INSTITUTE FOR DEFENSE ANALYSES

Overview of the Status of Quantum Science and Technology and Recommendations for the DoD

Stuart A. Wolf - Project Leader
Lance G. Joneckis
Steven Waruhiu
John C. Biddle
Olivia S. Sun
Leonard J. Buckley

June 2019

IDA Document D-10709

Log: H 19-000302

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Project AI-2-4462, "Impact of Quantum Technologies on Critical National Security Applications," for the Office of the Under Secretary of Defense for Research and Engineering/ASD(R&E). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

Stuart A. Wolf, Project Leader
swolf@ida.org, 703-845-6718

Leonard J. Buckley, Director, Science and Technology Division
lbuckley@ida.org, 703-578-2800

Copyright Notice

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-10709

Overview of the Status of Quantum Science and Technology and Recommendations for the DoD

Stuart A. Wolf - Project Leader
Lance G. Joneckis
Steven Waruhiu
John C. Biddle
Olivia S. Sun
Leonard J. Buckley

Executive Summary

Introduction

Within the last few decades, quantum science and technology have become areas of tremendous worldwide interest and have thus garnered significant investment. The Basic Research Office in the Office of the Under Secretary of Defense for Research and Engineering asked IDA to carry out this overview study of quantum technologies to identify where DoD funds should be focused to ensure that the DoD and the United States maintain their current advantage in this key scientific and technological field. We analyzed areas of quantum technology with the potential to change the way we sense, communicate, and compute. The focus of this report is on quantum sensing and metrology, quantum communication, and quantum computing, including investments DoD should make to ensure the United States is not a victim of technological surprise. To reach the conclusions below, several databases of research publications and citations were accessed to determine who the top researchers are and where the top research is performed. In addition, several previous studies, recent press releases, and scientific publications were reviewed, to complement the extensive knowledge of this field by several of the authors of this report, and to identify those areas of quantum research that should be emphasized as important for the future of the DoD.

Conclusions

Quantum Sensing and Metrology

A large number of fields—such as magnetic, electric, photon, electromagnetic—can be sensed and measured with better precision than classical sensors. In addition, time, position, and acceleration can also be measured more precisely using quantum systems with both single and multiple qubits. A number of important applications have been proposed. However, no reliable demonstrations have occurred yet (e.g., quantum radar). Although this is definitely a growth area for quantum science and technology, the DoD needs to clearly understand the potential capabilities and what impact they can have.

We note that these technologies are not expected to be disruptive changes in the state of the art. Consequently, the rise of China in this field is not expected to lead to any dire strategic disadvantages. Although advanced quantum sensors can provide significant improvements in terms of size, weight, and power and performance in a number of different

missions, future advances in this area by China and others are not expected to lead to a quantum surprise.

Quantum Cryptography and Communication

Quantum key distribution (QKD) and quantum communication via "teleportation" using quantum repeaters have been very active areas of research and development, starting with the landmark work by Bennett and Brassard (BB84) and the experimental demonstration of atom teleportation by Blatt in 2004. This direction has become quite mature; several companies are producing hardware that can be used for QKD over kilometer-scale distances.

China is a dominant player in QKD technologies—China demonstrated QKD over a satellite link. But there are several challenges inherent in QKD (e.g., authentication) that currently preclude its use in practical applications. Although overcoming these challenges might be considered a "quantum-leap" in capability, there are several non-quantum alternatives to QKD for achieving secure communication. There is not much incentive to continue government support for this technology.

Quantum Computing

Given the broad prevalence of encryption methods that rely on prime factorization to secure communications, the rapid or sudden development of a working quantum computer that can implement Shor's algorithm to factor large numbers would constitute a quantum surprise. This particular concern is well known and is under close watch by the Intelligence Community. Other potential surprises that may be of particular concern to DoD are not obvious. To date, only a small number of niche problems have been identified in the literature where fault-tolerant quantum computing provides a clear advantage over traditional methods. This may change over time as researchers gain more experience in noisy intermediate-scale quantum (NISQ) computers, and it is worthwhile for DoD to monitor this area. Nevertheless, besides the potential impact on encryption, there is no clear strategic consequence to the rise of China and others in this field.

Recommendations

Overall, we recommend that DoD support for quantum information continue, although in a focused manner to heavily support those areas where applications important for the DoD have been identified or where some key capability is envisioned. Some specific areas that we feel are particularly important are those for precision navigation (time and position), magnetic field, electric field, and electromagnetic field sensing, and development of noisy intermediate- and large-scale quantum processors that can be heavily exercised to find what problems they can tackle that are difficult or impossible for classical processors.

1. Quantum sensing is a relatively mature field where capabilities that can be fielded could be realized in the near term (i.e., less than 5 years). Given this potential, we recommend that DoD make a concerted effort to transition the technology out of the lab and start exploring potential use cases in detail, with the eventual near-term goal of testing and fielding working prototypes.
2. Quantum Communication is not recommended as a priority for the DoD. In the particular case of QKD, it is not clear if there is much value in this area based on its current challenges and the availability of alternative approaches. Given that other countries, particularly China, appear to be heavily invested in this area, monitoring advances in QKD is prudent.
3. The DoD must be prepared to play a significant role in quantum computing, particularly throughout the (decade long) NISQ transitional phase, because quantum computing is a technology that can significantly contribute to a shift in the balance of power.
4. Short-term investment decisions by the DoD should be based on the strategic importance of quantum computing and simulation and not solely on applications that directly lead to new or improved military capabilities. At present, such applications for the DoD are unclear despite over 30 years of quantum computing algorithm research.
5. Develop a grounded understanding of practical quantum computing based on engineering and benchmarking to improve on preliminary analysis arguing for the advantage of quantum computers based on algorithmic complexity.
6. Do not invest in other approaches to quantum computing. In light of the limited applications of analog quantum computing, fundamental concerns regarding scalability, and division of effort over the range of approaches to quantum computing, investment by the DoD in analog quantum computing is not warranted. Results and conclusions from IARPA's quantum enhanced optimization effort, which is exploring many of these issues, should provide sufficient information in several years to reevaluate a recommendation for the DoD not to fund other forms of quantum computing.
7. The impact of quantum computing and simulations will be strategic and long term. The likelihood of technology surprise affecting military capabilities is low. The best way of avoiding surprise is with an open, long-term commitment to the development of quantum computing.

Contents

1. Introduction

A. Background

Within the last few decades, quantum science and technology have become areas of tremendous worldwide interest and have thus garnered significant investment. The Basic Research Office in the Office of the Under Secretary of Defense for Research and Engineering asked IDA to carry out this overview study of quantum technologies to identify where DoD funds should be focused to ensure that the DoD and the United States maintain their current advantage in this key scientific and technological field. We analyzed areas of quantum technology with the potential to change the way we sense, communicate, and compute. The focus of this report is on quantum sensing and metrology, quantum communication, and quantum computing, including investments DoD should make to ensure the United States is not a victim of technological surprise. To reach the conclusions below, several databases of research publications and citations were accessed to determine who the top researchers are and where the top research is performed. In addition, several previous studies, recent press releases, and scientific publications were reviewed, to complement the extensive knowledge of this field by several of the authors of this report, and to identify those areas of quantum research that should be emphasized as important for the future of the DoD.

We expect quantum technologies to have a significant impact on future military capabilities, although it is too early to decide where these impacts will occur. This report will assess the current state of quantum research around the world by examining the literature to determine the primary players and institutions. Trends in the movement of research dollars will also be followed, using press releases and private contacts.

We will review each of the potential key applications in some detail to provide a timeline to realize them, focusing on those applications that may be disruptive, particularly if realized outside the United States.

Finally, we will provide recommendations on how the DoD should proceed to mitigate the effects of unforeseen advances by our adversaries.

B. "Quantum Leaps" in Quantum Technology – How Important

Quantum mechanics may be the most important discovery of the 20th century since it enables many of the technological miracles we enjoy. Computers, phones, lasers, the internet, and information storage are among the technological innovations made possible by our understanding of quantum mechanics. Moreover, quantum mechanics also allowed

us to develop a deep understanding of sub-nuclear particles, atoms, molecules—in fact, the properties of all materials—almost everything around us. But it was not until the last few decades of the 20th century that certain features of quantum mechanics began to be seriously explored. These were the "spooky" features of quantum mechanics that even Einstein had difficulty accepting—*superposition* and *entanglement*. The reason superposition and entanglement took so long to become technologically significant is that they manifest themselves for very particular quantum systems that involve individual photons, electrons, electron spin, atoms, ions, and special superconducting rings and their interactions. Typically, both superposition and entanglement are fragile and occur in extremely short time periods before the environment destroys them.

