National Institute of Standards and Technology physicist Katie McCormick adjusts mirror to steer laser beam used to cool trapped beryllium ion, as part of efforts to improve quantum measurements and quantum computing, October 26, 2018 (National Institute of Standards and Technology/James Burrus)

The Quantum Internet

How DOD Can Prepare

By Lubjana Beshaj, Samuel Crislip, and Travis Russell

In the 1980s, Richard Feynman famously posed the idea of a computer that harnessed the power of quantum mechanics to carry out calculations.[1] Feynman observed that the computers of his day had a difficult time modeling complex molecular systems. He observed that if the computer harnessed the laws of quantum mechanics, it could easily model such molecular systems. By the mid-1990s, the concept of a quantum computer was well established in academia, and at that time mathematician Peter Shor discovered a polynomial-time algorithm for factoring large integers on one.[2] It was soon observed that such an algorithm, by quickly computing keys for decryption, would break many widely used encryption schemes previously considered secure.

Recent advances in quantum technology made by state and private actors transformed the quantum computer from an idea to working prototype. Although a computer capable of carrying out Shor's algorithm is likely still years away, stakeholders in government and industry have largely accepted the need to prepare for a quantum future. The most obvious feature of this preparation is the race by the National Institute of Standards and Technology and others to produce secure postquantum cryptographic schemes that are unlikely to be impacted when full-scale quantum computing comes to fruition.[3] Less attention has been paid,

Dr. Lubjana Beshaj is a Cyber Fellow of Mathematics in the Army Cyber Institute and an Assistant Professor in the Department of Mathematical Sciences at the United States Military Academy (USMA). Command Sergeant Major Samuel Crislip, USA, is Command Sergeant Major at the 782nd Military Intelligence Battalion Command in Fort Gordon, Georgia. Dr. Travis Russell is a Research Scientist in the Army Cyber Institute and an Assistant Professor in the Department of Mathematical Sciences at the USMA.

however, to the infrastructure that will need to be in place to support a network of active quantum computers. Such a network is commonly referred to as the *quantum Internet*.

In this article, we discuss how the quantum Internet is likely to develop, according to experts. Following the model proposed by Stephanie Wehner, David Elkouss, and Ronald Hanson, we break this development into six stages.[4] Each stage introduces a new technology that makes the Internet "more quantum" than it was at the previous stage. As we discuss each development, we draw the reader's attention to technologies and trends of interest to the Department of Defense (DOD). We argue that increasing DOD focus on quantum technology and a viable quantum Internet may lead to innovations in the areas of secure communications, quantum sensing, and clock synchronization, as well as other yet-to-be-discovered technologies.

We wish to emphasize that this article elaborates on the model proposed by Wehner, Elkouss, and Hanson but does not propose an alternative version, though other models may well exist, and the actual way in which a quantum Internet may develop is entirely unknown. The six stages we describe are such that, at each stage, a new technology is introduced that addresses a vulnerability of the previous stage. In this article we do not address the potential costs or returns on investments in these technologies; we describe the technologies only qualitatively. We also do not speculate when these technologies will be widely available, as there is ample conjecture on this question in the literature.

The future viability of (and accessibility to) a quantum Internet could shape the strategic environment for U.S. military forces. This environment comprises the critical operational areas in which DOD finds itself during competition, conflict, or combat. These operations are known, sometimes interchangeably, as multidomain or all-domain operations (MDO/ADO). Joint doctrine currently recognizes land, sea, air, space, and cyber as the warfighting domains within MDO/ADO.[5] A quantum Internet is especially applicable to the cyber domain, as it requires many of the current physical components of the Internet—while necessitating an expansion of many of those assets and an inclusion of new technologies. As DOD and the U.S. Government invest in developing a quantum Internet or securing their access to it, they will witness a growth in their cyber domain capabilities, which, due to the interwoven nature of MDO/ADO, will translate to gains in the other warfighting domains.

