IBM Quantum Scientist Dr. Maika Takita, in Thomas J. Watson Research Center IBM Quantum Lab, September 10, 2020 (Courtesy IBM/Connie Zhou)

Quantum Computing
A New Competitive Factor with China

By Doug Quinn, Patrick Wolverton, and Scott Storm

On May 7, 2021, cyber terrorists used ransomware to cripple the Colonial Pipeline, which provides nearly half of the gasoline and jet fuel supplies to the U.S. East Coast.[1] The effects of this attack were felt by millions of Americans over the next few weeks, as nearly 12,000 gas stations reported being completely empty.[2] Four days later, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint cybersecurity advisory out of concern that the ransomware effort could spread to other critical infrastructure sectors such as manufacturing, legal, insurance, healthcare, and energy.[3]

Imagine a future in which malign actors or strategic competitors of the United States have harnessed a more capable means, *quantum computing* (QC), that can break through cyber security measures once thought almost impossible to breach. In that future, China mounts a whole-of-society effort that leverages the entirety of its government, academia, and industry to outpace the rest of the world in developing a versatile QC capability. Without a similar approach to mitigate these threats, the United States and its

Commander Doug Quinn, USN, is a Contract Specialist in the Naval Sea Systems Command at the Washington Navy Yard. Lieutenant Colonel Patrick Wolverton, USAF, is Deputy Chief of Staff at U.S. Cyber Command J2. Lieutenant Colonel Scott Storm, USAF, is Cognitive Models Branch Chief at the 711th Human Performance Wing.

John Tenniel illustration from Lewis Carroll's *Alice's Adventures in Wonderland* of Alice playing croquet with a flamingo and a hedgehog (Courtesy Alice-in-Wonderland.net) allies will find it harder to protect vulnerable information systems, compromising their pursuit of national and global interests. The winner in the race to develop quantum-based technology will have the potential to shape the world in ways that can hardly be imagined today—for better or worse. The application of quantum technologies has the potential to reshape the national security landscape.

Future advancements in QC will increase the level of this *present* threat. “The potential for harm is enormous. If these encryption methods are broken, people will not be able to trust the data they transmit or receive over the Internet, even if it is encrypted. Adversaries will be able to create bogus certificates, calling into question the validity of any digital identity online,” states Dorothy Denning, a distinguished cyber security expert with more than 50 years of experience in computer sciences and cyber threats.[4] However, Dr. Denning also notes that researchers are currently working to find ways to mitigate this threat to data encryption.[5] The application of quantum technologies has not only the potential to protect or disrupt global information but also the power to decide which nation will be the world’s foremost superpower of the 21st century.

What Is “Quantum” All About?

Quantum theory gives us our best account of nature in the realm of the very small in which particles behave in ways that can seem unnatural. Albert Einstein once colorfully dismissed quantum mechanics as “spooky action at a distance”; however, over the past few decades, physicists have successfully demonstrated the reality of this spooky action.[6] If quantum physics was adapted into a fictional children’s story—Alice’s Adventures in Quantum Wonderland, perhaps—we could more plainly express what may seem so unnatural or spooky. This fictional children’s story would include quantum principles such as superposition, entanglement, multiplicity, and decoherence.

Superposition describes the fact that quantum particles are in many states *at once* and, interestingly, until the particle is observed. The state of the particle is best described as a superposition of all those possible states.[7] If we were reading Alice’s Adventures in Quantum Wonderland, Alice would be everywhere at once—she would be on the riverbank, falling down the rabbit hole, questioning her identity to the blue caterpillar, and arguing with the King and Queen of Hearts all at the same time. However, only when the King and Queen of Hearts observe Alice does she become fixed in a particular state or situation. This version—Alice’s Adventures in Quantum Wonderland—is truly stranger than fiction.

Entanglement is what Einstein was referring to as “spooky action at a distance.” Entanglement links certain quantum particles so that the quantum state of each particle of the group cannot be described independently of the state of the other particle(s), and entanglement can occur over long distances. In the case of Alice’s Adventures in Quantum Wonderland, imagine having the homonym, homophone, homograph, and heteronym words in the book shift states, as these words are “entangled” in the story. Just as the reader can derive the true meaning of the word, physicists can derive the states of entangled quantum particles wherever those words appear in the story. Now that is a spooky action at a distance.

Multiplicity is a phenomenon that allows quantum computers to store a multiplicity of quantum states simultaneously, while classical digital computers can store only one state at a time, or can store many states but in different memory locations. Alice’s Adventures in Quantum Wonderland is a multiple-ending story with many possible outcomes. The reader is never permitted to read all the chapters in one sitting, but over time the reader can document the many different possible endings, resulting in a great appreciation for the complexity of the characters.

Decoherence occurs when quantum bits (qubits) fall out of a state of superposition.[8] The volatility of qubits can cause data to be lost or altered, which can significantly reduce the accuracy of computational results. The White Rabbit in Alice’s Adventures in Quantum Wonderland experiences decoherence whenever he attempts to read his pocket watch, at which point the watch stops. In this story the White Rabbit mutters, “Oh dear! Oh dear! I’ve lost the time!” This causes the White Rabbit to “lose” any information regarding the time of day, and he therefore has no appreciation for being late to his duties as herald to the King and Queen of Hearts. In this version of the story, he gladly stops to help Alice after she arrives in Quantum Wonderland and assists her in getting home. This greatly alters the story and makes it highly inaccurate when compared to the original *Alice’s Adventures in Wonderland*.

How Is QC Different?