To understand quantum computing, we must understand some properties of electrons, particularly their spin since they are a prototypical quantum system. They *spin* in two possible quantum states, +½ and –½, denoting *spin up* and *spin down*. Whenever the spin is "measured" it is in one of these two states. Quantum mechanics, however, allows the electron spin to be in a *superposition state*, which can be mathematically described as a linear combination of spin up and spin down. Thus, one can say the spin can be both spin up and spin down at the same time. If a number of electron spins are put into such a symmetric state and the spin state is measured, half will be up and the other half will be down. But there is no way to tell beforehand which electrons will be in which group. In fact, the spin can be put into an infinite number of these superposition states, and the outcome of any measurement reflects the coefficients of the terms in the linear combination. This property is what defines a *quantum bit*, or *qubit*, and it allows a qubit to "explore" an infinitely large space of potential values, whereas a *digital* (*classical*) *bit* can only explore 0 and 1. Herein lie the seeds of quantum computing.

Two electron spins become entangled when the measurement of one determines the measurement of the other despite the large distance (relative to their size) between them. Entanglement is also a property of photons, whose quantum states can be considered left and right polarization. If a single photon passes through a nonlinear medium that splits it into two, each part with half the initial energy, then the resulting photons can travel in different directions as long as momentum is conserved. These photons are entangled in a very special state called an *EPR state*, after Einstein, Podolsky, and Rosen. That is, the photons are in a symmetric superposition of left and right polarizations and can travel far from each other, but as longer they don't interact with the environment (*scatter*), the measured polarization of one will always be the opposite of the other. In other words, if the polarization of one is measured to be left, the polarization of the other will be measured right, despite perhaps being at different ends of the universe. This was the *EPR paradox*, which Einstein called "spooky action at a distance." Experimentally, the EPR state was confirmed and consequently became a strong validation of quantum mechanics.

Alas, the biggest impediment to using superposition and entanglement is that they are fragile states, easily destroyed by interaction with the environment. The *coherence time* is the time over which these states can be used for technology. It is the time in which operations involving these states can be done reliably before interactions destroy the "coherence" required. For example, for computing, the coherence time must be greater than 1000 times the time for a single *gate* or qubit operation. Even in this case, the quantum bit needs to have error-correction protocols, which require many backup qubits for each qubit needed for the computation.

C. Quantum Applications

The infinite "parallelism" provided by superposition and entanglement is the basis for many applications and the development of new technologies:

- **Quantum sensing and metrology** are important applications that provide significant improvements in capabilities such as *precision timing, navigation,* and *sensing*. These benefit from the fact that entanglement increases the precision by the number of entangled qubits rather than by the square root of the number of bits as for classical systems.
- **Quantum communications,** including quantum key distribution (QKD), enable completely new capabilities that could not have been done without superposition and/or entanglement. These are theoretically absolutely secure because they are based on single qubits, typically photons whose quantum states cannot be cloned. Note, however, that there are still many challenges to implementing these in a fully secure way because of technical issues rather than theoretical ones.
- **Quantum computing** has the promise of providing orders-of-magnitude enhancements to computing because of the resources currently required for some algorithms, such as Shor's algorithm for factoring of large numbers. This algorithm scales polynomially due to the infinite phase space that can be explored by a single qubit as opposed to a classical bit. Thus, it provides a feasible way of factoring very large numbers orders of magnitude faster than the algorithms possible on classical computers. There are significant challenges to implementing the type of fault-tolerant quantum processor that can tackle this algorithm, however, and it may still be several decades away from fruition.

Simulating quantum systems using arrays of qubits whose interaction can be controlled to mimic various *Hamiltonians* of interest is another capability that is new; it was one of the original motivations for quantum computing and it may be an early application of quantum computing that provides key understandings of material systems unobtainable in any other way.

The breadth of applications and their importance has provided impetus for the worldwide emphasis on research on quantum information, including large efforts in China, Europe, Japan, Russia, Australia, and Canada. Although these efforts are primarily focused on basic research, a growing amount is applied research with the intent of demonstrating "quantum supremacy"—the moment when quantum computers will be able to perform a computational problem that cannot be done using traditional or classical techniques or infrastructure.

2. Methodology

A. Scope

This review only looked at quantum areas that are enabled or facilitated by the special quantum properties of superposition and entanglement previously described. These topics were succinctly reviewed for their technological importance and potential disruptive capability.

B. Quantum Technology Landscape

Various sources such as the Web of Knowledge or Google Scholar were used to determine the most cited researchers and most cited areas of quantum research or technology. We felt that there was a definite correlation between the importance of the work, the technical area, and the number of citations. Even though there were some omissions since some work, particularly that conducted outside the United States, is not published and therefore not cited, we feel that we captured a complete picture of the quantum landscape in this way.

Depending on the particular quantum area and the number of citations, we have identified either the top-10 or top-20 researchers in each of the topic areas. We typically determined the primary researcher as the last author. This is a standard procedure when publishing a scientific paper. Usually, the first author, often a student or postdoctoral fellow, contributes most to the research; the last author is the professor or the principal investigator for the research. We have, however, catalogued both the first and last author of the most cited publication, as well as the country of origin of these authors, to determine where the key elements of the work were performed. This information has been analyzed and put in a form that we hope will enable us to infer what might be a disruptive technology, where it may be developed, what might be the timeline, and what research gaps need to be filled by appropriate resources.

C. Topical Surveys

- Quantum sensing that can enable the sensing of various fields (e.g., magnetic and electric) with unprecedented sensitivity.
- Quantum metrology that can provide, for example, the highest precision atomic clocks and measure acceleration or rotation with unprecedented precision.

- Quantum communication that enables ultra-secure communication using exotic transfers of quantum information like teleportation.
- Quantum cryptography and QKD that enable the generation of encryption keys that are proved unbreakable (with certain caveats).
- Quantum computing and related development of quantum algorithms that can provide significant speedup in computing problems that are extremely difficult to solve or inaccessible for conventional computers.

3. The Quantum Technology Landscape

A. Citation Metrics

To infer where significant quantum computing research is conducted, or has been conducted in the past, we built a database from some of the most cited papers in quantum physics. We extracted research-paper data from the Web of Science database. Specifically, for each quantum-related topic, we extracted the 30 most cited papers—30 being arbitrary—recognizing that after the top 10 to 20, the rest of the papers were minimally cited. Additionally, though the oldest paper was published in 1973, in our database citations do not begin appearing until 1991. For each quantum-related topic, the authors and countries with the most citations provide an indirect signal to the sources of important research. We then aggregated the authors and ranked them according to their citation counts. Thus, by taking note of their affiliations, organizations, and countries, we could glean an understanding of the research landscape across the globe, especially novel research. For each area of research, we found the nationalities of the top-50 most cited researchers. Figure 1 summarizes our findings.

The European Union's research is just as advanced as that in the United States, with countries such as Austria, Germany, and the Netherlands leading the way. Although China has been breaking ground in quantum communications research, it still does not have the most cited researchers.

We also tracked the current state of research for quantum sensing, quantum computing, and quantum communication across the globe. In Figure 2, we see how Europe, Russia, and China's efforts compare with those of the United States, both as a whole and within the last 5 years. It is clear from these graphs that the United States and Europe are dominant in research on quantum computing both overall and in the last 5 years, but it is also clear that China, which is a close third in quantum sensing overall, has in the last 5 years overtaken both the United States and Europe in publications and Europe in citations. In quantum communications in the last 5 years, China has overtaken the United States and Europe in publications but still lags in citations.