Quantum Technology and the Quantum Internet

For our purposes, the term *quantum Internet* refers to any network of computer systems or communication devices that employ technologies that are inherently quantum. It does not necessarily refer to a new Internet separate from the current one; rather, the term refers to an emerging infrastructure that will be intertwined with the existing Internet. A quantum Internet would likely be necessary to carry out communication between fully operational quantum computers once that technology has developed; however, we see that a quantum Internet would enable much more than the integration of quantum computers, which might not be realized for many years. A quantum Internet, or even the addition of quantum components to the existing Internet, allows for the future integration of quantum computers into the existing Internet and makes possible the transfer and storage of an entirely new kind of information, known colloquially as *quantum information*. Whereas classical information is encrypted and stored as sequences of bits—that is, strings of 0s and 1s—quantum information is encoded in the state of a system of quantum bits, or qubits. A single qubit is the quantum state of a particle in a superposition of a pair of possible states, which is often regarded as a mixture of 0 and 1. In practice, qubits are often encoded as the polarization of a photon or the spin of an electron, though other possibilities have been studied. With access to multiple qubits, the entire system could become "entangled" so that the state of one qubit is closely correlated with the state of another (potentially remote) qubit. In this way, computations carried out on separate qubits in distant locations may instantaneously interfere and affect one another.[6]

The laws of quantum mechanics endow quantum information with many properties that distinguish it from classical information and make new applications possible. For example, the no-cloning theorem of quantum mechanics makes it impossible to design an apparatus that takes as input a qubit and produces as output two copies of the same qubit. In other words, an eavesdropper who intercepts a qubit in transit cannot copy the qubit and send the original to its destination undetected. Moreover, the measurement principle of quantum mechanics implies that if an eavesdropper measures any property of a qubit in transit, the state of the qubit will change. Such change could be detected on receipt so that manipulated qubits could be discarded. Entanglement makes possible many other applications, such as new clock synchronization protocols and taking advantage of existing correlations between remote entangled qubits.[7] In summary, a quantum Internet has the potential to alter not only the infrastructure of the cyber domain but also the nature of the information stored and transmitted within that infrastructure.

Although the exact process by which the existing Internet will evolve into a quantum Internet is unknown, experts have recently weighed in on what the process might entail.[8] In the following pages, we describe six stages of development that are predicted to occur as the quantum Internet emerges. At each stage a new technology is introduced that enables significantly more functionality to the quantum Internet. In addition to a summary of these stages, we offer commentary concerning how new technologies introduced at each stage could affect the interests of DOD and what steps the department might consider taking to implement these technologies. We also note which technologies already exist and how different private and government actors have invested in them.

Trusted Repeater Stage

At the first stage of the development of the quantum Internet, the Internet continues to transmit only classical information; however, it could do so more securely by incorporating quantum repeaters into the existing infrastructure. At this stage, a pair of quantum repeaters requires only the ability to perform a single quantum protocol, namely quantum key distribution (QKD; see figure 1). This protocol allows for the generation of a secret key that is securely distributed to adjacent quantum repeaters.[9] A classical message could then be encoded at one repeater, securely transmitted to the next repeater, and finally decoded. This process could be carried out between each pair of consecutive repeaters, each generating a new secret key, ensuring the transmission of the classical message from source to destination by chaining together multiple repeaters. The term *trusted repeater* stems from the requirement that the message be decodable at each repeater. Hence, secure transmissions rely on the trustworthiness of the sequence of repeaters. The advantage of sending information this way is that the security of the message is guaranteed between repeaters, even in the presence of an eavesdropper. The message could not be decoded without the secret key, and the security of the distribution of the secret key between repeaters is guaranteed by the laws of quantum mechanics rather than the computational difficulty of the decryption process. In other words, an intercepted message could not be decoded except by guessing the key, now or in the future, even with the aid of a powerful computer or even a quantum computer.[10]

