The Heritage Foundation

BACKGROUNDER

No. 3385 | FEBRUARY 5, 2019

Quantum Science and National Security: A Primer for Policymakers

Klon Kitchen

Abstract

Advancing quantum science promises to expand human knowledge and to fundamentally reshape the nature of technological innovation. These same developments, however, could profoundly affect U.S. national security and shift the global political and economic balance. In fact, some of the United States' chief rivals are explicitly pursuing this aim. Policymakers should take the time now, before this scientific revolution is fully realized, to understand and to prepare for the potential quantum disruption.

Introduction

Quantum science—research on how the universe works at the levels of molecules, atoms, and electrons—appears poised for a series of breakthroughs. Specifically, researchers are advancing the ability to replicate and manipulate the mind-bending actions occurring among very small particles. These advancements, if realized, would fundamentally reshape everything science knows about everything. But significant challenges remain, and many of the most remarkable quantum promises are still decades away—if they are realizable at all.

Even so, while it is always wise to question grandiose declarations of world-changing innovations, there is also good reason to take seriously many of the advancements in quantum science. Policymakers now have the rare opportunity to foresee what can be described as a medium-probability, high-impact innovation and to carefully consider and reasonably prepare for its implications. Of particular importance is the potential impact on national security.

Key Points

- Quantum science appears poised for a series of breakthroughs, some of which could significantly impact U.S. national security.
- There are three broad areas in which the promise and the risk of quantum disruption appear to be most proximate: quantum computing, quantum sensing, and quantum communications and encryption.
- China and the United States are the clear centers of gravity for quantum science research—and competition between the two is tightening.
- U.S. policymakers should prioritize oversight of the nation's quantum science efforts, as well as encourage the United States' long-term quantum competitiveness.
- While many of the advancements in quantum science are promising, knee-jerk government spending would not be as helpful. What is needed is informed and deliberate engagement on the economic, social, and political implications of these advancements.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3385**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Quantum science could open new possibilities in computer processing and storage, data collection and analysis, and information and communications security. But the United States could also face a series of rapid—and possibly decisive—vulnerabilities to national security if quantum advantage is preemptively realized by one of its global competitors. This, then, demands a clear-eyed understanding of the basics of quantum science, some of its most important applications to national security, the state of the race for quantum advantage, and the key objectives policymakers should pursue in order to realize quantum science's hopes while simultaneously navigating its attendant challenges.

What Is Quantum Science?

Quantum science is scientific research building on *quantum theory*, the governing hypothesis of how nature works at the level of atoms, photons, and other subatomic particles. The word "quantum" refers to the notion that all energy, light, and matter is composed of discrete units, or *quanta*. This theory was formally described in 1900 by German physicist Max Planck, who sought to explain why radiation from so-called "black bodies"[1] changes color as it heats up. Although quantum theory differs significantly from the laws of classical physics, it also complements classical physics and is the best theory for explaining much of the universe.

There are two especially important phenomena within quantum physics that differentiate it from classical physics and that appear to hold the greatest promise for future innovation. The first phenomenon is particle *superposition*.

Superposition. Classic physics states that two things cannot occupy the same space at the same time or be wholly present in more than one place at a time. Quantum physics, however, says that the world is held together by objects that exist in two distinct states simultaneously: This state is called superposition. For example, a molecule consists of two atoms "glued" together by an electron. This electron could be associated with either atom; however, quantum theory suggests that this single electron must be associated with each atom at the same time for them to be properly joined. This is the only way scientists are able to understand everything from photosynthesis to lasers.

Put simply: Superposition means that a quantum object can be "this" and "that," "there" and "here," or "down" and "up" at the same time. Confused? Good, that means you are getting it. As physicist Niels Bohr observed, "Those who are not shocked when they first come across quantum theory cannot possibly have understood it."[2] The other key phenomenon is equally mystifying.

Entanglement. *Entanglement* is when two or more quantum objects become linked so that any measurement of one immediately determines the state of the others—regardless of the distance between them. It is as if there are two spinning quarters on opposite sides of the universe and whenever one is stopped from spinning, the other also stops and displays the same value (e.g., heads or tails) as the first. Albert Einstein rejected entanglement as "spooky action at a distance," but it has since been demonstrated in multiple experiments, including a Chinese effort using pairs of photons separated by more than 745 miles.[3] Again, if all of this sounds crazy, you are with the experts. In his book, *In Search of Schrödinger's Cat: Quantum Physics and Realty*, John Gribbin summarizes the uniqueness of the quantum world this way:

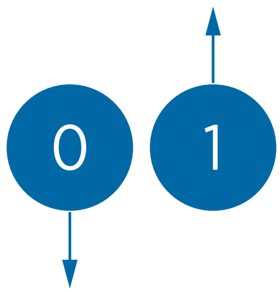
> In the world of the very small, where particle and wave aspects of reality are equally significant, things do not behave in any way that we can understand from our experience of the everyday world.... [A]ll pictures are false, and there is no physical analogy we can make to understand what goes on inside atoms. Atoms behave like atoms, nothing else.[4]