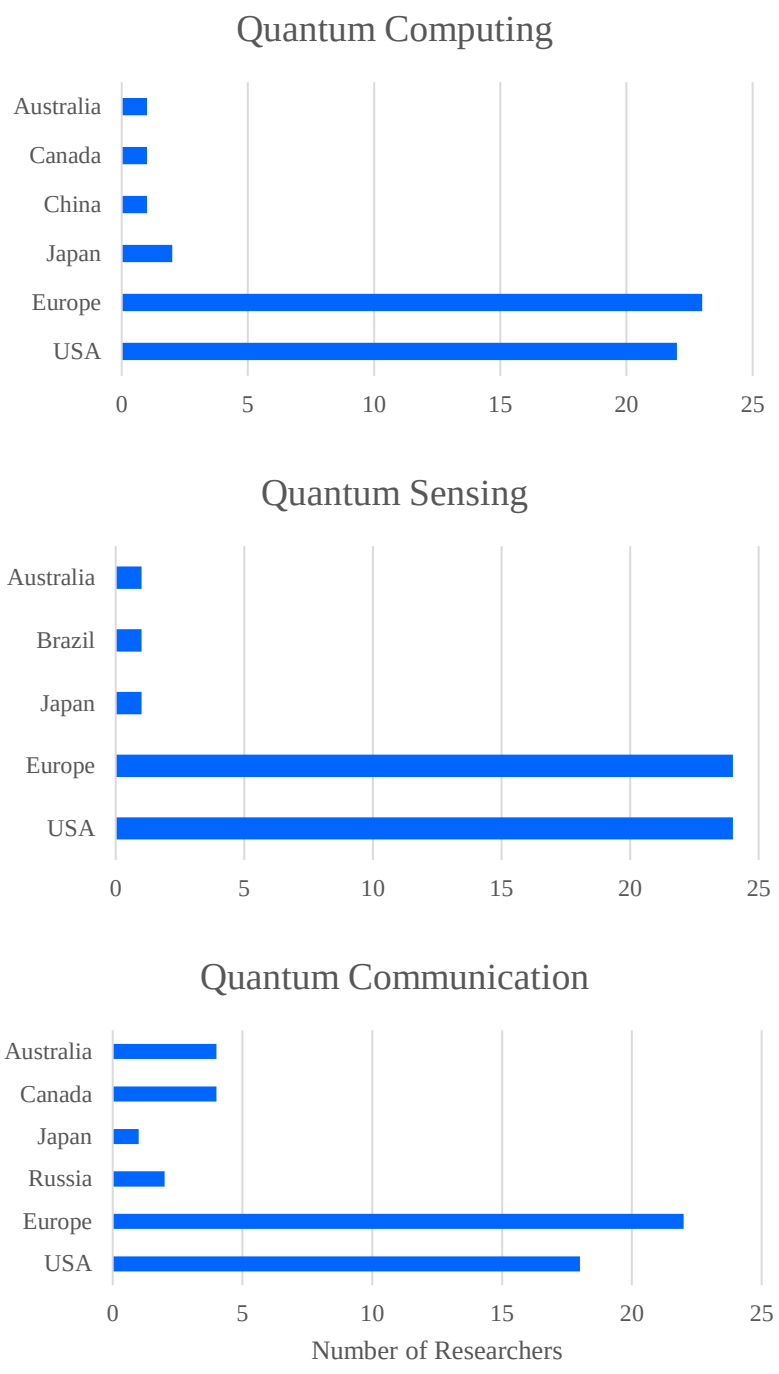


Figure 1. Nationalities of the Top-50 Most Cited Researchers in Quantum Computing, Quantum Sensing, and Quantum Communication

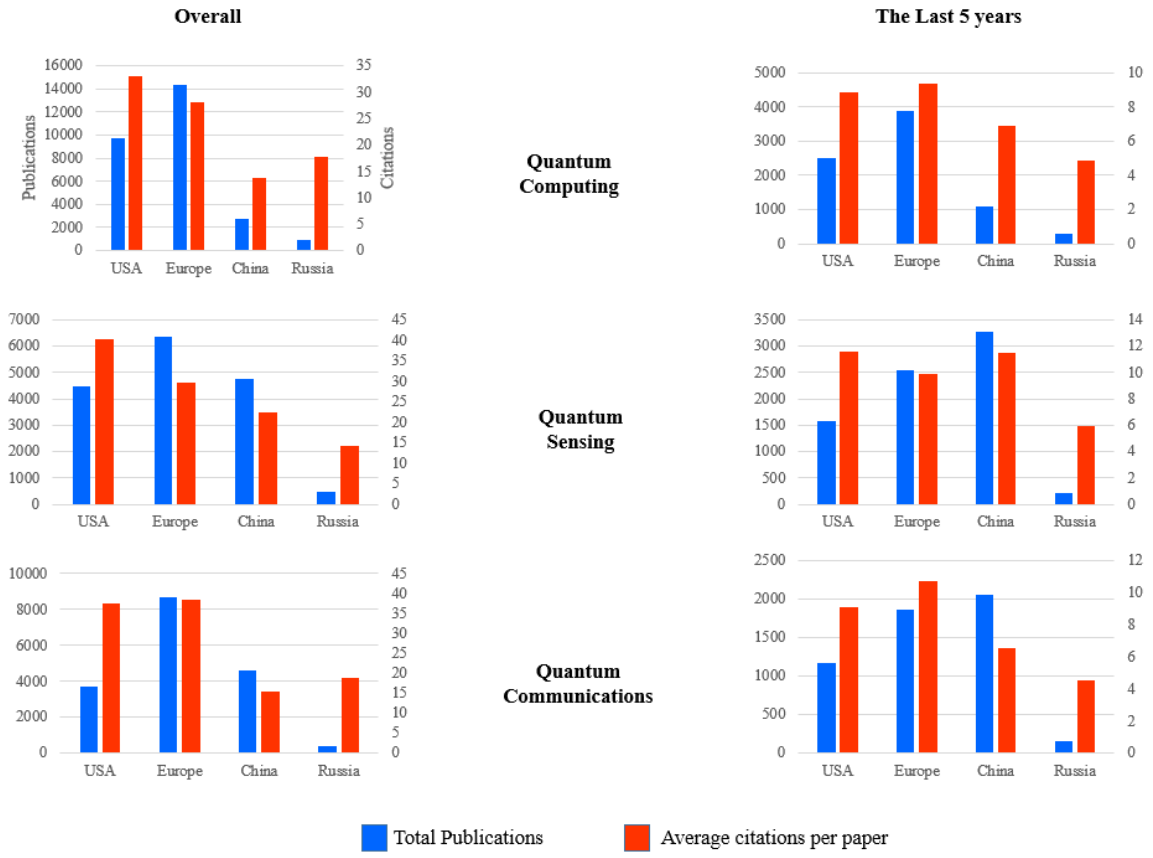


Figure 2. Current State of Research for Quantum Sensing, Quantum Computing, and Quantum Communication

B. Research Funding by Country

From a survey of newspaper articles published worldwide, we were able to garner ideas of how much countries are funding their research efforts. The European Union's "The Quantum Manifesto," which calls on Member States to invest a €1 billion initiative in quantum technology, is set to launch this year.[1] Although it is not a step-by-step plan to accomplish quantum goals, the initiative is proof that the EU plans to take on the ambitious and long-term commitment to advance quantum technologies. The manifesto was endorsed by more than 3400 experts across Europe.

The United Kingdom spends approximately $1 billion annually on technology research and postgraduate training, where quantum technologies accounts for about $40 million of this figure (Figliola 2018). Moreover, in 2013, the UK established a 5-year, $440

1 "Quantum Manifesto: A New Era of Technology," May 2016, http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf.

million National Quantum Technologies Program to push quantum R&D into commercial technologies.

In February 2018, SK Telecom—South Korea's largest wireless carrier—invested $65 million in ID Quantique of Geneva, Switzerland.[2] ID Quantique is currently the global leader in quantum safe cryptography and quantum-sensing solutions.

China declared quantum research as one of four "megaprojects" in its 15-year science and technology development plan for 2006–2020. Its annual funding has been estimated at $244 million (Figliola 2018). In 2017, China announced that it would begin building an $11 billion national quantum laboratory in the city of Hefei, due to open in 2020 (Herman 2018). It is difficult to ascertain the accuracy of these figures.