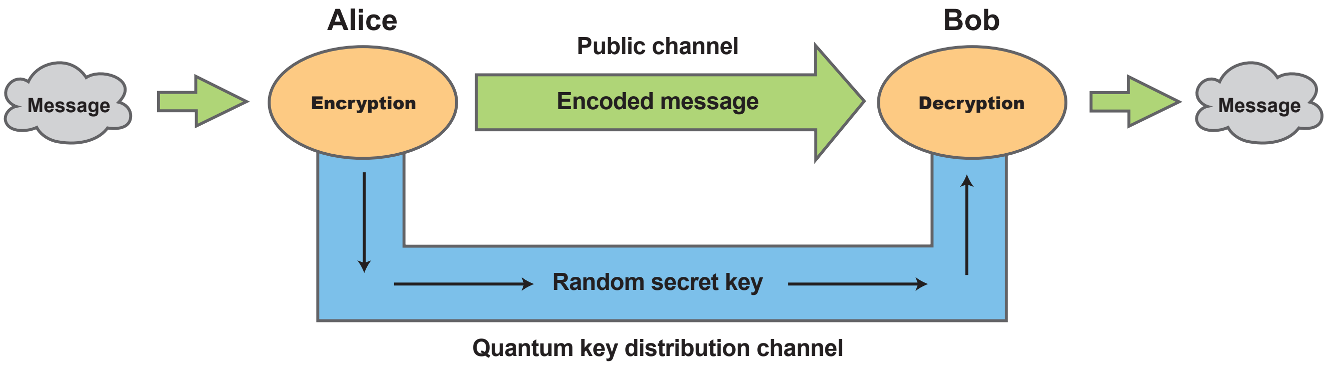
Investment in the trusted repeater stage is critical for DOD as it promotes secure communications that overcome traditional adversarial interception techniques. Military application of this stage would enable geographically separated commanders and subordinates to communicate operational details without concern of interception. This state provides an increase in battlefield overmatch capacity and might also promote a defeat in traditional direction-finding, a method of intercepting communication paths to track the originator's location or signal intercept techniques. This stage would also alert those in the communication chain of attempts to access those secure transmissions, thus "sounding an alarm" so appropriate action can be taken to prevent further interception efforts. Ultimately, increasing security, defeating interception, and reducing or eliminating transmitter detection allow a commander and his or her forces a more secure environment and offer a greater chance of success.

If DOD focuses on increasing capacity for trusted repeaters, it might also promote more secure intelligence transmission in deployed environments rather than rely on traditional intelligence networks. Traditional intelligence transmission techniques depend on complex secure networks that can be arduous in combat operations. Although an option to communicate intelligence through traditional means exists, such methods often require encryption, dedicated transmission channels, and considerations for the use of coded words or values—all of which delay receipt of intelligence. This impediment could be detrimental to a commander's decision-making cycle, upsetting the efficacy of intelligence while potentially forcing decisions without essential information. A quantum Internet with trusted repeaters, however, could provide the necessary expeditious and secure intelligence transmission environment that commanders would need in a combat environment.

Prepare-and-Measure Stage

At the second stage of the quantum Internet, the Internet can prepare a single qubit at an initial node and transmit it to a final node where it could be measured. This is the first stage at which the Internet could truly be considered *quantum*, in the sense that it is now able to transmit information in the form of qubits. It is important to note that successful qubit transmission is not likely at this stage. Because of the potential for a qubit to be lost, the receiver must detect whether the qubit has been received before measuring it; hence, all measurements are "postselected" on the knowledge that the qubit was successfully transmitted. The requirement to detect successful transmission implies some limitations on the set of protocols that could be performed, as any measurement of the qubit necessarily perturbs its state.[11] Nonetheless, even the ability to transmit qubits in this imperfect way makes possible important protocols, such as end-to-end QKD, without reliance on trusted quantum repeaters.[12]

Figure 1. Quantum Key Distribution



Colonel Timothy Lawrence, director of Air Force Research Laboratory (AFRL)'s Information Directorate, speaks during virtual Million Dollar International Quantum U Tech Accelerator event, September 1–3, 2020, in Rome, New York, where AFRL's Air Force Office of Scientific Research later awarded 17 quantum information science grants (U.S. Air Force)

