Review A* 57, no. 1 (1998): 127, https://doi.org/10.1103/PhysRevA.57.127.
[31] Yongshan Ding et al., "Systematic Crosstalk Mitigation for Superconducting Qubits via Frequency-Aware Compilation," *2020 53d Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)* (2020): 201–14, https://doi.org/10.1109/MICRO50266.2020.00028.
[32] John Chiaverini et al., "Realization of Quantum Error Correction," *Nature* 432, no. 7017 (2004): 602–5, https://doi.org/10.1038/nature03074; Matthew D. Reed et al., "Realization of Three-Qubit Quantum Error Correction with Superconducting Circuits," *Nature* 482, no. 7385 (2012): 382–85, https://doi.org/10.1038/nature10786; Alexander Erhard et al., "Entangling Logical Qubits with Lattice Surgery," *Nature* 589, no. 7305 (2021): 220–24, https://doi.org/10.5281/zenodo.4081412; and Bryn A. Bell et al., "Experimental Demonstration of a Graph State Quantum Error-Correction Code," *Nature Communications* 5, no. 3658 (2014): 1–10, https://doi.org/10.1038/ncomms4658.
[33] Matthias Steffen et al., "Quantum Computing: An IBM Perspective," *IBM Journal of Research and Development* 55, no. 5 (2011): 13:1–13:11, https://doi.org/10.1147/JRD.2011.2165678; and

Aaron Somoroff et al., "Millisecond Coherence in a Superconducting Qubit," *Physical Review Letters* 130, 267001 (2023), https://doi.org/10.1103/PhysRevLett.130.267001.

[34] Colin D. Bruzewicz et al., "Trapped-Ion Quantum Computing: Progress and Challenges," *Applied Physics Reviews* 6, no. 2 (2019): 021314, https://doi.org/10.1063/1.5088164. *Cryogenics* refers to the science that deals with effects of very low temperature, not necessarily the method of cooling.

[35] Fulvio Flamini, Nicolò Spagnolo, and Fabio Sciarrino, "Photonic Quantum Information Processing: A Review," *Reports on Progress in Physics* 82, no. 1 (2018): 016001, https://doi.org/10.1088/1361-6633/aad5b2; and Amirhossein Nourbakhsh et al., "Quantum Computing: Fundamentals, Trends and Perspectives for Chemical and Biochemical Engineers," arXiv preprint, arXiv:2201.02823 (2022), https://doi.org/10.48550/arXiv.2201.02823.

[36] Joran van Apeldoorn and Koen Groenland, "The Professional's Guide to Quantum Technology," Quantum Amsterdam, accessed 8 May 2023; and "McKinsey Technology Trends Outlook 2022," McKinsey & Company, August 2022.

[37] Christian L. Degen, Friedemann Reinhard, and Paola Cappellaro, "Quantum Sensing," *Reviews of Modern Physics* 89 (2017): 035002, https://doi.org/10.1103/RevModPhys.89.035002.

[38] Ivan Hrvoic and Greg M. Hollyer, "Brief Review of Quantum Magnetometers," GEM Advanced Magnetometers, accessed 9 May 92023.

[39] Krelina, "Quantum Technology for Military Applications," 15.

[40] *GPS Modernization: DOD Continuing to Develop New Jam-Resistant Capability, but Widespread Use Remains Years Away* (Washington, DC: U.S. Government Accountability Office, 2021).

[41] Martino Travagnin, "Cold Atom Interferometry for Inertial Navigation Sensors: Technology Assessment: Space and Defence Applications," *JRC Technical Reports,* JRC122785 (2020): 26, https://doi.org/10.2760/237221.

[42] Simon Templier et al., "Tracking the Vector Acceleration with a Hybrid Quantum Accelerometer Triad," *Science Advances* 8, no. 45 (2022), https://doi.org/10.1126/sciadv.add3854.

[43] Wyatt Taylor "Next-Generation Military Communications Challenges," Military Embedded Systems, 9 October 2019.