In Australia, Q-Ctrl, a 15-person company, became the country's first quantum tech startup. It was founded by the University of Sydney's Professor Michael Biercuk. The company produces Black Opal, a platform on qubits that reduces decoherence and errors at the physical layer. By the summer of 2018, Q-Ctrl had secured four major venture capital (undisclosed) funds: Sequoia China, which backed Google, Instagram, and PayPal; DCVC (also known as Data Collective), which previously invested in Square, Facebook, and Verisign; Rigetti Computing, the California-based developer of quantum integrated circuits; and Horizons Ventures of Hong Kong, which previously funded Spotify, Skype, and Facebook.[3]As a whole though, there is a lack of open-source data on government and private sector funding of quantum R&D for many countries, including China and even startups across the United States, Europe, and the Middle East.

---

[2] Catherine Simondi, "ID Quantique partners with SK Telecom," IDQ press release, February 26, 2018, https://www.idquantique.com/id-quantique-sk-telecom-join-forces/.

[3] George Nott, "Quantum Tech Start-up Q-Ctrl Secures Major VC Backing," July 10, 2018, CIO from IDG, https://www.cio.com.au/article/643582/quantum-tech-start-up-q-ctrl-secures-major-vc-backing/.

4. Quantum Technology Topic Areas

A. Quantum Sensing and Metrology

1. Basic Principle

Quantum sensing and metrology covers a broad array of technologies that take advantage of the strong sensitivity of certain quantum systems to measure various physical quantities. The details vary with the quantum system and the signal of interest, but the implementations generally include one or more of the following features (Degen, Reinhard, and Cappellaro 2017):

1. Quantized energy levels—an external signal either introduces a measurable shift in the energy levels or changes the transition rate between levels (e.g., the Zeeman effect for magnetic fields).
2. Quantum coherence (e.g., superposition, wave-particle duality)—quantum wave functions can constructively or destructively interfere; interaction with the environment can introduce relative phase shifts that alter the interference patterns (e.g., atomic interferometry).
3. Quantum entanglement—quantum correlations between individual quantum sensors (e.g., qubits) can be used to perform a type of coherent sensor fusion to improve measurement precision beyond the "standard quantum limit."

A wide range of quantum systems with one or more of the above features have been exploited to perform sensitive measurements. Here, we discuss a handful of such systems. Table 1 provides a summary of technologies and potential applications.

Table 1. Quantum Sensing Technologies and Potential Applications

Technology	Measured Quantities	Potential Applications
Atomic vapors	Magnetic fields, rotations, time	Navigation, precision clocks
Trapped ions	Magnetic and electric fields, force, rotations	Precision gravimeter, navigation, precision clocks, small-scale imaging
Rydberg atoms	Electric fields	Electrically small RF detectors
Quantum dots	Electric and magnetic fields	Small-scale electric sensing
Nitrogen vacancy centers	Magnetic and electric fields, temperature, pressure, rotations	Small-scale electric or magnetic sensing, navigation

Technology	Measured Quantities	Potential Applications
Superconducting circuits	Magnetic and electric fields	Small-scale imaging
Cold atomic matter waves	Magnetic fields, acceleration, rotation, time	Precision gravimeter, navigation, precision clocks
Quantum illumination	Photon counts	High contrast active sensing (e.g., quantum radar)

Source: Adapted from Table I in Degen, Reinhard, and Cappellaro (2017).

a. Atomic Interferometry

At very low temperatures, atoms can exhibit wave-like behavior that is similar to light. These coherent "matter waves" can be used to measure quantities that interact with mass (e.g., acceleration, rotations, etc.) by observing changes in wave interference patterns. The general concept involves coherently combining two matter waves that propagate through separate paths in the environment. Differences in the external potential between the two paths will have a predictable effect on the interference pattern that can be measured. Entangled atoms can also be used to improve sensitivity (Degen, Reinhard, and Cappellaro 2017; Barrett, Bertoldi, and Bouyer 2016).

b. Quantum Illumination

Quantum illumination (or so-called quantum radar) is a sensing scheme that leverages quantum correlations to improve the signal-to-noise ratio of target detection in active sensing (e.g., radar or lidar) (Lloyd 2008). The basic concept is that signal photons are first entangled with local qubits and then emitted toward the target. Measurements on these auxiliary qubits (or "ancilla" qubits) can then be used to reject photons from noise sources, improving signal to noise. This enhancement can be realized even if environmental noise destroys the entanglement with the signal photons (Zhang et al. 2015).

c. Atomic Vapors

High-density atomic vapors have been shown to be sensitive detectors for magnetic fields at room temperature or above (Degen, Reinhard, and Cappellaro 2017). Neutral atoms like potassium can be spin-polarized by a laser, effectively creating quantum magnetometers. In the presence of a magnetic field, the atoms will undergo state transitions that can be measured optically to infer the strength of the external field or its gradient (Dang, Maloof, and Romalis 2010; Kominis et al. 2003). Entanglement between vapor "cells" can also be used to improve sensitivity (Wasilewski et al. 2010).

d. Trapped Ions

Trapped ions can be used to measure a number of different physical quantities, including applied forces, electric and magnetic fields, and time. Ions trapped by electric or magnetic forces effectively form a controllable crystal with quantized modes of motion. External forces from the environment can lead to detectable transitions between these modes, providing a scheme for highly sensitive measurements of force or displacement (Biercuk et al. 2010). There are also sensing schemes that involve single trapped ions. For example, external radio frequency signals can excite an ion into a quasi-stable state that serves as a precision clock reference (Diddams et al. 2001). Also, weak forces can be sensed by single ion-traps by using lasers to couple motional modes to spin modes (Ivanov, Vitanov, and Singer 2016).

e. Rydberg Atoms

Rydberg atoms are atoms in highly excited electronic states that can be used to measure electric fields at room temperature (Facon et al. 2016). In general, Rydberg atoms have large dipole moments that cause the atoms to move in the presence of external fields. More specifically, the atoms transition between quantized levels of motion that can be detected with lasers or other measurement schemes. One of the main appeals of Rydberg atoms as an electrometer is that the performance of the sensor is not geometry dependent, in contrast to classical antennas where the size of the detector system cannot be much smaller than a wavelength of the signal of interest. This is the well-known Chu limit for classical antennas, which may be overcome by Rydberg atom quantum sensors (Cox et al. 2018).

f. Superconducting Circuits

Quantum circuits based on the Josephson effect can be used for a number of quantum sensing applications. The Josephson effect, which describes quantum tunneling at the interface of two superconductors, can be used to create macroscopic quantum systems that can be controlled with radio frequency signals. Superconducting quantum interface devices (SQUIDs), which have been used for some time to measure magnetic fields, are currently used in neural magnetic imaging (magnetoencephalography). Superconducting qubits based on charge or magnetic flux can be used to make sensitive measurements of electric and magnetic fields, respectively (Degen, Reinhard, and Cappellaro 2017).

g. Nitrogen Vacancy Centers in Diamond

Diamond crystals having nitrogen vacancies provide ensembles of electronic spin defects that can be used as qubits for quantum sensing at room temperature or higher (Degen, Reinhard, and Cappellaro 2017). Similar to atomic vapors, the spin states in the nitrogen vacancy centers can couple with external magnetic fields to produce state

transitions that can be measured to infer the external fields (Taylor et al. 2008). Negatively charged nitrogen vacancy centers can be used to measure rotations by exploiting a quantum phenomenon known as Berry's phase (Ledbetter et al. 2012).

2. Key Metrics

Performance metrics in quantum sensing will generally vary with application; however, some metrics common to most quantum sensors include the following (Degen, Reinhard, and Cappellaro 2017):

- Sensitivity—the signal that gives unity signal-to-noise ratio after 1 second of integration time. This essentially describes the coupling between the quantum system and the physical quantity of interest.
- Decoherence/relaxation time—the length of time the quantum system remains resistant to noise from the environment and stays "quantum–like."
- Dynamic range—the ratio of the maximum and minimal detectable signal.
- Sampling rate—how often the signal is sampled. Also determines the bandwidth of the measurement.
- Operating temperature—the temperature range the system can operate in. Many quantum systems require approximately milli-Kelvin temperatures.