Most people are familiar with the binary units (1s and 0s) used by classic computer processors. While modern computers use bit processors, QC uses qubit processors with hundreds or even millions of potential combinations, making them ideal for complex computations. The state of qubits does not necessarily reside on either side of the binary spectrum but exists in *both* states through the principle of superposition.[9] The figure illustrates how superposition introduces immense potential within the field of QC, as the qubits exist in a coherent superposition. A qubit does not have a set value between 0 and 1; rather, qubits have a probability of 0 and a probability of 1. A qubit can be in a combination of *both* states—resulting in enormous processing potential. So how does the processing power of one qubit compare to one bit? It is more a matter of how additional qubits scale. Each additional qubit *doubles* the processing power. For example, three qubits provide 2^3 processing power. Sixty-four qubits provide about 1 million terabytes of processing power—or 18,446,744,073,709,600,000 possibilities.[10]

Engineering the qubit today has been compared to the early days of the bit, and ordinary computers, in the 1950s.[11] Variations in the design of qubits under development reflect the nascent state of QC. By taking advantage of quantum principles, scientists can use new

Scientists perform calculations on "Taiyuan-1" superconducting quantum computing cloud platform, at Hangzhou International Science and Innovation Center of Zhejiang University, in Hangzhou, Zhejiang Province, July 22, 2022 (Alamy/Cynthia Lee)

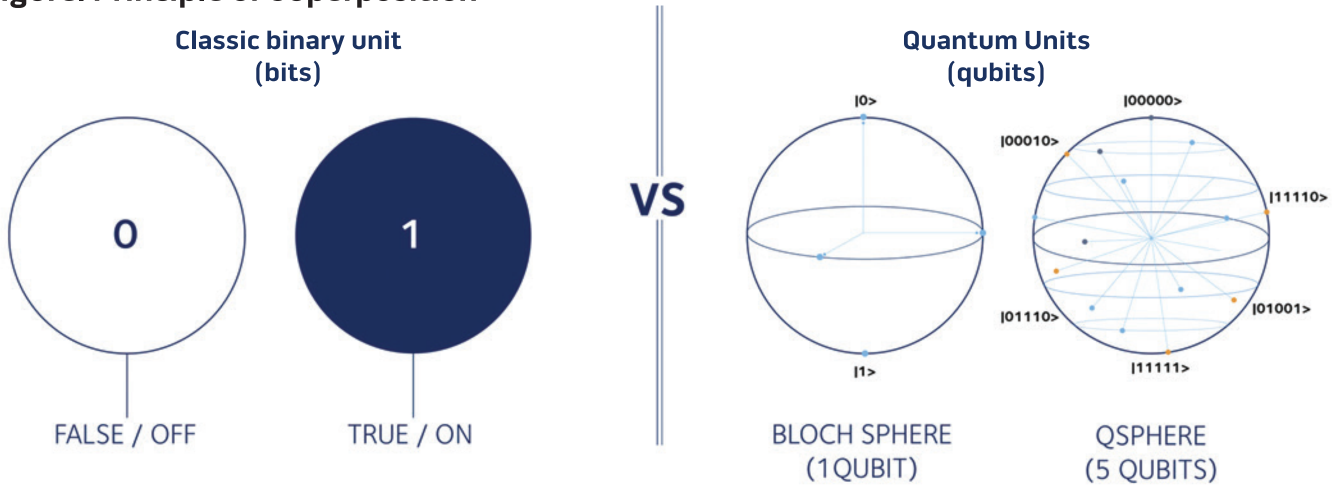
algorithms to solve complex problems exponentially faster than even the most advanced super computers in operation.[12]

Potential Applications

When discussing applications of quantum technologies, it is critical to note that nearly all existing demonstrations of quantum applications have occurred in highly controlled laboratory environments and that the success of these tests is not indicative of any near-term potential for commercial or government application. Conceptually, future implementation of quantum mechanics in modern technology will introduce robust real-world applications with significant utility to any agency or commercial entity with the means to procure quantum technologies.

Entire fields are taking shape, aimed at leveraging advancements in technology based off quantum principles. In theory, the strength of quantum technologies is rooted in the timely calculation of complex, large-scale combinatorics problems.[13] While the list of potential quantum applications is limited compared to the applications of classical computers, quantum applications

Figure. Principle of Superposition



Source: Alexander Fletcher, "Quantum Computing & Financial Technologies," LinkedIn, April 30, 2019.

are growing and evolving as industry continues to uncover computational problem sets that lend themselves to complex combinatorics. Cyber security, advanced materials research, logistics optimization, and weather forecasting all demonstrate promising advancements with Department of Defense (DOD) applications.[14] QC is being developed and tested for applications that will better enable accurate modeling, more complex and simultaneous simulations, more accurate analysis of probabilities, and tackling machine learning and artificial intelligence (AI)–focused problems.[15]

Private Sector and Educational Institution Investment

The list of U.S. companies investing in quantum research is extensive. Spending on quantum computers should reach hundreds of millions of dollars in the 2020s and tens of billions in the 2030s.[16] Household names such as Google, Microsoft, and IBM are examples of companies at the forefront of quantum development. Google AI Quantum is currently working to develop open-source tools and novel quantum algorithms that aim to accelerate machine learning and AI-related tasks.[17] Similarly, Microsoft has established a Quantum Team to address innovations in QC at what they deem "layers of the quantum stack."[18] This includes providing a collaborative cloud-based environment for quantum developers called Azure Quantum. Microsoft's Quantum network facilitates partnered quantum development with more than 20 companies and quantum education and research with more than 25 universities. Microsoft also provides a suite of online quantum learning tools to widen the aperture of quantum education. The IBM Quantum Network, made up of more than 100 Fortune 500 companies, universities, and national research laboratories, focuses on accelerated research and development (R&D) of commercial applications and education.[19] These three leaders in industry have taken a similar approach to their investment into quantum R&D. All three promote collaboration with industry and academia, development and distribution of open-source quantum tools, and a fundamental investment into education of the quantum sciences to promote a more capable workforce. U.S. private sector partnerships often cross national boundaries, and with academic institutions, further complicating what role DOD could or should play.