[44] Ashok K. Mohapatra et al., "A Giant Electro-Optic Effect Using Polarizable Dart States," *Nature Physics* 4, no. 11 (2008): 890–94, https://doi.org/10.1038/nphys1091; Christopher G. Wade et al., "Real-Time Near-Field Terahertz Imaging with Atomic Optical Fluorescence," *Nature Photonics* 11, no. 1 (2017): 40–43, https://doi.org/10.1038/nphoton.2016.214; and David H. Meyer et al., "Assessment of Rydberg Atoms for Wideband Electric Field Sensing," *Journal of Physics B: Atomic, Molecular and Optical Physics* 53, no. 3 (2020): 034001, https://doi.org/10.1088/1361-6455/ab6051.

[45] Charles T. Fancher et al., "Rydberg Atom Electric Field Sensors for Communications and Sensing," *IEEE Transactions on Quantum Engineering* 2 (2021): 1–13, https://doi.org/10.1109/TQE.2021.3065227.

[46] Eleni Diamanti et al., "Practical Challenges in Quantum Key Distribution," *NPJ Quantum Information* 2, no. 16025 (2016): 1–12, https://doi.org/10.1038/npjqi.2016.25.

[47] Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *International Conference on Computers, Systems & Signal Processing* 1 (1984): 175–79, https://doi.org/10.48550/arXiv.2003.06557; and William K. Wootters and Wojciech H. Zurek, "A Single Quantum Cannot be Cloned," *Nature* 299, no. 5886 (1982): 802–3, https://doi.org/10.1038/299802a0.

[48] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde, "Fundamental Rate-Loss Tradeoff for Optical Quantum Key Distribution," *Nature Communications* 5, 5235 (2014), https://doi.org/10.1038/ncomms6235; and Sheng-Kai Liao et al., "Satellite-to-Ground Quantum Key Distribution," *Nature* 549 (2017): 43–47, https://doi.org/10.1038/nature23655.

[49] Diamanti et al., "Practical Challenges in Quantum Key Distribution," 1–12; and Wei Li et al., "High-Rate Quantum Key Distribution Exceeding 100 Mb s^{-1}," *Nature Photonics* 17, no. 5 (2023): 416–21, https://doi.org/10.1038/s41566-023-01166-4.

[50] Feihu Xu et al., "Secure Quantum Key Distribution with Realistic Devices," *Reviews of Modern Physics* 92, no. 2 (2020): 025002, https://doi.org/10.1103/RevModPhys.92.025002; and Rupesh Kumar et al., "Experimental Vulnerability Analysis of QKD Based on Attack Ratings," *Scientific Reports* 11, no. 9564 (2021), https://doi.org/10.1038/s41598-021-87574-4.

[51] Yu-Ao Chen et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 kilometers," *Nature* 589 (2021): 214–19, https://doi.org/10.1038/s41586-020-03093-8.

[52] Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers, "Unconditional Security of Practical Quantum Key Distribution," *European Physical Journal D* 41, no. 3 (March 2007): 599–627, https://doi.org/10.1140/epjd/e2007-00010-4; and Feihu Xu et al., "Secure Quantum Key Distribution with Realistic Devices," *Reviews of Modern Physics* 92, no. 2 (2020), https://doi.org/10.1103/RevModPhys.92.025002.

[53] "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," National Security Agency, accessed 6 August 2023.

[54] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi, "Universal Blind Quantum Computation," *IEEE Symposium on Foundations of Computer Science* (2009): 517–26, https://doi.org/10.48550/arXiv.0807.4154; and Péter Kómár et al., "A Quantum Network of Clock," *Nature Physics,* no. 8 (2014): 582–87, https://doi.org/10.48550/arXiv.1310.6045.

[55] Christoph Simon, "Towards a Global Quantum Network," *Nature Photonics* 11 (2017): 678–80, https://doi.org/10.48550/arXiv.1710.11585.

[56] Lijun Ma, Oliver Slattery, and Xiao Tang, "Optical Quantum Memory and its Applications in Quantum Communication Systems," *Journal of Research of the National Institute of Standards and Technology* 125, no. 125002 (2020): 125, https://doi.org/10.6028/jres.125.002.

[57] Zheng-Da Li et al., "Experimental Quantum Repeater without Quantum Memory," *Nature Photonics* 13 (2019): 644–48, https://doi.org/10.1038/s41566-019-0468-5; and Koji Azuma et al., "Quantum Repeaters: From Quantum Networks to the Quantum Internet," arXiv preprint, arXiv:2212.10820 (2022), https://doi.org/10.48550/arXiv.2212.10820.