3. Potential Applications

a. Precision Navigation and Timing

One area of active research for quantum sensor technologies is how to leverage highly precise measurements of frequency, acceleration, rotation rates, and electric and magnetic fields for use in high-precision navigation and timing. Current navigation relies primarily on a global navigation satellite system, such as the Global Positioning System (GPS). In situations where GPS cannot be used as a reliable means of navigation, such as underwater or in dense urban environments, inertial navigation systems are used to determine the position, orientation, and velocity of a moving object. However, current inertial navigation systems drift over time due to integration error and require periodic GPS fixes to correct and adjust position and velocity measurements. Quantum sensors, on the other hand, are expected to deliver significantly more precise measurements of acceleration and rotations, reducing integration error, hence precluding the need for frequent GPS updates. In addition, high-precision quantum magnetometers or gravimeters can be used to map local features of Earth's magnetic and gravitational field, providing an alternative positioning system to GPS. Such sensors can be used for navigation in areas where GPS is not available (e.g., underwater) or cannot be used reliably (e.g., where denied by an adversary).

Efforts to develop quantum navigation systems are currently ongoing in the United States and the UK. In 2018, the UK developed a functioning laboratory prototype designed to fit on larger vehicles such as ships and trains. The Atomic Clock with Enhanced Stability (ACES) program at the Defense Advanced Research Projects Agency (DARPA) is currently working to develop smaller and more accurate chip-scale atomic clocks.

The ability to navigate in GPS-denied environments could enable missions that were not possible before. One example is undersea warfare. Currently, submarines rely primarily on inertial navigation systems when operating below the surface and ascend to the surface or to periscope depth periodically to fix their position via GPS or other satellite systems. Quantum sensors that enable submarines to navigate underwater for extended periods of time could provide a strategic advantage, as submarines at or near the surface are more vulnerable to detection and tracking by adversaries.

Other examples include situations where GPS is disabled by the actions of an adversary. Improved inertial navigation capabilities could provide a tactical advantage for a variety of air and ground systems by allowing those systems to operate in hostile environments.

b. Electrically Small Antennas

Quantum sensors based on Rydberg atoms can potentially be used as electrically small antennas that surpass the so-called Chu limit. In conventional antennas, the size of an antenna scales roughly with the wavelength of the expected signal. Hence, microwave antennas that operate at 3 GHz or below must be at least on the order of a few centimeters to reliably detect desired signals. Rydberg atoms, on the other hand, are not limited by this constraint and can be as small as a few microns. This feature could allow for radios in many different form factors that can significantly lower the size, weight, and power (SWaP) of current communication and RF sensing technologies.

This potential is currently being examined by DARPA in the Quantum-Assisted Sensing and Readout (QuASAR) program. A “Rydberg Radio” was also recently demonstrated (Anderson, Sapiro, and Raithel 2018).

c. Small-Scale Sensing

Quantum sensors can be used for small-scale sensing applications by overcoming the limits of classical optics. These can be used to detect and generate images of concealed and/or obscured objects, or objects that cannot be detected using classical imaging systems. Most of the current research efforts have focused on leveraging quantum entanglement to image objects with a resolution or signal-to-noise criteria that are beyond what is possible in classical imaging systems.

Potential applications in this area include using quantum sensors to image in low-light conditions or low signal-to-noise levels, imaging small-scale structures, and remote sensing with ghost imaging, which uses pairs of entangled photons to detect and generate images of objects without directly coming into contact with them.

The primary areas of interest for imaging small-scale structures that require image resolutions beyond the limits of classical optics lie in biological and medical applications, for example using quantum imaging to view biological processes such as enzyme and protein activity at the nanoscale. The other uses for quantum imaging have potential extensions to defense applications. The ability to image in extremely low-light conditions could enable an advantage in tactical situations, such as nighttime operations, where soldiers currently rely on image intensifiers to visualize their surroundings. The ability to detect objects with low signal-to-noise ratios or with concealed visible signatures could provide an advantage in target detection, classification, and identification and potentially counter adversaries' camouflage or other target-deception techniques.

Quantum sensors as small-scale imaging devices are currently being explored by DARPA in the Atomic Magnetometer for Biological Imaging In Earth's Native Terrain (AMBIIENT) program. The program seeks to develop high-precision, low-SWaP magnetometers for medical imaging and navigation.

d. High-Contrast Active Sensing (stealth defeat)

Traditional radar relies on sending and receiving radio waves to detect targets. Low-observable, or stealth, technology attempts to avoid detection by redirecting a radar system's signals, preventing sufficient signal from returning to the radar receiver and revealing the target's location. A potential application for quantum sensing is high-contrast active sensing, also referred to as quantum radar.

The quantum radar uses entangled photon pairs to pick out the reflected signal. This allows the quantum radar to potentially recognize received signals as target detections even when the signal-to-noise ratio is too low for conventional radars. This could potentially allow for the detection of stealthy targets or targets in high-clutter environments and reduce the efficacy of radar-jamming techniques.

In 2018, China claimed to have developed a prototype quantum radar, and Canada has also invested efforts in pursuing the technology. From currently available reports, it is unclear how mature either of these efforts are.

For quantum radar to provide an improved capability over conventional systems, a high-throughput source of entangled photons is needed. Developing such a source is technically challenging and to date has not been publicly demonstrated. In addition, theoretical studies suggest that the advantage in signal-to-noise ratio of quantum radar

compared with a conventional system with similar output power is limited to 6 dB (i.e., a factor of 4). It is unclear if this advantage is adequate to defeat stealth in typical scenarios.

The potential strategic implications of employing quantum radar to defeat stealth depend on which countries develop and implement the technology. The ability of U.S. adversaries to defeat stealth through the use of quantum radar could provide them with a strategic advantage and force the United States and its allies to alter current tactics that rely on stealth. To some extent, however, U.S. adversaries are already developing and employing tactics and technologies to reduce the advantages that stealth provides to Blue forces, and it is unclear if the quantum radar would be able to provide an additional significant advantage in this area. The quantum radar may have a larger impact on applications such as Blue force missile or hypersonic weapons defense, where conventional radar has difficulty detecting targets with sufficient accuracy and timeliness. In these applications, the quantum radar may enable missions or tactical strategies that are not possible with conventional radar.

e. Precision Gravimeter

Another potential application for quantum sensors is the quantum gravimeter, which leverages superposition to make highly precise measurements of the strength of gravity. Subtle changes in Earth's gravitational field can indicate the presence of oil or certain minerals or objects below ground or underwater. A quantum gravimeter could be used by oil and gas companies to detect deposits of oil and minerals or by construction companies to locate pipes buried deep underground. Gravimetry is already currently used in geophysical research and petroleum and mineral prospecting. However, current gravimeters cannot reach the levels of sensitivity that a quantum gravimeter could. For defense applications, a quantum gravimeter could potentially be used to detect camouflaged vehicles and aircraft, or concealed threats such as improvised explosive devices.

The technology for quantum gravimetry is relatively mature. To date, a few quantum gravimeters are commercially available. These include gravimeters developed by AOSense in the United States and by M Squared in the United Kingdom.

4. Recommendations

With the exception of quantum radar, quantum sensing is a relatively mature field where capabilities that can be fielded could be realized in the near term (i.e., less than 5 years). Given this potential, we recommended that DoD make a concerted effort to transition the technology out of the lab and start exploring potential use cases in detail, with the eventual near-term goal of testing and fielding working prototypes. This effort includes initiating studies to identify capability gaps that quantum sensors can address and

examining both incremental and novel uses of quantum sensors (e.g., whether high-precision synchronized clocks enable capabilities that were impractical beforehand).

Although quantum sensing technologies are not expected to be disruptive changes in the state of the art, we recommend that DoD stay abreast of adversary developments in these technologies.

B. Quantum Communications

1. Basic Principle

Quantum communication describes various technologies for transmitting quantum information across channels. This can either allow networking between quantum systems or improve the capabilities of classical communication channels. In general, these technologies rely on one or more of the following key features in quantum information theory (Gisin and Thew 2007):

1. Entanglement and non-locality—Entanglement allows for "non-local" correlations where two distant parties can essentially share the same quantum state. Actions on a shared entangled state by one party can affect the dynamics observed by another.
2. Quantum Uncertainty—Quantum uncertainty is a fundamental property of quantum systems, where certain pairs of physical properties cannot be known simultaneously with arbitrary precision. This allows for so-called complementary coding, in which a party must know how a quantum state is prepared to extract information from it.
3. No-cloning theorem—This theorem maintains that an unknown quantum state cannot be cloned with 100% fidelity without disturbing the state in some way. Hence, a party must have knowledge of the quantum state to prepare exact copies.