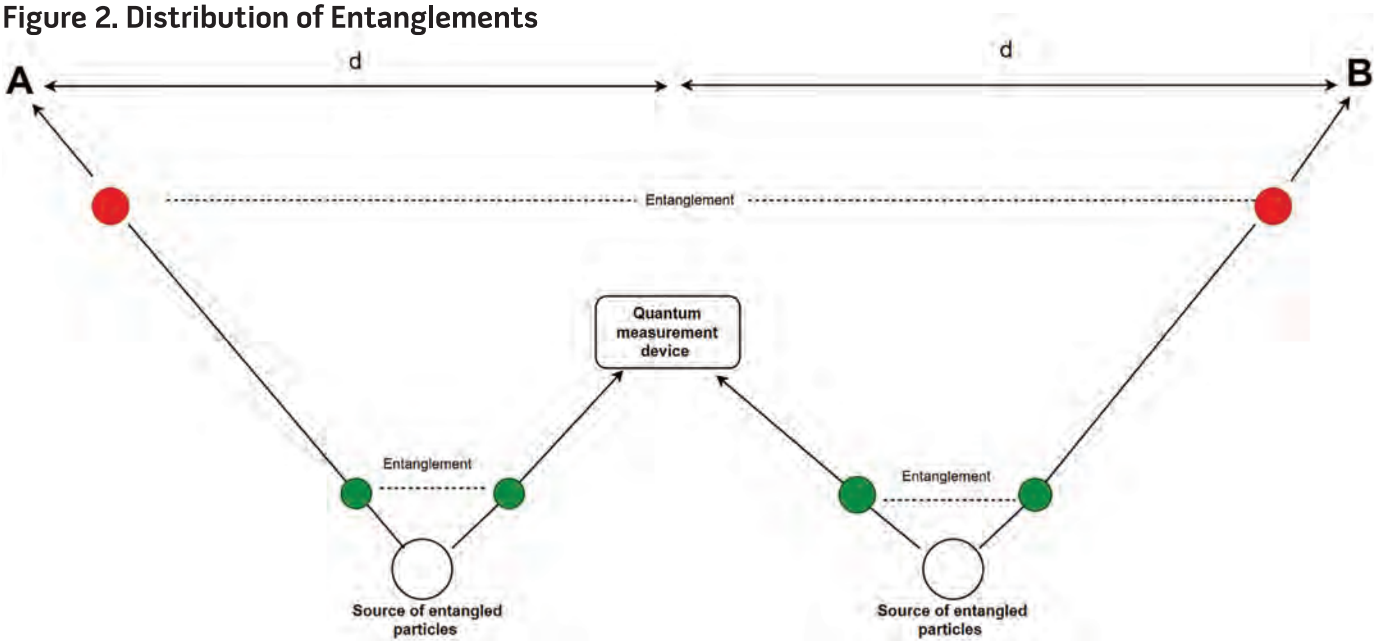
The prepare-and-measure stage requires DOD to realize the limitations of quantum transmission and the investment necessary to ensure a secure quantum Internet. The United States is falling behind China in efforts to capitalize on quantum technology, placing China on a path to achieve initial success in the realm of a quantum Internet, quantum communications, and quantum sensing. China is investing in its quantum military efforts, already claiming success in qubit transmission among Shanghai, Beijing, and other cities, via a land network of approximately 750 miles.[13] Although this achievement does not specifically indicate a successful demonstration of a quantum Internet, it does highlight that China is making gains while DOD and the U.S. Government are focusing primarily on quantum computing developments that do not fully advance the infrastructure necessary for a quantum Internet.

This second stage further establishes the principles of quantum sensing and its utility on the battlefield, as tactical surprise can set the stage for success in military operations. The concept of quantum sensing in this stage is possible when assessing perturbations in the quantum state. A quantum radar, such as the one Jonathan Baugh is developing at the University of Waterloo, in Canada, measures quantum states in a microwave beam and looks for anomalies in those states.[14] In military usage, the precision in quantum measurements would allow immediate and specific detection of combat assets, including problematic examples such as a stealth fighter or a submarine. The first military to develop such a radar will increase the effectiveness of its early-warning and target acquisition; therefore, the United States must reach quantum supremacy before its adversaries do.