1. In physics, a "blackbody" is any surface that absorbs all radiant energy falling on it.
2. Niels Bohr, *The Philosophical Writings of Niels Bohr, Vol. 2: Essays 1932–1957; Atomic Physics and Human Knowledge* (Woodbridge, CT: Ox Bow Press, 1958).
3. Lee Billings, "China Shatters 'Spooky Action at a Distance' Record, Preps for Quantum Internet," *Scientific American*, June 15, 2017, https://www.scientificamerican.com/article/china-shatters-ldquo-spooky-action-at-a-distance-rdquo-record-preps-for-quantum-internet/ (accessed November 26, 2018).
4. John Gribbin, *In Search of Schrödinger's Cat: Quantum Physics and Realty* (New York: Bantam Books, 1984).

FIGURE 1

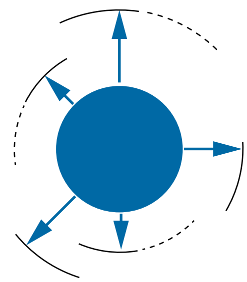
The Difference Between Conventional and Quantum Computers

CONVENTIONAL COMPUTERS:
Store and use information as individual bits encoded in one of two states, either 0 or 1.



Bits are processed sequentially, one step at a time, so repeated computations will lead to the same output.

QUANTUM COMPUTERS:
Encode information in "qubits," which can simultaneously contain an infinite and continuously changing number of states (including negative values). This is called "superposition."



Qubits are also "entangled," which means they can influence other qubits. Measurements yield probabilities that increase in confidence through repeated computations, then are reduced to 0 or 1 when measured.

SOURCE: Accenture Labs, "Think Beyond Ones and Zeroes," June 28, 2017, https://www.accenture.com/t20170628T011725Z__w__/us-en/_acnmedia/PDF-54/Accenture-807510-Quantum-Computing-RGB-V02.pdf (accessed January 21, 2019).

BG3385 heritage.org

Nevertheless, understanding of these mind-bending phenomena is advancing, and researchers are beginning to manipulate and leverage these phenomena toward revolutionary results. While these results and their attendant effects could span nearly all aspects of life, the applications for national security are worthy of special consideration.

Quantum Science and National Security

The applications of quantum science to national security are vast, but there are three areas in which the promise and the risk of quantum disruption appear to be most proximate. Quantum computing is the first of these applications.

Quantum Computers. Quantum computers use the unique properties of quantum mechanics to enable computers that are exponentially more powerful at certain tasks than any supercomputer ever built. Conventional computers, at their most basic level, store and use information as individual bits, which encode information as either a "0" or a "1." Computer programs do what they do by manipulating millions of bits in different patterns to accomplish different tasks.

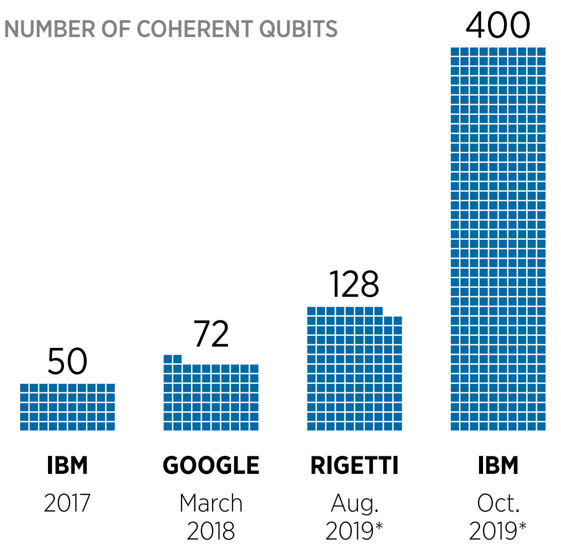
Leveraging superposition, quantum computers produce bits that can not only be "1" or "0", but also "1" and "0" at the same time. These small shapeshifters are called "qubits." These qubits can be entangled and used to express and to test probabilities at scales and at speeds currently unachievable. With every qubit that is added to a microchip, that microchip's processing and probabilistic power grows exponentially. It is generally believed that we need at least 100 "coherent"[5] qubits on a processing chip to realize the first fruits of meaningful quantum computing—and the qubits are adding up.

In August 2018, California-based Rigetti Computing announced plans to build a processor with 128 coherent qubits within 12 months. If realized, this would be a 78 percent increase over Google's 72-qubit processor unveiled in March 2018 and a 156 percent increase over the former leading 50-qubit processor

5. "Coherence" refers to the amount of time that a quantum entity—in this case, a qubit—can remain in superposition.