These key results in quantum information theory allow for a number of interesting applications in information processing and transmission. We now briefly discuss some of the main areas in the field.

a. Quantum Networking

The general goal of quantum networking technologies is to pass quantum information across distance channels at high throughput and low loss. This is especially challenging given the fragility of quantum states and the no-cloning theorem. However, a number of techniques leverage entanglement to improve channel efficiencies. These include quantum teleportation, entanglement swapping, entanglement purification, and super-dense coding.

These techniques allow for intermediary nodes called "quantum repeaters" that preserve quantum fidelity, enabling long-distance transmission of quantum information.

Physical implementations of quantum channels are almost exclusively done with photons because of their long coherence times and their suitability for long-distance transport. Hence, many of the enabling technologies in quantum networking involve low-loss mediums such as optical fibers, the efficient generation of single photons (especially of entangled pairs), accurate manipulation of photonic states, storage and retrieval of photonic quantum information (i.e., "quantum memory"), and efficient and accurate detection of photonic states. Table 2 lists some notable examples of such technologies.

Table 2: Photonic Technologies for Quantum Communication

Photon Sources	Parametric down converters Quantum dots Four wave mixing resonators Nitrogen vacancy centers in diamond Solid state
Photon Manipulation	Femtosecond laser writing UV writing Integrated quantum circuits
Photon Detection	Single photon avalanche photodiode Transition edge sensor Space (time) multiplexing Nanowires
Quantum Memory	Rare-earth ion-doped solids Nitrogen vacancy centers in diamond Raman scattering in crystalline solids Alkali metal vapors Molecular storage and processing

Source: Flamini, Spagnolo, and Sciarrino (2018); Heshami et al. (2016).

b. Quantum Cryptography, Quantum Key Distribution

Quantum cryptography describes a general area of research that examines the use of quantum information theory (particularly the features discussed above) to obscure information (e.g., communication that prevents eavesdropping). The vast majority of research in this field is in QKD. The goal of QKD is to use a quantum channel to transmit a secret "key" between two parties (say Alice and Bob), which can subsequently be used with conventional normal cryptographic schemes (e.g., one-time pad). Due to the no-cloning theorem, an eavesdropper (Eve[4]) must make measurements on the quantum states

[4] In quantum cryptography, it is typically assumed that Eve has access to unlimited resources and can mount any attack that is allowed by quantum mechanics.

sent through the channel to discern any information about the secret key. However, since such action will disturb the channel, Eve's presence can be detected if Alice and Bob follow a proper protocol. A number of such QKD protocols under study have proved to be "information-theoretic secure," meaning that the security is based on information theory rather than public-key encryption, which relies on computational hardness to ensure security.

A challenge with QKD protocols is that the security relies heavily on the quality of the physical hardware. For example, the well-known BB84 protocol assumes an ideal single-photon source. Actual photon sources will sometimes emit several photons, making the protocol susceptible to a clever "photon-number-splitting" attack. In addition, QKD implementations that rely on photon polarization are susceptible to a "Trojan-horse" attack where the eavesdropper uses a laser to probe the sender's (Alice's) equipment to extract information without being detected. Such attacks are examples of quantum hacking, a field of study examining the limitations of QKD implementations. There is active research in developing device-independent quantum cryptography protocols that are robust to quantum hacking techniques (e.g., the "decoy state" protocol to prevent photon-number-splitting attacks); however, in general, QKD protocols must assume some level of quality in the underlying hardware to ensure security. This is a noted difficulty in certifying the security of technologies implementing QKD.

2. Key Metrics

Key performance metrics in quantum communication technology include the following:

- Channel losses—the amount of attenuation in the channel. This effectively determines the probability of a single photon traversing the media and is determined by the photon wavelength, type of medium, and temperature.
- Channel noise—describes operational errors such as depolarization, dephasing, etc. that can alter the state of the photon in passage.
- Transfer rate/Secure Key Rate—in QKD, the number of bits per second successfully transmitted for use as a secure key. This includes the quantum bit-error rate inherent in the protocol to ensure security.

The list above is by no mean exhaustive. Some key metrics will depend on the enabling technology of interest. For example, for single photon sources, the number of photons emitter per second is a key metric.

3. Potential Applications

a. Secure Communications

The most touted application of quantum communications technology is the potential for "unconditionally secure" communication via QKD. Current encryption technologies generally rely on "computational hardness" to ensure security, which can potentially be defeated in the future by advanced computing capabilities, such as a quantum computer implementing Shor's algorithm. Note that this potential weakness is not just a concern for future communications; an adversary could intercept and store encrypted traffic and wait for computing technology to advance (e.g., a quantum computer to be developed) to decrypt the traffic. This potential weakness in current encryption techniques has driven a great deal of interest in post-quantum encryption techniques. Since QKD relies on fundamental properties of quantum information instead of computational hardness to ensure security, QKD can potentially fill this gap.

A number of technologies have been reported in the media and elsewhere that claim to provide secure communications via QKD. A high-profile example is the Quantum Experiments at Space Scale (QUESS) project that demonstrated QKD between the Chinese Micius satellite and ground stations in China and Austria. There are also several companies offering commercial products that implement QKD protocols, among them ID Quantique in Switzerland, MagiQ Technologies, Inc. in the United States, QuintessenceLabs in Australia, and SeQureNet in Paris.

Despite this promise, there are many practical challenges to successfully implementing QKD. The most notable challenge is authentication (e.g., Alice confirming that she is communicating to Bob and vice-versa). QKD still requires a classical channel to implement the protocols, so an eavesdropper (Eve) can pretend to be Bob unless there is some way to verify Bob's identity. Although there are various workarounds under study (e.g., position-based verification), there is currently no scalable solutions to this issue that does not rely on current classical encryption techniques.

Another practical challenge in QKD is certifying that a channel is secure. As mentioned earlier, the security of QKD relies heavily on the capabilities of the physical hardware. To verify that an implementation of QKD is secure, one needs to verify that the source, repeaters, detectors, etc. are within standards and that the channel losses are within certain thresholds. This is in contrast to software-defined encryption schemes, where certifications are based on calculations. QKD therefore requires a different way of thinking than what is typically practiced in the cryptography community. In fact, these practical issues were noted by the U.S. Government in its decision not to certify QKD-based systems for securing U.S. Government information.

b. Quantum Transport/Quantum Internet

Quantum networking would allow quantum technologies such as sensors and quantum computers to exchange information. This could allow for distributed quantum computing and sharing of remote quantum capabilities. The transport of quantum information across lengthy channels has been demonstrated under varying conditions, so the underlying technology is relatively mature. However, since many of these capabilities (e.g., quantum computers) have not yet been realized, the potential for a quantum internet is not yet fully appreciated.

4. Recommendations

The case for continued investment in QKD is weak. As discussed above, fundamental challenges such as authentication limit practical implementations of QKD, and it is unclear if QKD provides any definitive advantages over non-quantum alternatives (e.g., post-quantum cryptography). Although heavy investment in QKD by China and other countries may suggest that this area should be closely monitored, it is expected that the Intelligence Community will take on this role. Hence, continued DoD investment in this area is not recommended.

C. Quantum Computing and Simulation

There are many excellent introductions to quantum computing covering (1) the basic concepts (Nielsen and Chuang 2010; Preskill 2018; Ladd et al. 2010), (2) physical platforms (Clarke and Wilhelm 2008, Blatt and Wineland 2008), and (3) algorithms (Montanaro 2016, Childs and Van Dam 2010). In particular, we highly recommend the recent National Academy of Science report *Quantum Computing: Progress and Prospects* (Grumbline and Horowitz 2019). This report should be noted for its fair (unbiased), complete, and up-to-date discussion of quantum computing.

Several factors govern the transition of quantum computing from a research topic to a sustainable computing technology. Ultimately, the most important event for quantum computing is that a quantum computation (1) has a customer (either a government or a commercial company) willing to pay for it, and (2) the computation is beyond the means of other commercially computation technology. Until that happens, quantum computing will be supported as a research effort, either commercially or by the government (including foreign governments).

At present, there is significant interest from commercial companies, including IBM, Microsoft, Google, and Intel. There are also a number of startups pursuing quantum computing, such as Rigetti and IonQ. Commercial interest is not limited to the United States. The Chinese company Alibaba, for example, has efforts in quantum computing.