Quantum Supremacy: China vs. the United States

The term *quantum supremacy* is frequently used as a measure of milestone achievement in quantum technology development. Unlike the military definition, *supremacy* in a QC context refers to a quantum advantage over other systems rather than complete dominance. In October 2019, Google reported reaching quantum supremacy when a quantum computer with a stable 54-qubit processor exceeded the capacity of traditional computers.[20] The significance of Google declaring quantum supremacy has been widely debated. Critics claim that loosely structured tasks designed specifically to take advantage of quantum principles were used to declare quantum supremacy and that the task itself was not informative.[21] Proponents insist that the demonstration illustrates a general understanding of the system, and verification of the output data against the output from traditional systems indicates that the quantum computer is performing as intended. This proof-of-concept demonstration of quantum supremacy is

Table 1. Collaborative Development for Quantum Computing (Representative/Non-Exhaustive)

Companies Developing Quantum Hardware	Academic/Public-Sector Collaborators	Private-Sector Collaborators
IBM	University of Melbourne, Oak Ridge National Laboratory, University of Oxford, Los Alamos National Laboratory, National Taiwan University	JP Morgan, Goldman Sachs, Barclays, ExxonMobil, Samsung, Dupont, Daimler, Mercedes-Benz, Raytheon, Delta Airlines
Google	University of Waterloo, Oak Ridge National Laboratory, NASA, University of California Santa Barbara	Daimler, Volkswagen
Microsoft	Purdue University, Case Western Reserve University, Pacific Northwest National Laboratory, University of Sydney, Technical University of Copenhagen, Eindhoven University of Technology, University of California Santa Barbara, University of Sydney	Honeywell, Dow, Ford, 1QBit, Bohr Technology, Cambridge Quantum Computing, Entropica Labs, GTN, OTI Lumionics, ProteinQure, QC Ware, Qulab, QxBranch, Riverlane Research, Solid State AI, Strangeworks, and Zapata Computing
Intel	University of Toronto, University of Chicago, Delft University of Technology	
Biogen		Accenture Labs, 1QBit
D-Wave	University of Waterloo, Los Alamos National Laboratory, Oak Ridge National Laboratory	Google, Lockheed Martin, Volkswagen, Amazon Web Services, NEC Corporation
Honeywell		Microsoft, JP Morgan
Rigetti	University of California at Berkeley	Amazon Web Services
Alibaba	University of Science and Technology of China, Chinese Academy of Sciences	

a necessary early step toward developing more useful applications and attracting more investors.

While the incompleteness of open-source information makes it difficult to determine the current winner of the quantum race, a strong case can be made that China is leading the United States in the race for a global QC advantage. In a *Forbes* article titled "Quantum USA vs. Quantum China: The World's Most Important Technology Race," Paul Smith-Goodson notes, "One of China's main goals is to surpass the United States and to become the global high-tech leader. President Xi funded a multi-billion-dollar quantum computing mega-project with the expectation of achieving significant quantum breakthroughs by 2030."[22]

In March 2021, China released its latest five-year strategy, which called for increased investment in advanced technologies such as artificial intelligence and quantum computing. Despite its name, the strategy provides broad goals for China out to 2035, including a 7 percent boost in annual spending on advanced technologies. China hopes this additional R&D investment will create economic independence from the United States as well as bolster its national security. Furthermore, the Congressional Research Service notes, "China is developing strategic technologies and digital infrastructure (including a cryptocurrency) and aims to advance its digital infrastructure and domestic rules globally."[23] China's long-term approach to QC is apparent as seven of the top ten universities with QC patents ranked globally are Chinese.[24] While quantity does not indicate quality, it is worth noting that Chinese patents from quantum computing outpace the United States 1,657 to 1,439.[25]

In addition to the threat of China's own technological advances is the growing threat of the Chinese stealing intellectual property and data. China has increasingly stolen data from DOD and U.S. private industry over the past decade. In 2015, the National Bureau of Asian Research estimated the United States lost $1.2 trillion in revenue over 3 years as the result of Chinese counterfeiting, piracy, and stolen data.[26] Throughout 2018, the Department of Justice indicted Chinese intelligence officials and cyber actors for stealing secrets from U.S. aviation companies as well as intellectual property from other U.S. companies.[27]

Kari Bingen, former Principal Deputy Under Secretary of Defense for Intelligence, told a subcommittee of the House Armed Services Committee in 2018 that China has made it a priority to maliciously acquire foreign technologies, including those developed within the United States, to advance its economy and to modernize its military.[28] In one such example, as late as April 2021, the *Washington Post* reported that FireEye and CISA discovered there was reason to believe that sophisticated Chinese government hackers had infiltrated the information systems of dozens of U.S. Government agencies, defense contractors, financial institutions, and other critical sectors.[29] While the extent of the breach is still unknown, FireEye and CISA are already sending out alerts to those affected by the incidents. China's track record of stealing data from U.S. personnel and companies is clear and persistent, and the security of U.S. information systems will be at significantly greater risk with the fielding of QC technology. These unethical practices of stealing intellectual property give China an advantage over countries that continue to abide by international laws. In the race for quantum supremacy, taking unethical shortcuts may make the difference in who finishes first.