CHART 1

Qubit Processing Speeds Growing Rapidly



* Projected

SOURCE: Brian Wang, "Rigetti Computing Hopes to Have a Functioning 128 Qubit Quantum Computer Within 12 Months," August 8, 2018, https://www.nextbigfuture.com/2018/08/rigetti-computing-hopes-to-have-a-functioning-128-qubit-quantum-computer-within-12-months.html (accessed January 21, 2019).

BG3385 heritage.org

built by IBM in 2017.[6] But qubits are not just powerful, they are also very sensitive.

For a qubit to achieve superposition, they must operate at around 15 millikelvin, a temperature colder than interstellar space. This has led to several different approaches to building quantum computers, some of which not only keep things cool but that also use rare metals that are highly conductive, as well as so-called ion traps that use electromagnetic fields and lasers to capture and to manipulate atoms. (See "Types of Quantum Computers" for more on the different types of quantum computers and their sensitivities.)

Because qubits are extremely sensitive to their environment and because their transition frequencies (the frequency that a quantum unit changes from one state to another) are precise, repeatable, and identical, qubits might also be used in sensors that would far exceed current capabilities. Which brings us to our second national security application, quantum sensing.

Quantum Sensing. One application currently being explored by the U.S. military involves coupling quantum clocks with quantum-enabled sensors for gravity, acceleration, and rotation to provide precise navigation, even in environments in which global positioning satellites are denied.[7] Similar capabilities might one day be used to detect stealth systems based solely on the atmospheric disruption they produce by being at a location in time and space,[8] or perhaps detecting and identifying chemical or biological agents using very small samples. In a world where opponents are becoming more sophisticated in their deception and denial capabilities, quantum sensing could provide a game-changing advantage. Or, in the hands of opponents, a game-changing risk. But even if this data can be collected, it still needs to be stored and moved securely, leading to the third application: quantum communications and encryption.

Quantum Secure Communications. Current efforts to leverage quantum theory for communications and data security tend to focus on the creation and distribution of quantum encryption keys—cryptographic "codes" that are generated using qubits to encrypt and decrypt information. These quantum keys are beneficial because they leverage properties of entanglement to alert both keyholders (the sender and the receiver) of any attempted interference with the key by a third party. Importantly, however, even messages encrypted using quantum keys are still transmitted via conventionally encrypted communications lines—leaving them susceptible to interception.

6. Brian Wang, "Rigetti Computing Hopes to Have a Functioning Qubit Quantum Computer Within 12 Months," Next Big Future, August 8, 2018, https://www.nextbigfuture.com/2018/08/rigetti-computing-hopes-to-have-a-functioning-128-qubit-quantum-computer-within-12-months.html (accessed January 3, 2018); Julian Kelly, "A Preview of Bristlecone, Google's New Quantum Processor," Google AI, March 5, 2018, https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (accessed January 29, 2018); and Will Knight, "IBM Raises the Bar with a 50-Qubit Quantum Computer," *MIT Tech Review*, November 10, 2017, https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/ (accessed January 29, 2018).
7. Martin Giles, "The U.S. and China Are in a Quantum Arms Race That Will Transform Warfare," *MIT Tech Review*, January 3, 2019, https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/ (accessed January 4, 2018).
8. Ibid.

Types of Quantum Computers

There are multiple approaches to building quantum computers—each with their own strengths and weaknesses. The two approaches that appear to hold the most promise are the Adiabatic quantum computer ("annealer") and the Gate Model quantum computer ("standard model").

- **Adiabatic quantum computer.** This approach uses a formula known as the adiabatic theorem[1] to perform calculations and is best suited for optimizing problems. The key point on these quantum computers is that they are easiest to build, but they can only be applied against a specific function. Even so, companies like Google are betting big on this approach and many believe quantum annealers—quantum computers focused on a discrete dataset—will constitute an important evolutionary step towards a general quantum computer.
- **Gate Model quantum computer.** This approach is far more complex because these machines perform calculations using quantum application "gates"—a basic quantum circuit leveraging multiple entangled qubits. Unlike the task-specific Adiabatic approach, Gate Model quantum computers build blocks of these quantum gates to mimic conventional computing and are, therefore, at least theoretically, closer to a general-use computer.

Even as researchers advance these and other approaches to quantum computing, significant technical challenges remain. The most fundamental of these challenges is "noise." Noise is shorthand for small unwanted variations in data or in the physical computing environment that disrupt or prevent efficient computation. Classical computers are very good at removing noise. Qubits and the complex computing environments that they require, however, remain critically vulnerable to noise.