The invention of Shor's algorithm in 1994 (Shor 1994) was a key event in causing quantum computing to be viewed as a serious computational means that, while still far from practical, nevertheless held the potential of performing computations far beyond the reach of classical computation. Specifically, Shor's algorithm factors integers. Such capability would break RSA public-key encryption and many other variants of public key encryption, which is the basis for the security of the Internet, the DoD, and other pieces of critical cyber infrastructure. Shor's algorithm has a super-polynomial speedup in algorithmic complexity. This caught the interest of NSA, which has invested in classified and unclassified quantum computing research for decades. Much of the unclassified research in the Intelligence Community has been sponsored by the Director of National Intelligence through the Intelligence Advanced Research Projects Activity (IARPA) and NSA's Laboratory for Physical Sciences in the Research Directorate.

Interest was primarily restricted to government and academia, but as progress in complementary metal oxide semiconductor (CMOS) technology slowed and now faces fundamental limits to miniaturization, interest in quantum computing as an alternative computing technology increased. While no one expects a quantum bit, or a qubit, to cost the same as a classical bit (a few CMOS transistors) it was speculated that other (important) quantum algorithms could have super-polynomial or at least significant polynomial speedups and thereby justify the cost of a quantum computer.

1. Quantum Computing Models

The fundamental laws of quantum mechanics govern a quantum computation. The information is the physical (quantum) state, whereas in a classical computation the information is discrete, represented in a classical physical state, and manipulated via changes to its physical state. A quantum computation therefore relies on superposition and entanglement. It is also a coherent state, meaning the state is described by amplitudes that can constructively and destructively interfere. Quantum computing gains its advantage through entanglement, superposition, and coherent evolution. Maintaining the coherence of the quantum state has proved difficult to achieve.

There are several classes of quantum computer. This report is primarily focused on the gate-based quantum computer using the quantum Turing machine model as defined in Deutsch (1985). It extends the classical Turing machine into the quantum domain, where the state of the computation is a quantum state and that state evolves according to the laws of quantum mechanics through the application of discrete gates. Because the gates perform discrete transformations this can be thought of as a digital quantum computer.

In the hierarchy of digital computation models, the digital quantum computer is the most powerful, just above the classical Turing model. In this hierarchy, each compute model encompasses all the models below it and has additional capabilities that cannot be provided by any of the lower compute models. The quantum Turing machine is potentially

the most capable form of digital computing we know of. But quantum computers may have value because of their ability to more efficiently perform computations of interest than alternative (classical) computational models.

In addition to digital quantum computers, there are also analog quantum computers, such as the D-wave machine. Initially, the D-wave machine was an adiabatic quantum computer, but when it proved too hard to control the noise, the D-wave machine became a quantum annealer, primarily for optimization problems. Another example of an analog quantum computer is the coherent Ising machine (Inagaki et al. 2016).

In classical digital computers, noise is eliminated from each operation by a thresholding operation. Occasionally, this thresholding operation will lead to an error in computational state, and such errors can be caught by error detection and correction if necessary. One of the surprises in digital quantum computing is that the same outcome is possible, namely the elimination of state errors, but because of the nature of quantum systems (basically, that observing the systems destroys the quantum state), the way it is done is quite different. Whereas for analog computing noise is continuously accumulated and the state is distorted. Because states are quantized in a quantum computer, the system ends up in the wrong state through a discrete transition, though it may be a nearby state. The fundamental challenge with analog computing and especially quantum analog computing, is there are never clear answers regarding performance until the machine is built, and, hence, the scalability of analog computing and its applicability for a wide range of computations is always uncertain.

The size of a digital computer is limited by resources, not by noise. Larger systems may have to have more extensive error correction (because of the aggregate number of elementary computations performed), but it is generally understood how to proceed when architecting a larger digital system. Hence, while analog computation can solve small problems, it is difficult to understand all the ways noise in analog computers leads to computation errors. This sensitivity limits the size and type of computation in ways that are difficult to characterize.

To reach its ultimate potential, digital quantum computing is expected to proceed through three stages: component quantum computation (CQC), noisy intermediate-scale quantum (NISQ) computing, and fault-tolerant quantum computing (FTQC). Currently, we are entering the NISQ stage for superconducting and trapped ions. Other qubit technologies, such as quantum dots, are in the component stage, and no approaches are close to being in the fault-tolerant stage of quantum computing.

a. Component Quantum Computing

The primary purpose of the CQC state is to demonstrate and mature the basic elements in a platform necessary for building a quantum computer. Platforms are defined by the

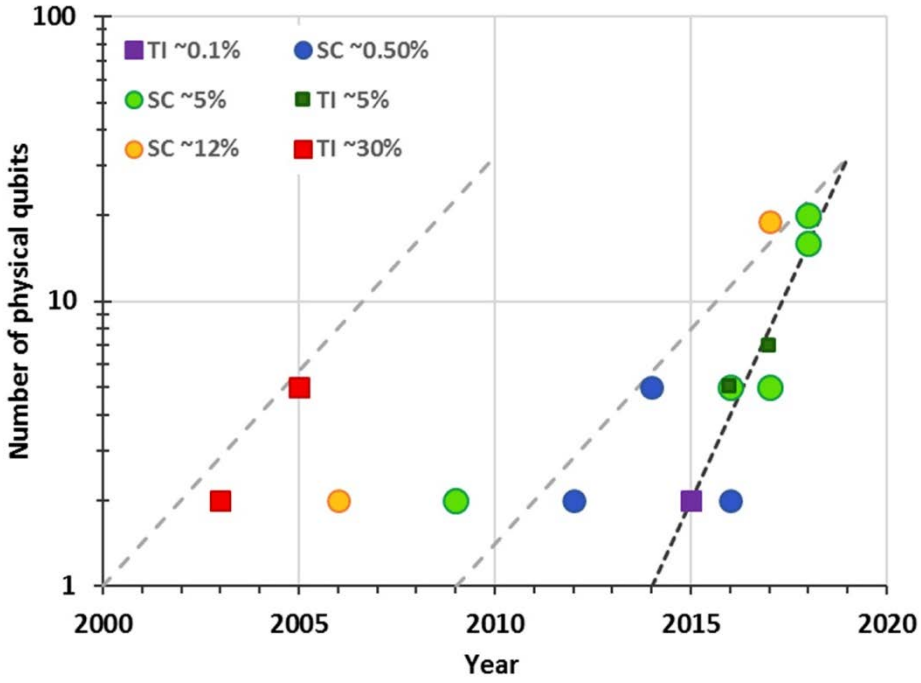
technology used for the qubits. At present, superconducting and trapped ions are sufficiently mature to have moved through the component stage onto the NISQ stage. The computational capability of the CQC is highly limited; most demonstrations have been proofs of principle. Five basic requirements—the DiVincenzo criteria (Ladd et al. 2010)—need to be met in the CQC stage:

1. Scalable physical system of well characterized qubits. At a minimum, scalable means the ability to work with a small number of qubits in a way that could be extended to a large number of qubits. Demonstrations are typically limited to about 10 qubits.
2. Ability to initialize the qubit to a known state with high accuracy. Typically, the qubit has to start the computation as either a 0 or a 1 with at least three nines (i.e., 0.999) of accuracy.
3. Universal gate set. A complete set of gates such that any quantum state can be approximately reached. Complete gates set often depend on the technology and contain from four to seven types of gates. The gate sets can be overly complete, with the additional gates included for computational efficiency.
4. Long decoherence time. Environmental noise must be sufficiently controlled such that the state of the qubit remains coherent until corrective means can be taken. At a minimum 100–1000 gate operations should be possible within the decoherence time.
5. A measurement capability to read addressable qubits in the computational basis with many nines of accuracy.

For trapped-ions quantum computing (Blatt and Wineland 2008), nature provides the qubit. Much of the challenge is in engineering the mechanisms for holding and manipulating the ions and providing the control for gate operations and measurement. Ions can be held in either bulk (3D) traps or surface traps. Surface traps, which are more scalable, are the preferred means. Gate interactions use optical pulses from highly stable lasers, and single-gate operations take on the order of a microsecond. Reported fidelities are three to four nines for single-qubit gate operations and two to three nines for two-qubit gate operations (Figure 3 and Figure 4). The venture-capital-backed company IonQ is a leading commercial company attempting to further develop trapped-ion technology into a computing platform.