In December 2020, just over a year after Google declared quantum supremacy, a team of researchers from the University of Science and Technology in China declared that *they* had achieved quantum supremacy. The team developed a system called *Jiuzhang*, which manipulated light in the form of photons rather than the super-cold conducting metal used by the Google team. Jiuzhang produced results for its intended task in minutes, compared to the 600 million years it would have taken the world's most powerful supercomputer to complete.[30] The Chinese team, like Google, admitted Jiuzhang was designed only to compute this specific equation and nothing else.[31] Even though the scientific community has not verified the authenticity of this experiment and its results, it shows the potential for multiple paths to stabilizing qubits and achieving quantum supremacy.

Most experts assess it will take at least 10 to 20 years before the United States or China builds a mature or fully error-corrected QC capability.[32] China is not waiting for the United States to figure out how to build the best quantum computer. Its recent quantum supremacy announcement and increased spending on advanced technology are unsettling when coupled with their track record of stealing data and undermining U.S. interests.

Threats to U.S. Encryption

What would be the risk if China possessed a superior QC capability? DOD top secret networks are protected by a 256-bit Advanced Encryption Standard (AES). To crack this encryption, someone would need to try a maximum of 1.1 x 10^{77} different key combinations. To put this into perspective, the most powerful computer in 2017 was the Chinese Sunway TaihuLight. This computer, using brute force, would require 885 quadrillion years to crack a 128-bit AES encryption, which is less mathematically complex than the 256-bit AES. The world's most powerful computer would need more time than the universe has existed to try all number combinations.[33] Taking this into consideration, 256-bit AES is considered the gold standard and quantum resistant. For now, the consensus is that information protected by 256-bit AES is safe; however, unexpected leaps in quantum technological advancements could put the sovereignty of these systems at risk.

Another common type of encryption used by DOD is Rivest-Shamir-Adleman (RSA), which is an encryption method that uses two mathematically linked keys. A public and private key is often used with the DOD Public Key Infrastructure (PKI) and other common unclassified applications. Jon R. Lindsay, in *Strategic Strategies Quarterly*, discusses the mathematical application and security of RSA:

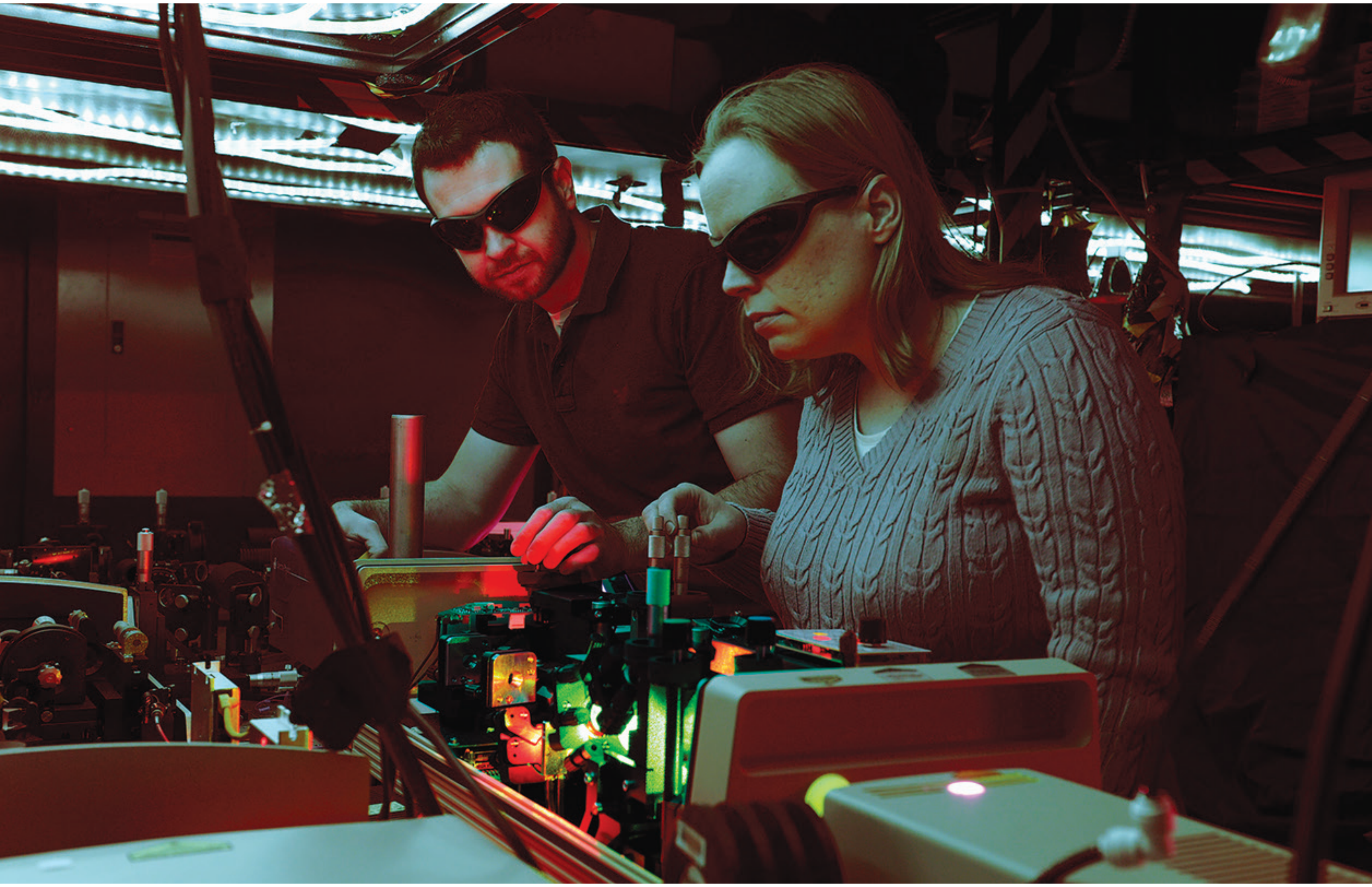
"Modern RSA works because the public key is based on an exceptionally large number (i.e., two to the power of 2048) while the private key is based on its prime factors. . . . A typical desktop computer would need more than six quadrillion years to crack 2048-bit RSA."[34] However, Peter Shor, an American professor of applied mathematics at MIT, may have changed the outlook on the security of RSA. In 1994, Shor developed a quantum algorithm that factors prime numbers for large numbers. Currently, this algorithm is limited by today's computers and their capabilities. If Shor's algorithm was coupled with the right capability, such as a quantum computer, then the DOD PKI would be at risk; some experts believe the encryption could be broken in a matter of hours. Jon A. Lindsay summarized it best when he stated:

> *An intelligence adversary with the right kind of machine could potentially break RSA, decrypt classified data, and forge digital signatures. All networks and applications on those networks, public and private, using vulnerable cryptography would be put at risk. Because military operations in all physical environments—land, sea, air, space—rely on many of the same information technologies and networks that power the global economy, a systematic vulnerability in the cyber domain would become a systematic vulnerability in all domains.*[35]

If China were to successfully create a quantum computer and use it with Shor's algorithm, it could create a catastrophic breach for DOD and other government agencies.

U.S. Federal Legislation and Governance

The significance of quantum technology has not been lost on the Federal Government. In 2015, an executive order launched the National Strategic Computing Initiative to advance U.S. leadership in high-performance computing, to include QC.[36] In 2018, the U.S. National Science and Technology Council, which coordinates the science and technology policy of the President, developed a National Strategic Overview for Quantum Information Science. Related to this announcement,



Researchers at Air Force Research Laboratory Information Directorate in Rome, New York, advance quantum technologies from individual quantum bit (or qubit) level to system level, January 16, 2015 (U.S. Air Force/Albert Santacroce)

Pleiades supercomputer at NASA Ames is one of many supercomputers used to find limit of quantum supremacy, April 10, 2015 (NASA/Ames Research Center/Dominic Hart)

the National Science Foundation and the Department of Energy (DOE) committed $249 million to 118 research projects related to quantum information science (QIS).[37] In 2019, Executive Order 13885 established the National Quantum Initiative Advisory Committee under the Office of Science and Technology Policy. The committee consists of a director and 22 members appointed by the Secretary of Energy. Committee members represent industry, universities, Federal laboratories, and other Federal agencies.[38] The National Quantum Initiative Advisory Committee facilitated the enactment of the National Quantum Initiative Act, which provides an investment mechanism through which the National Science Foundation, National Institute for Standards and Technology (NIST), and DOE can support R&D of quantum technology.[39] In response to the National Quantum Initiative Act, the DOE Office of Science launched multiple research programs in QIS with up to $625 million in funding over 5 years. This includes the standup of five national QIS research centers that focus on diverse collaborative QIS R&D, technology transfer, and development of the quantum workforce.

While research in many areas of quantum applications is still in its infancy, DOD has been exploring quantum military applications for the past 20 to 30 years.[40] Recently, the 2020 National Defense Authorization Act (NDAA) allows the secretary of each military Service to "establish or designate a defense laboratory" and mandates that the "Secretary of Defense shall ensure that no less than one such laboratory or center is established or designated."[41] The Air Force and Navy have since established laboratories dedicated to quantum information sciences and QIS-enabled technologies and systems.[42] The 2020 NDAA also asks for the Secretary of Defense to submit a report by the end of 2021 to the congressional defense committees on "current and potential threats and risks posed by quantum computing technologies." The report provides recommendations on how to counter any risks posed by quantum technologies.[43] In early 2022, the Office of the Under Secretary of Defense for Research and Engineering released a memo outlining a technology strategy that will "chart a course for the [U.S.] military to strengthen its technological superiority amidst a global race for technological advantage." Quantum science is identified as one of 14 critical technology areas vital to maintaining national security.[44] Congressional leaders are also taking action to ensure that the country's scientific workforce is prepared to address the emerging quantum threat. In a recent bipartisan effort, legislation proposed in the Senate aims to streamline the DOD and private sector hiring pipeline for students graduating with degrees related to the quantum sciences.[45] If passed, this legislation would signify a large U.S. investment in its future quantum intellectual capital.

Other key quantum technology stakeholders within the Federal Government include the National Aeronautics and Space Administration (NASA) and the Department of Commerce. NASA's Quantum Artificial Intelligence Laboratory collaborates with multiple hardware development and research groups such as Google to conduct tests on near-quantum computing hardware, with the goal of evaluating the potential of quantum computing capabilities.[46] The Department of Commerce, through

NIST, is also deeply invested in quantum research. NIST conducts quantum-based research through partnerships with academic institutions. One such effort is the Joint Quantum Institute, a collaborative research endeavor among the University of Maryland, NIST, and the Laboratory for Physical Sciences, which conducts research in the fields of quantum computing, quantum many-body physics, and quantum control, measurement, and sensing.[47]

President John F. Kennedy's national priority of beating the Soviets to the moon may be comparable to the current race against China to harness the potential of the quantum, though not nearly as well recognized by the public. Each milestone reinforces global dominance and undoubtedly unlocks potentially disruptive technologies to national and global economies. The U.S. Government requested $844 million for quantum information science R&D in fiscal year (FY) 2023, which is an 8 percent decrease from FY2022.[48] When compared to the space race in the 1960s, the United States similarly spent $903 million on the Apollo and related programs in 1960 (adjusted for inflation in FY2020).[49] Spending on the Apollo and related programs then peaked in 1965 at $40.9 billion—48 times greater.