While it is sometimes possible to run a quantum error correction (QEC) algorithm to emulate a noise-free environment, there is high operational cost for doing so as these QECs require large numbers of qubits and thereby dramatically reduce the overall computational power of the quantum computer. Thus far, researchers simply have not been able to produce the necessary number of stable qubits to absorb this cost while sustaining meaningful quantum computational power. These and other challenges mean that quantum computers are still a theoretical—not a guaranteed—approach to computing.

1. The adiabatic theorem was originally developed by Max Born and Vladimir Floch in 1928. Stated simply, the theorem postulates that quantum mechanical systems adapt their forms when subjected to gradually changing environments. But when the environment changes quickly, their forms are unchanged due to insufficient time for the form to adapt.

More complex systems of quantum networks—in which data is not only secured at rest with quantum keys but also in transit by quantum mechanics—are being researched and could one day produce systems that can transmit, store, and process data using networks of entangled quantum memories. Having computers fast enough and powerful enough to establish quantum-secure communications, however, would likely also render legacy encryption critically vulnerable because these powerful computers would also be able to break this encryption.

In late 2015, Google announced that its D-Wave 2X quantum annealing machine was able to run an algorithm *100 million times* faster than a conventional computer.[9] Current encryption standards—the standards we use to secure everything from personal banking transactions to nuclear launch codes—use a complex algorithm ("cipher") to transform data into a series of seemingly random characters ("ciphertext") that is unreadable to anyone who does not have the encryption key needed to decipher the data. Assuming the highest level of currently available encryption,

9. Hartmut Neven, "When Can Quantum Annealing Win?" Google AI, December 8, 2015, https://ai.googleblog.com/2015/12/when-can-quantum-annealing-win.html (accessed on November 26, 2018).

the world's most powerful supercomputer (currently the Summit supercomputer at the U.S. Department of Energy's Oak Ridge National Laboratory in Tennessee[10]) could take more than 1 billion years to break this encryption. A fully functional quantum computer, however, may be able to do this near instantaneously.

The stakes, then, for realizing quantum advantage and for avoiding quantum surprise can hardly be overstated. This begs the question: What is the state of the race for quantum leadership?

The Race for Quantum Advantage

The race for quantum advantage is not a sprint, and it is not a marathon. It is a free-for-all in which the finish line is vague and where the participants use self-determined routes. Some researchers are advancing the number of stable qubits on microchips, while others are writing the software that will eventually run on quantum computers, while still others are exploring ways to move these capabilities to the "cloud" so that they can be leveraged at scale. This makes it difficult to assess who is "winning" the quantum race, especially as the race gets more crowded. Even so, the relative levels of research and funding within China and within the United States set them apart as centers of gravity for quantum science.

Australia, Canada, and Europe. The public programs in Australia, Canada, and Europe often benefit from significant technical expertise. However, they are relatively small in both investment and in the underlying industrial bases to support them. Australia announced in 2016[11] that it would invest nearly $18 million over five years for the development of a silicone quantum-integrated chip while Canada is pouring $76 million into the University of Waterloo's Transformative Quantum Technologies program.[12] Both nations are also partnering with the United States on a quantum-enabled navigation effort.[13] The Netherlands will spend $150 million on its QuTech Initiative over 10 years[14] while the European Union is slated to invest $1.3 billion in its Flagship Quantum Program over the same time period.[15] The United Kingdom is currently planning $400 million for its Quantum Hub Network over five years.[16]

Russia. The promise of quantum science and Russia's known prioritization of defense-related technology suggests the country's quantum sciences research is likely progressing. Moscow's systemic economic weakness, however, and the nation's prioritization of other emerging technologies (i.e., artificial intelligence, hypersonic missiles) would also suggest government investment in quantum research may be relatively small. In truth, there is very little publicly available information on these programs.

What little information exists indicates the Russian Quantum Center (RQC)—a notionally non-government research center in Skolkovo—constitutes the hub of Russian quantum science research. Launched in 2012, the RQC has 11 separate research programs investigating challenges such as "quantum simulators and integrated photonics," "coherent micro-optics and radio-photonics," and "quantum measurements"—all of which have commercial and national security applications.[17]