Entanglement Generation Stage

At the third stage of development, the Internet can generate a pair of maximally entangled qubits and distribute them—one to node A and another to node B. This process must succeed with nearly unit probability. This stage bypasses the postselection requirement of the previous stage and enables a greater variety of protocols to be carried out between node A and node B. This stage could be implemented using true quantum repeaters, which function by receiving a qubit, entangling it with another, and passing the second qubit along (see figure 2). This "daisy chain" of entangled qubits results in the distribution of entanglement between the initial and final nodes of the chain.[15]

Figure 2. Distribution of Entanglements


A
d
d
B
Entanglement
Quantum measurement device
Entanglement
Entanglement
Source of entangled particles
Source of entangled particles

Successfully distributed entangled qubits allow nodes to transmit qubits securely using a process called *quantum teleportation*. In addition, new and more secure forms of QKD could now be carried out between the end nodes, and the security of these new QKD protocols would no longer require end users to trust even their own measurement devices,[16] increasing their security.

At this stage, DOD could start to realize instantaneous communication regardless of the capacity of data flow, a critical component to promote military superiority via a more coordinated and immediate information environment. Dominance in the operational environment centers on forces, weapons, and systems that can maneuver, react, defend, and destroy at the time and space of a commander's choosing—and the surety of communications systems. At the entanglement generation stage, commanders have access to end nodes that allow secure and nearly instant transmissions, providing an edge to their forces with immediate synchronization of effort; this is especially true when simultaneous nonkinetic and kinetic effects are required to achieve a particular objective, as timing becomes critical through exercising instantaneous, uninterrupted communication. These issues showcase the urgency of investment and research in achieving a capable quantum Internet.

Quantum-Memory Stage

The next stage is crucial for a large quantum network to be possible. The main difference between this stage and the previous one is that at this newer stage multiple qubits can move from one network node to another. Quantum memory allows for a network to be established one state at a time, storing the quantum states as they are received from the network. This approach makes sending larger quantum states by quantum teleportation possible, which increases the volume of quantum information that can be transmitted. Moreover, at this stage, quantum clock synchronization and quantum anonymous transmission become feasible via a multiparty entanglement system.[17] Entanglement and quantum communication ensure that time signatures across multiple parties are authentic, improving the security of communication transmissions.[18]

The military would benefit from an advancement at this stage through more precision in clock synchronization, maximizing its ability to further achieve simultaneous operations during large-scale conflicts beyond what is accessible with the previous stage's communication gains. Clock synchronization translates into exactness in both time alignment and GPS fidelity—crucial components for achieving military objectives in both time and space. The Defense Advanced Research Projects Agency notes the potential for improvement with quantum synchronization, which could increase efficiency from a billionth to a trillionth of a second.[19] This gain may seem inconsequential, but any increase in accuracy could mean the difference between success and defeat on the battlefield. Major Matthew Myer highlights this point well from an infantry perspective. As ground troops rely on air platforms to defeat the enemy in close missions—missions that may create incidents of fratricide due to the proximity of enemy and friendly forces—pilots must often change tactics and weapons systems to accommodate.[20] Every individual relying on lifesaving measures or the availability of a weapons system appreciates any increase in accuracy and timeliness.