Recommendations

Since 1989, U.S. military strategy has been defined in terms of ends, ways, and means, which provides a framework for military strategy and offers a lens for subsequent types of planning.[50] This same approach can be used to establish a simple yet effective strategic framework for quantum technology development and integration into DOD systems.

The end (that is, what the objective is) for DOD when it comes to QC is mitigating the potential threats to the homeland enabled by quantum technological advancements. Since China is already invested heavily in quantum technologies with a long-term outlook, DOD should assume that QC poses a long-term threat to homeland defense. The end includes a mature, secure, and profitable QC industry that benefits society in various ways that justify the investment.

The way (how the objective will be achieved) is an engaged and informed DOD and Federal Government that will mitigate the threat and better enable the United States and its allies to achieve a quantum advantage over its adversaries. The United States and its allies must develop a reliable and robust QC capability and the knowledge of how to harness that capability before the Chinese establish a true quantum advantage. DOD must efficiently and effectively integrate with industry and academia into a whole-of-society approach to quantum innovation that promotes intellectual synergy, while simultaneously ensuring that these efforts align with national security interests. DOD should continue to actively pursue collaboration with other government agencies, the private sector, academic institutions, and its allies and constituents abroad. These partnerships will enable DOD to advocate for government collaboration on projects with an increased focus on protecting advances in quantum R&D from habitual thieves of U.S. intellectual property. These partnerships will allow DOD to shepherd targeted research toward areas advantageous to national security and homeland defense while allowing companies in the private sector autonomy on projects not directly tied to DOD. Moreover, the ways can be achieved via well-informed organizations with common goals that underlie national defense.

DOD also needs to examine challenges within its own acquisition processes to remain ahead of the pacing quantum threat.[51] In January 2020, DOD established the Adaptive Acquisition Framework in DOD Instruction (DODI) 5000.02, which affords program managers the flexibility to tailor an acquisition between six different acquisition pathways.[52] Tailoring pathways for specific requirements is intended to better allow for more timely and less costly acquisitions. While such policy changes are laudable, DOD should provide specific guidance regarding the acquisition of quantum-based technologies in a future iteration of DODI 5000.82, *Acquisition of Information Technology*, as quantum-based technologies will present unique challenges to the acquisition process and will likely prove disruptive to established technologies.

Federal Government programs that support technological innovations and expedite critical acquisitions may not sufficiently target DOD challenges with quantum-based technologies. The Small Business Innovation Research and Small Business Technology Transfer programs are targeted at innovation but are limited to small businesses and have contract thresholds that likely exclude many of the large businesses that are already heavily invested in QC R&D. Sole-source contracts are intended to reduce the acquisition timeline by excluding competition in certain circumstances. Per the Federal Acquisition Regulation, a sole-source contract may be awarded if the supply or service "demonstrates a unique and innovative concept or demonstrates a unique capability of the source to provide the particular research services proposed."[53] However, there is no obligation for the company to enter a contract with DOD. Furthermore, any company would have an incredible amount of negotiating leverage over DOD as that technology becomes more viable and potentially a threat to homeland defense. Awarding contracts in a timely manner and efficiently (when most needed) to compel advancements in quantum computing will be essential for the Federal Government and DOD.

The primary means (the resources necessary to implement the strategy) for DOD is earmarked funding and, to a lesser degree, dedicated manpower. DOD must have sufficient funding to advance QC. Targeted funding for R&D could result in effects that are advantageous to U.S. national security and the national economy. U.S. spending on QC should be benchmarked as a percentage of gross domestic product and tied to spending by the Chinese at a minimum. The threat to homeland defense also necessitates dedicated DOD manning for addressing QC challenges now. While a whole-of-society approach has begun for DOD, QC will eventually necessitate a restructuring of command and control. The National Security Agency and its partners U.S. Cyber Command, U.S. Northern Command, and CISA are best equipped to address QC risks based on their information mission sets. Quantum research in the field of cyber security is a particular area of interest and investment for DOD. While DOD is heavily invested in its broadly defined role within the larger National Quantum Initiative, dedicating money and intellectual capital to an R&D effort that focuses on cyber security challenges of quantum within the realm of DOD cyber infrastructure is paramount to the maintained sovereignty of critical information systems.

Conclusion

Some of America's brightest minds are actively researching the vast potential of quantum computing. DOD is likely going to play an essential role within the field of QC, and projected spending indicates that role will increase going forward. The DOD role in developing state-of-the-art technologies ensures that the commercialization of QC will be heavily influenced by the agency. Unlike its counterparts in the private sector and academia, DOD has a defined obligation for defense of the homeland, as stated in the National Security Strategy and National Defense Strategy.

Falling behind other nations will significantly increase security risks to the United States, not the least of which is the compromise of U.S. public or private information systems via malign cyber attacks. This threat necessitates that DOD increase its role in emerging QC technologies, including those related to quantum cryptography and nonquantum technologies considered quantum resistant. In a worst-case scenario, China prioritizes quantum technology R&D more than the United States, continues to invest heavily, and achieves a quantum advantage independently, leaving the United States behind.

While the consensus within the scientific community is that mature (or fully error-corrected) quantum computers are a decade or more from realistically becoming a threat to the United States, DOD must actively remain engaged to accurately assess risks. The U.S. Government, private sector, national laboratories, and academic institutions have already invested significant time and funding to address the quantum challenge in a collaborative environment; however, DOD's role must be better aligned with the strategic risks to homeland defense. Failure by DOD to fully understand the strategic landscape or to delay seizing the initiative within the field of quantum computing will result in a disadvantage that the United States cannot afford. **JFQ**

Notes

[1] Aaron Gregg, Sean Sullivan, and Stephanie Hunt, "As Colonial Pipeline Recovers from Cyberattack, Leaders Point to a 'Wake-Up Call' for U.S. Energy Infrastructure," *Washington Post*, May 13, 2021, https://www.washingtonpost.com/business/2021/05/13/colonial-pipeline-ransomware-gas-shortages/.