10. Morgan McCorkle, "ORNL's Summit Supercomputer Named World's Fastest," Oak Ridge National Laboratory, June 25, 2018, https://www.ornl.gov/news/ornl-s-summit-supercomputer-named-world-s-fastest (accessed January 31, 2018).
11. Government of Australia, "Advancing Quantum Computing Technology," April 1, 2016, https://archive.innovation.gov.au/page/advancing-quantum-computing-technology (accessed January 7, 2019).
12. News release, "Government of Canada Invests $900 Million to Transform University," Canada First Research Fund, September 6, 2016, http://www.cfref-apogee.gc.ca/news_room-salle_de_presse/press_releases-communiques/2016/University_of_Waterloo-eng.aspx (accessed January 7, 2019).
13. Carten Cordell, "Military to Collaborate with Allies on Quantum Navigation Project," FedScoop, July 16, 2018, https://www.fedscoop.com/military-collaborate-allies-quantum-navigation-project/ (accessed January 7, 2019).
14. QuTech, "The Netherlands Invests €135 Million in Quantum Technology," QuTech, June 1, 2018, https://qutech.nl/investmentquantumtechnology/ (accessed January 7, 2019).
15. Stuart Wills, "Europe's 'Quantum Flagship' Officially Sets Sail," Optics & Photonics, October 31, 2018, https://www.osa-opn.org/home/industry/2018/october/europe_s_quantum_flagship%E2%80%9D_officially_sets_sail/ (accessed January 7, 2019).
16. "Quantum Technologies: A £1 Billion Future Industry for the U.K.," U.K. Quantum Technology Programme, http://uknqt.epsrc.ac.uk/ (accessed January 7, 2019).
17. RQC Evaluation Committee, "Evaluation Report of the Russian Quantum Center—RQC," May 1, 2018, http://www.rqc.ru/pdf/Evaluation_report_of_the_Russian_Quantum_Center-RQC.pdf (accessed January 8, 2019).

According to a recent report on the RQC by its international evaluation committee, the center hosts more than 170 scientists, working in 12 different laboratories containing approximately $9 million worth of equipment in a 13,455-square-foot (1,250-square-meter) facility. Since its founding, the RQC has reportedly published more than 450 peer-reviewed papers and commercialized six technology start-ups.[18] To place this into context, Stanford University alone has more than 6,200 externally sponsored research projects, with a total budget of $1.64 billion in 2017–2018, resulting in more than 700 scientific papers every year.[19]

In summary, as a global power, Russia's quantum science research likely exceeds in sophistication—and perhaps even in scale—many other international efforts. It almost assuredly, however, does not match the pace and scale of innovation occurring within China and within the United States.

China. China's central government is driving the country's quantum research and investment. While it would be a mistake to equate government action with quantum advantage, it would also be a mistake to dismiss this centralized approach. The state-led model provides some efficiencies by leveraging China's considerable research and economic base against a narrowed field of the government's highest priorities like offensive and defensive national security applications. In fact, there is good reason to believe national security is precisely what is driving Beijing.

The illegal disclosures by former National Security Agency (NSA) contractor Edward Snowden reportedly played a key part in jumpstarting China's quantum science program.[20] Having discovered some of the capabilities of the NSA to collect and to monitor global communications, Beijing began prioritizing quantum-secure communications, and they are making significant progress.

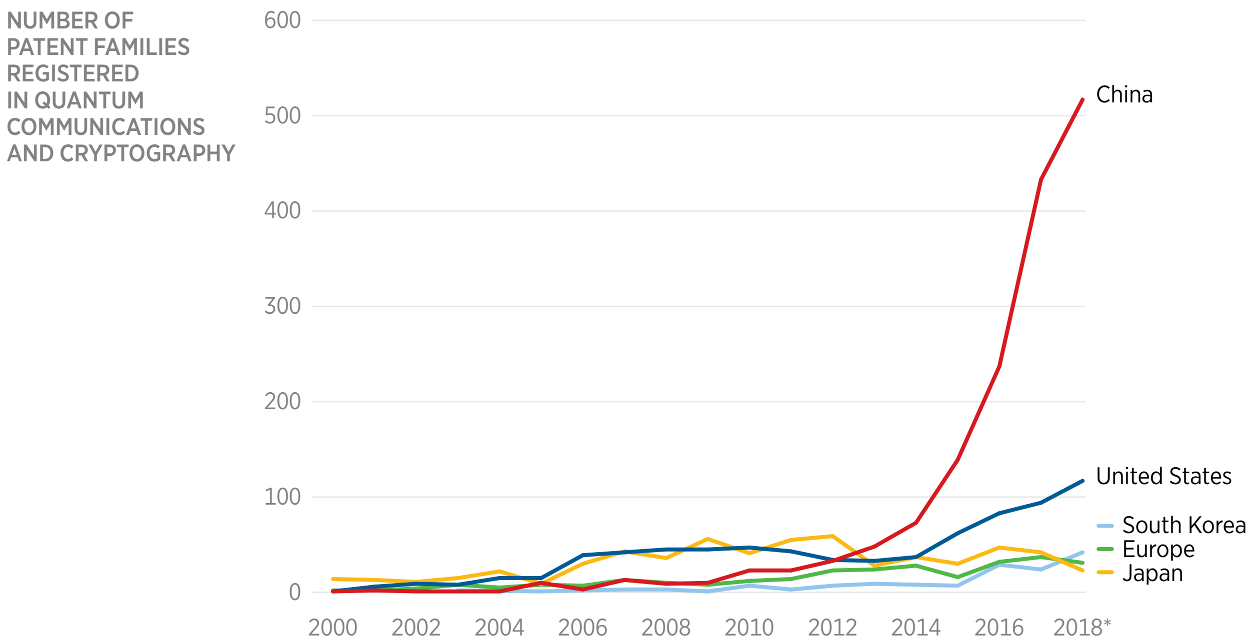
In 2016, China surprised many observers when it launched the first-known quantum satellite into low-Earth orbit.[21] This Micius satellite was later used in 2017 to hold a quantum-encrypted video call between Chinese and Australian scientists (using quantum encryption keys only).[22] A ground-based network in the northern province of Shandong has also been built, providing a proof of concept for a quantum-encrypted Internet.[23] Advancements like these are certain to continue.