Few-Qubit Fault-Tolerant Stage

A fault-tolerant design enables a system to continue its intended operations, possibly at a reduced level, rather than failing completely when only some part of a system breaks. The term *few qubits* here refers to the fact that the number of qubits available is still small enough that the end nodes themselves could be simulated on a classical computer.[21] Nevertheless, a classical computer may be unable to simulate the entire network. Reliable qubits are diffcult to engineer, but standard fault-tolerance schemes exist that use seven or more physical qubits to encode each logical qubit, with still more qubits required for error correction.[22] The large overhead makes testing fault-tolerance schemes with multiple encoded qubits difficult. Access to fault-tolerant gates makes possible more accurate clock synchronization as well as distributed quantum computing—that is, a network of quantum computers interconnected by quantum and classical channels. Because quantum computers are interconnected by quantum channels, users could leverage the entanglement required to obtain an increase of computational power. Moreover, small quantum computers linked by quantum connections could be a stepping-stone to future large-scale quantum computers. Even in this limited scenario, it might be feasible for users to perform computations at speeds not currently possible with quantum computers, as researchers working on Google's machines recently demonstrated.[23]

A fault-tolerant design could provide DOD with a viable quantum network on which it could rely in a satellite-denied environment, so that forces could continue to execute operations despite any adversary's effort to defeat the military's satellite connectivity. The Pentagon realizes this scenario as a realistic vulnerability and understands the benefits that quantum provides in overcoming it; however, DOD's investment in maturing

Marine with Charlie Company, 8th Communication Battalion, conducts radio communication check during Exercise Cyber Fury 21, at Camp Lejeune, North Carolina, July 26, 2021 (U.S. Marine Corps/Armando Elizalde) this technology is only a fraction of the budget China, another quantum giant, has dedicated to quantum development.[24] Therefore, to realize this stage and achieve a fault-tolerant design durable enough to survive the brutal conditions on the front lines of combat, DOD must continue to promote expertise in quantum computing and networking through initiatives such as the Million Dollar International Quantum U Tech Accelerator, a Navy and Air Force event that reviews pitches from experts competing for contracts to develop future quantum capabilities for DOD, while also promoting collaboration, innovation, and training in these technologies.[25]

Quantum Computing Stage

This ultimate stage allows for the realization of all protocols. These protocols, among many others, would deliver secure communication, secure login networks, quantum-enhanced GPS, secure voting, quantum digital signature, gravitational wave detection, and so forth. But having a full-fledged quantum computer at the end of each node has both advantages and risks. One of the main risks is the breaking of cryptography as it currently exists. Shor's algorithm solves the discrete logarithm problem by using a quantum computer to factor a large integer.[26] With the advent of such quantum algorithms, as well as quantum computers, and a quantum Internet, an adversary could efficiently break the universally adopted public key cryptosystem schemes (for example, RSA, DSA [digital signature algorithm], and ECC [elliptic-curve cryptography]) that rely on the computational difficulty of such factoring problems.

If DOD achieves the quantum computing stage first, it could take advantage of each of the previous stages while also having access to a system of quantum computers that could provide the level of analysis commanders need to succeed in any operational environment. A full-fledged quantum Internet means immediate access to quantum systems across

U.S. Cyber Command Cyber National Mission Force members participate in training and readiness exercise at Fort George G. Meade, Maryland, May 24, 2021 (U.S. Army/Josef Cole) the Internet, thus offering immense computing power to analyze all possible data points that commanders have available to aid in the decision cycle. A quantum computer could pinpoint the best possible solution faster than could any classic computer. Moreover, the potential problem sets quantum computers can solve are still unfathomable, which means the power of these computers to aid on the battlefield, in real time, could change the character of war in ways we still do not understand. However, the success of the U.S. Armed Forces in the quantum environment is possible only if DOD elects to invest in the quantum Internet now.

DOD and other stakeholders should regard the development of the quantum Internet as a process that will occur over several stages, rather than as a single entity that will appear once quantum computing becomes feasible. By tracking and analyzing how the quantum Internet develops stage by stage, DOD could remain in step with technological advances of state and private actors and thus be better prepared for the eventual emergence of quantum computing. Conversely, ignoring this development and only countering the eventual emergence of a quantum computer, by investing in postquantum technologies, would put DOD at a disadvantage compared with other state and private actors. JFQ

Notes

[1] Richard P. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics* 21, nos. 6/7 (June 1982), 467–488.