[2] Will Englund and Ellen Nakashima, "Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations," *Washington Post*, May 12, 2021, https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/.

[3] "Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware," Cybersecurity & Infrastructure Security Agency, May 11, 2021, https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware.

[4] Dorothy E. Denning, "Is Quantum Computing a Cybersecurity Threat?" *American Scientist* 107, no. 2 (March–April 2019), 83–85, https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat.

[5] Ibid.

[6] Gabriel Popkin, "Einstein's 'Spooky Action at a Distance' Spotted in Objects Almost Big Enough to See," *Science*, April 25, 2018, https://www.sciencemag.org/news/2018/04/einstein-s-spooky-action-distance-spotted-objects-almost-big-enough-see.

[7] Scott Buchholz et al., "The Realist's Guide to Quantum Technology and National Security," *Deloitte Insights*, February 6, 2020, https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html.

[8] Philip Ball, "The Universe Is Always Looking," *The Atlantic*, October 20, 2018, https://www.theatlantic.com/science/archive/2018/10/beyond-weird-decoherence-quantum-weirdness-schrodingers-cat/573448/.

[9] *Quantiki* (October 26, 2015), s.v. "qubit," https://www.quantiki.org/wiki/qubit.

[10] Cathal O'Connell, "Quantum Computing for the Qubit Curious," *Cosmos*, July 5, 2019, https://cosmosmagazine.com/physics/quantum-computing-for-the-qubit-curious/.

[11] Adrian Cho, "No Room for Error," *Science*, July 9, 2020, https://www.sciencemag.org/news/2020/07/biggest-flipping-challenge-quantum-computing.

[12] Max G. Levy, "New Quantum Algorithms Finally Crack Nonlinear Equations," *Quanta Magazine*, January 5, 2021, https://www.quantamagazine.org/new-quantum-algorithms-finally-crack-nonlinear-equations-20210105/.

[13] Francesco Bova, Avi Goldfarb, and Roger G. Melko, "Commercial Applications of Quantum Computing," *EPJ Quantum Technology* 8, no. 2 (January 2021), https://doi.org/10.1140/epjqt/s40507-021-00091-1.

[14] Stephen Gossett, "10 Quantum Computing Applications and Examples," *Built In*, June 8, 2022, https://builtin.com/hardware/quantum-computing-applications; Scott Buchholz, Caroline Brown, and Deborah Golden, "A Business Leader's Guide to Quantum Technology," *Deloitte Insights*, April 15, 2021, https://www2.deloitte.com/us/en/insights/topics/innovation/quantum-computing-business-applications.html.

[15] Gossett, "10 Quantum Computing Applications and Examples."

[16] Duncan Stuart, "Quantum Computers: The Next Supercomputers, but Not the Next Laptops," *Deloitte Insights*, December 11, 2019, https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/quantum-computing-supremacy.html.

[17] "Explore the Possibilities of Quantum," Google Quantum AI, n.d., https://research.google/teams/applied-science/quantum/.

[18] "Azure Quantum," Microsoft Azure, 2023, https://azure.microsoft.com/en-us/solutions/quantum-computing/.

[19] IBM Quantum, IBM, n.d., https://www.ibm.com/quantum-computing/.

[20] Frank Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," *Nature*, October 23, 2019, https://www.nature.com/articles/s41586-019-1666-5.

[21] John Preskill, "Why I Called It 'Quantum Supremacy,'" *Quanta Magazine*, October 2, 2019, https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/.

[22] Paul Smith-Goodson, "Quantum USA vs. Quantum China: The World's Most Important Technology Race," *Forbes*, October 10, 2019, https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/?sh=46c1c62272de.

[23] "China's 14th Five-Year Plan: A First Look," *Congressional Research Service*, January 5, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11684.

[24] "Infographics on Quantum Computing: Patent Trends and Analysis," PatSeer, n.d.,

https://patseer.com/infographics-on-quantum-computing-patent-trends-and-analysis/.

[25] Ibid.

[26] *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, update to the *Intellectual Property Commission Report* (Washington, DC: National Bureau of Asian Research, 2017), https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/.

[27] "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," Department of Justice, October 10, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading; "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," Department of Justice, December 20, 2018, https://www.justice.gov/usao-sdny/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer.

[28] Lisa Ferdinando, "DOD Officials: Chinese Actions Threaten U.S. Technological, Industrial Base," Department of Defense, June 21, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1557188/dod-officials-chinese-actions-threaten-us-technological-industrial-base/.

[29] Ellen Nakashima and Aaron Schaffer, "Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors," *Washington Post*, April 21, 2021, https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html.

[30] Becky Bracken, "Chinese Breakthrough in Quantum Computing a Warning for Security Teams," *Threatpost*, December 7, 2020, https://threatpost.com/chinese-quantum-computing-warning-security/161935/; Zen Chan, "A Leap of Quantum Computing in China, a Threat to Internet Security," *01*, February 2, 2021, https://vocal.media/01/a-leap-of-quantum-computing-in-china-a-threat-to-internet-security; Tom Simonite, "China Stakes Its Claim to Quantum Supremacy," *Wired*, December 3, 2020, https://www.wired.com/story/china-stakes-claim-quantum-supremacy/.

[31] Emily Conover, "The New Light-Based Quantum Computer Jiuzhang Has Achieved Quantum Supremacy," *Science News*, December 3, 2020, https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy.