The number of scholarly articles citing Chinese technology research is growing—even when compensating for concerns about citation inflation and other forms of fraud[24]—indicating the country is increasingly seen as a leader and an innovator within the research community.[25] In 2014, China was already filing about the same number of quantum-computing patent applications as the United States.[26] In 2017, Chinese filings were *double* those offered by the United States.[27] Commenting on China's determined focus, Robert Young, director of the Lancaster Quantum Technology Center and an adjunct professor at the Institute of Fundamental and Frontier Science in Chengdu, explains that "China basically missed out on the digital revolution and that really set them and their economy back. It doesn't want to be caught napping again."[28]

18. Ibid.
19. Stanford University, "Research at Stanford," https://facts.stanford.edu/research/ (accessed January 8, 2019).
20. Amit Katwala, "Why China's Perfectly Placed to Be Quantum Computing's Super Power," *Wired*, November 14, 2018, https://www.wired.co.uk/article/quantum-computing-china-us (accessed January 3, 2019).
21. Mike Wall, "China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite," August 16, 2016, https://www.space.com/33760-china-launches-quantum-communications-satellite.html (accessed January 3, 2018).
22. Kyree Leary, "Quantum Video Call Displays the Future of Secure Communication," Futurism, February 2, 2018, https://futurism.com/quantum-video-secure-communication (accessed January 3, 2019).
23. Katwala, "Why China's Perfectly Placed to be Quantum Computing's Super Power."
24. "Looks Good on Paper," *The Economist*, October 3, 2013, https://www.economist.com/china/2013/10/03/looks-good-on-paper (accessed January 14, 2019).
25. Hepeng Jia, "China's Citations Catching Up," Nature Index, November 30, 2017, https://www.natureindex.com/news-blog/chinas-citations-catching-up (accessed January 3, 2019).
26. "Quantum Applications Patent Landscape Report," Patinformatics, January 1, 2018, https://patinformatics.com/wp-content/uploads/2018/01/Quantum-Applications-Patent-Landscape-Report-Opt.pdf (accessed January 3, 2019).
27. Ibid.
28. Katwala, "Why China's Perfectly Placed to be Quantum Computing's Super Power."

CHART 2

Growth of Quantum-Related Patent Filings



* Provisional data

SOURCE: Martin Giles, "The US and China Are in a Quantum Arms Race That Will Transform Warfare," *MIT Technology Review*, January 3, 2019, https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/ (accessed January 29, 2019).

BG3385 heritage.org

Achieving quantum advantage is one of Beijing's "megaprojects," and they are backing it up with a reported $10 billion National Laboratory for Quantum Information Sciences. Jian-Wei Pan, one of China's leading quantum scientists, explains, "With modern information science, China has been a learner and a follower. Now, with quantum technology, if we try our best we can be one of the main players."[29] Jian-Wei is correct.

In their excellent report, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership,*[30] Elsa B. Kania and John K. Costello state the challenge clearly:

> China's advances in quantum science could impact the future military and strategic balance, perhaps even leapfrogging traditional U.S. military–technological advantages. Although it is difficult to predict the trajectories and timeframes for their realization, these dual-use quantum technologies could "offset" key pillars of U.S. military power, potentially undermining critical technological advantages associated with today's information-centric ways of war, epitomized by the U.S. model.

The United States of America. The United States' private sector largely drives the nation's quantum science efforts—allowing curious minds and industry to determine which avenues of research offer the most intellectual and economic promise. Unlike the Chinese model, this approach enables a broad range of activity as well as an agility to quickly pivot away from scientific "dead ends." While creat-

29. Ibid.

30. Elsa B. Kania and John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, Center for a New American Security, September 2018, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406 (accessed January 25, 2019).

ing a more dynamic research environment, it must be observed that this approach might occasionally suffer from a type of attention deficit disorder when difficult (but fundamental) research is not sufficiently monetized to support long-term development. This is where the U.S. government often plays a key role.