[2] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings: The 35th Annual Symposium on Foundations of Computer Science* (Washington, DC: Institute of Electrical and Electronics Engineers, 1994), 124–134.

[3] "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," National Institute of Standards and Technology Call for Proposals, December 20, 2016, available at <https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms>.

[4] Stephanie Wehner, David Elkouss, and Ronald Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science* 362, no. 6412 (2018), available at <https://science.sciencemag.org/content/362/6412/eaam9288.full>.

[5] Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, December 1, 2020), IV-6.

[6] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, UK: Cambridge University Press, 2000).

[7] Richard Jozsa et al., "Quantum Clock Synchronization Based on Shared Prior Entanglement," *Physical Review Letters* 85, no. 9 (August 2000), 2010–2013, available at <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.2010>.

[8] Wehner, Elkouss, and Hanson, "Quantum Internet."

[9] Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science* 560 (2014), 7–11. Originally published as Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *International Conference on Computers, Systems & Signal Processing*, vol. 1 of 3 (Bangalore, India: Institute of Electrical and Electronics Engineers, December 1984), 175–179, available at <https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>.

[10] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus, "The Case for Quantum Key Distribution," in *Quantum Communication and Quantum Networking*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 36, ed. Alexander Sergienko, Saverio Pascazio, and Paolo Villoresi (Heidelberg, Germany: Springer, 2010).

[11] Nielsen and Chuang, *Quantum Computation and Quantum Information*.

[12] Charles H. Bennett and Stephen J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," *Physical Review Letters* 69, no. 20 (November 1992), 2881–2884.

[13] Tom Stefanick, "The State of U.S.-China Quantum Data Security Competition," *Brookings*, September 18, 2020, available at <https://www.brookings.edu/techstream/the-state-of-u-s-china-quantum-data-security-competition/>.

[14] Martin Giles, "The U.S. and China Are in a Quantum Arms Race That Will Transform Warfare," *MIT Technology Review*, January 3, 2019, available at <https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/>.

[15] Nicolas Sangouard et al., "Quantum Repeaters Based on Atomic Ensembles and Linear Optics," *Reviews of Modern Physics* 83, no. 1 (2011), 33–80.

[16] Umesh Vazirani and Thomas Vidick, "Erratum: Fully Device-Independent Quantum Key Distribution," *Physical Review Letters* 116, no. 8 (February 2016).

[17] Jozsa et al., "Quantum Clock Synchronization."

[18] Howard Barnum et al., "Authentication of Quantum Messages," in *Proceedings: The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002* (Washington, DC: Institute of Electrical and Electronics Engineers, 2002), 449–458.

[19] *Quantum Sensing and Computing: Advancing National Security Through Fundamental Research* (Washington, DC: Defense Advanced Research Projects Agency, n.d.), 2, available at <https://www.darpa.mil/attachments/QuantumSensingLayout2.pdf>.

[20] Matthew R. Myer, "Danger Close: Calculating Risk Within the 'Last 100 Yards,'" *Infantry Online*, 2013, available at <https://www.benning.army.mil/infantry/magazine/issues/2013/May-June/Myer.html>.

[21] Maarten Van den Nest, "Classical Simulation of Quantum Computation, the Gottesman-Knill Theorem, and Slightly Beyond," *Quantum Information & Computation* 10, no. 3 (March 2010), 258–271.

[22] Peter W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," *Physical Review A* 52, no. 4 (October 1995), R2493–R2496, available at <https://www.cs.miami.edu/home/burt/learning/Csc670.052/pR2493_1.pdf>.

[23] Frank Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature* 574 (2019), 505–510, available at <https://doi.org/10.1038/s41586-019-1666-5>.

[24] Jon Harper, "Pentagon Trying to Manage Quantum Science Hype," *National Defense*, December 10, 2020, available at <https://www.nationaldefensemagazine.org/articles/2020/12/10/pentagon-trying-to-manage-quantum-science-hype>.

[25] Ibid.

[26] Shor, "Algorithms for Quantum Computation," 124–134.