[32] Lamont Wood, "The Clock Is Ticking for Encryption," *Computerworld*, March 21, 2011, https://www.computerworld.com/article/2550008/the-clock-is-ticking-for-encryption.html#:~:text=But%20using%20quantum%20technology%20with.

[33] Douglas Crawford, "How Does AES Encryption Work?" *ProPrivacy*, February 4, 2019, https://proprivacy.com/guides/aes-encryption; Benjamin Scott, "Military-Grade Encryption Explained," *NordPass*, August 12, 2020, https://nordpass.com/blog/military-grade-encryption-explained/#:~:text=Military%2Dgrade%20encryption%20refers%20to.

[34] John R. Lindsay, "Surviving the Quantum Cryptocalypse," *Strategic Studies Quarterly* 14, no. 2 (Summer 2020), 49–73.

[35] Ibid.

[36] Executive Order 13702, *Creating a National Strategic Computing Initiative* (Washington, DC: The White House, July 29, 2015), https://irp.fas.org/offdocs/eo/eo-13702.pdf.

[37] Hamish Johnston, "U.S. Invests $249m in Quantum Information Science as White House Unveils Strategic Overview," *Physics World*, September 28, 2018, https://physicsworld.com/a/us-invests-249m-in-quantum-information-science-as-white-house-unveils-strategic-overview/.

[38] Executive Order 13885, *Establishing the National Quantum Initiative Advisory Committee* (Washington, DC: The White House, August 30, 2019), https://www.govinfo.gov/content/pkg/DCPD-201900584/pdf/DCPD-201900584.pdf.

[39] Akhil Iyer, *Tech Factsheets for Policymakers: Quantum Computing* (Cambridge, MA: Belfer Center for Science and International Affairs, 2020), https://www.belfercenter.org/sites/default/files/files/publication/QC_2.pdf.

[40] David Vergun, "DOD Officials Discuss Quantum Science, 5G and Directed Energy," DOD, March 9, 2021, https://www.defense.gov/Explore/News/Article/Article/2530494/dod-officials-discuss-quantum-science-5g-and-directed-energy/.

[41] *National Defense Authorization Act for Fiscal Year 2020*, S. 1790, 116th Cong., 1st sess., January 3, 2019, https://www.congress.gov/116/bills/s1790/BILLS-116s1790enr.pdf.

[42] Brandi Vincent, "Inside the Air Force Research Laboratory's Contemporary Quantum Pursuits," *Nextgov*, January 6, 2021, https://www.nextgov.com/emerging-tech/2021/01/inside-air-force-research-laboratorys-contemporary-quantum-pursuits/171201/; Paul Cage, "Naval Research Laboratory Designated Navy's Quantum Information Research Center," U.S. Navy Office of Information, September 28, 2020, https://www.navy.mil/Press-Office/News-Stories/Article/2364183/naval-research-laboratory-designated-navys-quantum-information-research-center/.

[43] Dwight Weingarten, "House Panel Approves NDAA Cyber, Quantum Provisions," *MeriTalk*, June 22, 2020, https://www.meritalk.com/articles/house-panel-approves-ndaa-cyber-quantum-provisions/.

[44] "USD(R&E) Technology Vision for an Era of Competition," Under Secretary of Defense for Research and Engineering, February 1, 2022, https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf.

[45] William McCormick, "Senators Introduce Legislation to Assist DOD Quantum Computing Efforts; Sen. Maggie Hassan Quote," *ExecutiveGov*, April 16, 2021, https://www.executivegov.com/2021/04/senators-introduce-legislation-to-assist-dod-quantum-computing-efforts-sen-maggie-hassan-quote/.

[46] "NASA Quantum Artificial Intelligence Laboratory (QuAIL)," National Aeronautics and Space Administration, November 9, 2022, https://www.nasa.gov/content/nasa-quantum-artificial-intelligence-laboratory-quail.

[47] "Research," Joint Quantum Institute, n.d., https://jqi.umd.edu/research.

[48] *National Quantum Initiative Supplement to the President's FY 2023 Budget: A Report by the Subcommittee on Quantum Information Science, Committee on Science of the National Science & Technology Council* (NSTC) (Washington, DC: NSTC, January 2023), https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf.

[49] "Project Apollo Cost Data: Project Apollo 1960–1973," comp. Casey Drier, The Planetary Society, https://docs.google.com/spreadsheets/d/e/2PACX-1vTKMekJW9F8Z3f-Wnx-IxvHSPD35iZxZxDVoqIp25FaxxXjO-qJ2Rk-zS858dND0N_3cwcacbIX8gr9xt/pubhtml.

[50] Ian King, "Beyond Ends, Ways, and Means: We Need a Better Strategic Framework to Win in an Era of Great Power Competition," *Modern War Institute*, September 3, 2020, https://mwi.usma.edu/beyond-ends-ways-and-means-we-need-a-better-strategic-framework-to-win-in-an-era-of-great-power-competition/.

[51] A 2017 Government Accountability Office (GAO) report identified six areas that innovative companies had cited as challenges that deter them from working with DOD: complexity of DOD's process, unstable budget environment, long contracting timelines, intellectual property rights concerns, government-specific contract terms and conditions, and an inexperienced DOD contracting workforce. See "Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies," GAO-17-644 (Washington, DC: GAO, July 20, 2017), https://www.gao.gov/products/gao-17-644.

[52] DOD Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Washington, DC: DOD, January 23, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.PDF.

[53] Federal Acquisition Regulation, Part 6.302, "Circumstances Permitting Other Than Full and Open Competition," *Acquisition.gov*, December 30, 2022, https://www.acquisition.gov/far/part-6#FAR_6_302.