The Department of Defense has been investing in and researching quantum science for decades (approximately $96 million in 2018 and another $565 million by 2023),[31] and other government agencies like the CIA, NASA, and the Department of Energy (DOE) also have ongoing quantum partnerships with the private sector.[32] In September 2018, for example, the DOE announced it would distribute $218 million among 87 different quantum-science research initiatives at 28 U.S. universities and nine national laboratories.[33] The Commerce Department's National Institute for Standards and Technology (NIST) also has a dedicated effort to establish mechanisms and standards for upgrading government information systems so that they eventually employ quantum-resistant security.[34] NIST is also leading a consortium of public and private enterprises to support the development of the quantum computing industry.[35] Even so, China's growing technological capacity is eliciting a number of new government initiatives aimed at securing American technological security and superiority.

In September 2018, the Trump Administration issued its National Strategic Overview for Quantum Information Science, detailing several policy priorities, including "creating a quantum-smart workforce," "deepening engagement with quantum industry," "providing critical infrastructure," "maintaining national security and economic growth," and "advancing international cooperation."[36] Later, in December 2018, the President also signed the National Quantum Initiative (NQI) into law, providing $1.275 billion over five years for the establishment of multiple quantum science and technology research centers, each with a focus on a particular quantum technology or application and under the direction of the Department of Energy, the National Science Foundation, and NIST.

The law also requires the President to establish a National Quantum Initiative Advisory Committee composed of government and private-sector experts who will guide federal quantum research, establish goals and priorities for these programs, assess and recommend what federal support is required for these programs, and evaluate opportunities for international cooperation. The NQI also creates a subcommittee on quantum information science at the National Science and Technology Council and a National Quantum Coordination Office within the White House's Office of Science and Technology Policy.

Even as the U.S. government continues to organize its various quantum science efforts, the U.S. private sector remains the engine for quantum science innovation.

The Private Sector

The real action in quantum science is in the private sector, with growing quantum computing efforts at companies like Google, Honeywell, Hughes Research, IBM, Intel, Lockheed-Martin, Microsoft, and Northrop Grumman. Though they have been slower to enter the quantum space, Chinese technology companies like Alibaba, Baidu, and Tencent are also rapidly expanding their quantum research and development. Many of these companies are also teaming with top universities, like Google and the Univer-

31. Patrick Tucker, "How the U.S. Is Preparing to Match Chinese and Russian Technology Development," Defense One, August 22, 2018, https://www.defenseone.com/technology/2018/08/how-us-preparing-match-chinese-and-russian-technology-development/150758/ (accessed January 4, 2019).
32. "D-Wave Forms Independent Subsidiary for U.S. Government Business," D-Wave, October 18, 2016, https://www.dwavesys.com/press-releases/d-wave-forms-independent-subsidiary-us-government-business (accessed January 4, 2019).
33. U.S. Department of Energy, "Department of Energy Announces $218 Million for Quantum Information Science," September 24, 2018, https://www.energy.gov/articles/department-energy-announces-218-million-quantum-information-science (accessed January 14, 2019).
34. National Institute for Standards and Technology, "Post-Quantum Cryptography," January 3, 2017, https://csrc.nist.gov/projects/post-quantum-cryptography (accessed December 26, 2018).
35. National Institute for Standards and Technology, "NIST Launches Consortium to Support Development of Quantum Industry," September 28, 2018, https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry (accessed December 26, 2018).
36. White House, "National Strategic Overview for Quantum Information Science," September 1, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf (accessed January 14, 2019).

sity of California Santa Barbara, Lockheed Martin and the University of Maryland, and Intel and the Delft University of Technology. Additionally, a new brand of quantum-focused investment funds, like Quantum Valley Investments and Quantum Wave Fund, are supporting new start-ups in the field—all of whom are racing to realize the economic windfall of cracking the quantum code.

Many of these companies have distributed research efforts located in multiple countries. Google and Microsoft, for example, have cutting-edge research centers in China and elsewhere (though neither are currently conducting quantum research in China). In many ways, this is advantageous to everyone because it allows quantum research to leverage deep pools of expertise wherever they exist while also encouraging a type of "open-source" collaboration. The majority of quantum research is shared publicly and then used to spur new research by other teams. This has a compounding beneficial effect. But because of quantum science's potential to disrupt the global balance of economic and political power, the location and context of these research advancements matters.

What happens, for example, if quantum research being done by an American company in China discovers a breakthrough that could enable legitimate quantum advantage? Here you would have a private American company—which has possibly received U.S. government support for their research—developing a game-changing technology within the borders of the United States' chief global challenger whose government, by law, has access to all information and research gathered and done within its borders. Further, it is entirely likely that companies operating in environments like China have already been infiltrated by hostile government agents and are knowingly or unknowingly hemorrhaging proprietary research and applications, which are then fed to their foreign competitors. Challenges like these, coupled with the broader national security implications discussed above, require a series of policy objectives that should guide U.S. efforts going forward.

Policy Recommendations

In light of the newly established National Quantum Initiative and in light of the government's ongoing quantum research, policymakers should prioritize oversight of these efforts as well as encourage the United States' long-term quantum security and competitiveness. While many of the advancements in quantum science are promising, knee-jerk government spending will not be as helpful as informed and deliberate engagement on the economic, social, and political implications of these advancements. The following are some practical policy recommendations toward these ends.

Oversight. Research is occurring and resources are flowing, but critical gaps remain in our understanding of the nation's comprehensive quantum posture and that of our allies and of our challengers. Filling these knowledge gaps is a key priority. The U.S. must:

- **Understand the threat.** Congress should task the Secretary of Defense (SECDEF) and the Director of National Intelligence (DNI) with an annual joint assessment of the nation's quantum security posture and capabilities as well as those of its international challengers and enemies. These reports should also include assessments of the U.S. ability to collect against and to assess foreign adversarial quantum programs. Similarly, the House and Senate Armed Services Committees and Select Committees on Intelligence should hold annual hearings on the subject of quantum science and national security.

- **Know what is already being done.** The Government Accountability Office should immediately complete a report listing all U.S. government quantum-science initiatives along with their respective areas of focus, budgets, research plans and schedules, and critical needs. This report should be made available to Congress and to the newly established National Quantum Initiative Advisory Committee (NQIAC) and should be used to establish a baseline understanding of U.S. ongoing efforts. The NQIAC should also establish a regular dialogue with Congress regarding its priorities, plans, and challenges.

- **Win the "must wins."** The National Quantum Coordination Office within the White House, in conjunction with the SECDEF and DNI, should develop a mechanism for determining which quantum technologies are "must wins" for national security, as well as a plan for ensuring these areas are sufficiently supported regardless of their ability to be monetized in the private sector.

- **Secure networks faster—if we can.** While the National Institute of Standards and Technology is developing quantum-resistant algorithms to protect critical infrastructure and other systems from being hacked, the program's tentative timeline extends beyond 2034. Congress should work with NIST and the President to determine what, if anything, can be done to reduce this timeline to minimize the risk of quantum surprise.

- **Pursue smart cooperation.** Congress should task the DNI, SECDEF, the Secretary of Commerce, and any other relevant department or agency head with developing a series of concrete policy recommendations for how the United States can encourage and participate in the global sharing of quantum research and development while simultaneously advancing and protecting U.S. national security. These recommendations should include steps that can be taken to mitigate the counterintelligence threats posed by overt and covert foreign infiltration and acquisition of American quantum technology companies and patents.

Encouraging American Quantum Competitiveness. The United States will be best positioned to ensure its security if it guards and expands its competitiveness in quantum science and applications. This requires an economic environment that respects the rule of law and rewards private enterprise. To achieve these ends, the U.S. should:

- **Facilitate a common understanding.** The U.S. government should seek opportunities to deepen its collaboration with industry and academia so that, as these institutions pursue various quantum projects, they do so with a fuller understanding of these projects' geopolitical implications. The Department of Defense, for example, should consider establishing a Quantum Defense Security Consortium consisting of government, industry, and academic leaders who cooperate to encourage shared situational awareness and opportunity development in national-security-related quantum science.

- **Protect IP.** Bolstering U.S. protections for intellectual property (IP) rights will be a fundamental part of becoming the preferred environment for quantum research and innovation. Domestically, federal antitrust agencies like the Justice Department and the Federal Trade Commission should abandon their anti-IP policies and reestablish their previous view for patents as property rights meriting strong protections. The U.S. Patent Office should also develop policies to expand, not constrain, protections for issued patents that are subject to administrative review after being granted.

- **Push IP partners.** Internationally, the U.S. government should insist that foreign governments keep their IP and antitrust commitments made in existing and future bilateral treaties.

- **Punish IP thieves.** Finally, we should more aggressively punish international IP thieves by limiting their access to U.S. markets, sanctioning them, or both. The U.S. might also consider punishing the customers of IP thieves who continue to purchase stolen goods and services. While these and other measures will not fully stop the illegal transfer of U.S. IP, they will contribute to an environment in which leaders in quantum science feel more secure in realizing the benefits of their labors.

Conclusion

Many of the largest promises of quantum science remain elusive and may ultimately prove unobtainable in the near- to mid-term. Nevertheless, recent advancements indicate that our core understanding of quantum mechanics and our ability to apply these theories to new technological innovations is expanding—as are those of our global competitors. This expansion provokes legitimate hopes and concerns about the United States' ability to secure its people and its interests. Policymakers would be wise, then, to develop their understanding of these technologies and of their implications, as well as to take actions that encourage the nation's capacity to secure its people and interests as it runs the quantum science race.

*—**Klon Kitchen** is Senior Research Fellow for Technology, National Security, and Science Policy in the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy at The Heritage Foundation.*