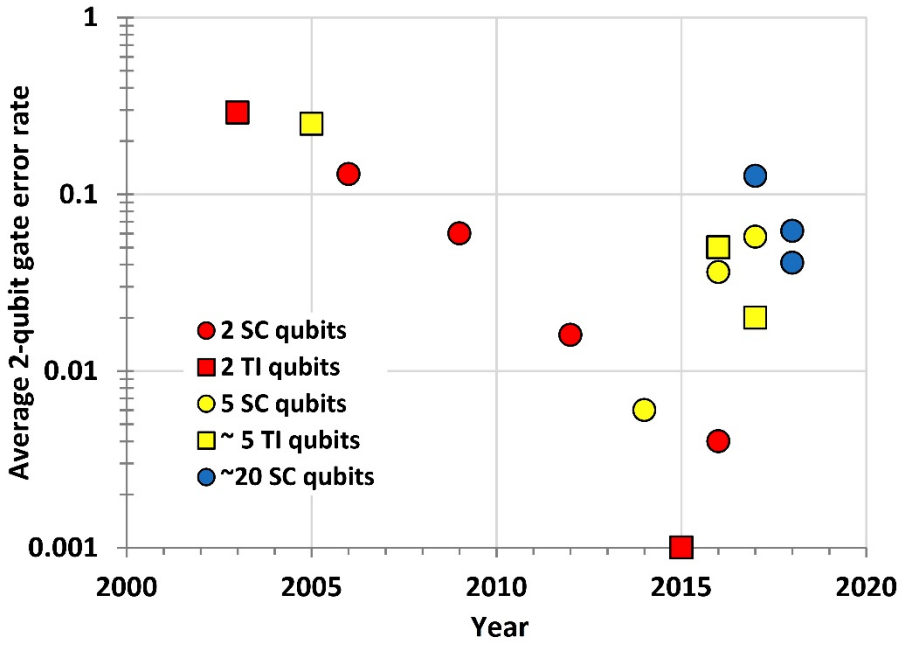
Superconducting qubits are solid-state devices fabricated using traditional very large scale integration fabrication process (Clarke and Wilhelm 2008). Much effort has been expended in designing qubits having extended lifetimes and high-fidelity operations. The results has been the transmon qubit first demonstrated at Yale and its variants. The chip has to be cooled to a milliKelvin. Gate interactions signals are in the gigahertz range. Gate

operations are on the order of 10 ns. IBM and Google have efforts in superconducting qubit platforms. Intel has invested in the component technology and will likely have a platform in the near future. The venture-capital-funded company Rigetti Computing has superconducting qubit platforms.



Source: Grumbling and Horowitz (2019).

Figure 3. Progress in the Number of Qubits in a System for trapped ion (TI) and superconducting (SC) platforms.



Source: Grumbling and Horowitz (2019).

Figure 4. Progress in Error Rate (approximately the inverse of the fidelity). Integration of larger numbers of qubits led to higher error rates, possibly cause by crosstalk or correlated noise.

We have focused on the most mature component platforms that have transitioned to the NISQ stage of quantum computing. Other technologies, including quantum dots (Kloeffel and Loss 2013), photonic (Rudolph 2017), dopants in silicon (Pla et al. 2012), neutral atoms (Weiss and Saffman 2017), color centers in diamond (Prawer and Greentree 2008), topological qubits (Aasen et al. 2016), while less mature, may still be of interest, particularly for issues of scalability and manufacturability. None of these other platforms are ready enter the NISQ phase.

Either the trapped-ion or the superconducting may survive the NISQ phase and possibly enter the FTQC phase. Each of these platforms has advantages and disadvantages, but at present neither is positioned to dominate quantum computing. Investment should continue into alternatives to the superconducting and trapped-ions platforms at the CQC phase.

b. Noisy Intermediate Scale Quantum Computing

NISQ computing is the first phase of quantum computing, where machines will have a sufficient number of (physical) qubits to potentially demonstrate the advantages of quantum computing. The continued maturation of the platform needs to increase both the quality and number of qubits to where logical qubits can be demonstrated. The demonstration of a logical qubit marks the point of transition to FTQC.

Being restricted to physical qubits places severe limitations on the types of computations that can be performed. Notably, the depth of computation (the number of sequential gate operations performed) has to be low, specifically on order of the coherence time of qubit. There is still the possibility for a high number of parallel gate operations, although this significantly increases the complexity of the control system.

One of the stated goals in the NISQ phase is to demonstrate "quantum supremacy," that is, to perform a computation on a NISQ computer that is clearly beyond the capabilities of current classical computing. A key challenge in achieving quantum supremacy is finding an algorithm that runs on a NISQ platform. While it is possible to factor small numbers on a NISQ computer using Shor's algorithm, for example, the largest number a NISQ machine will be able to factor could be factored with pencil and paper (1 sheet), which therefore fails to demonstrate quantum supremacy. The algorithm chosen for quantum supremacy will likely be an esoteric algorithm, specifically crafted for this purpose (Markov et al. 2018). As a result, the algorithm will not solve a problem of practical interest. A strong claim of quantum supremacy should be based on a problem for which there is a sufficient understanding based on classical computing approaches to that problem and not on an esoteric problem specifically designed for a quantum computer for which classical approaches have not been developed.

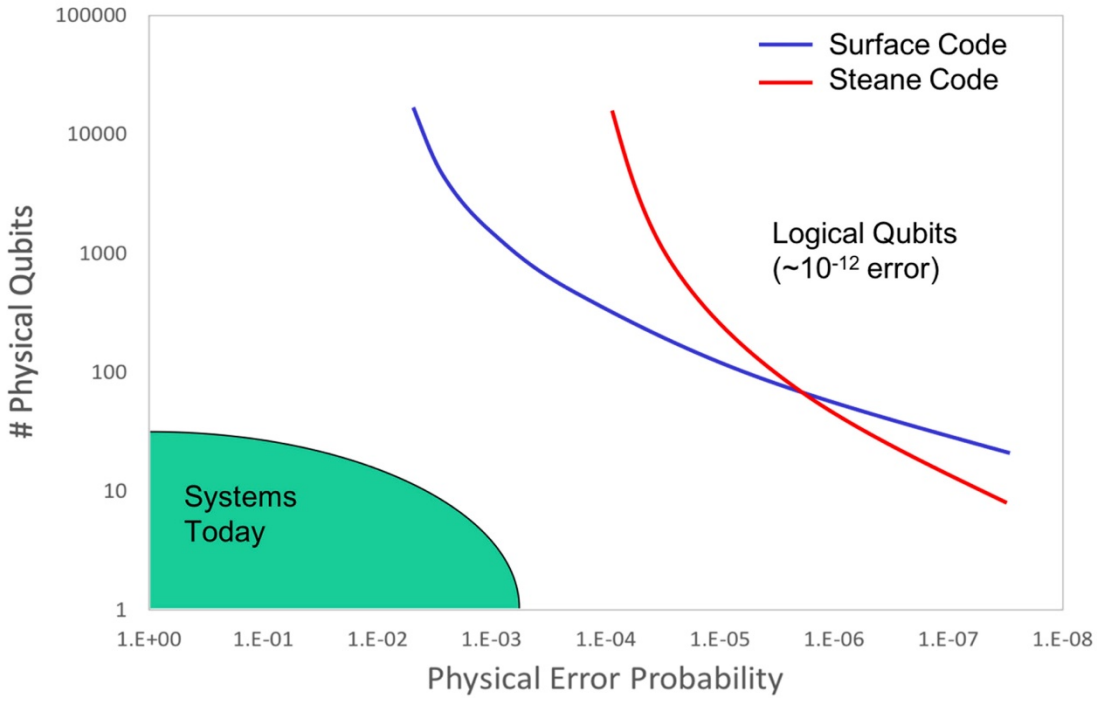
It will likely be at least a decade for the continued development of the platform to the point where it supports at least one logical qubit. The risk is that without the sales of NISQ machines, resources will not be available to support the commercial development over this extended time frame. Commercial success in the NISQ phase will largely be dependent on applications, which will be challenging (see next section). For the first 35 years of quantum computing it has been challenging to find indispensable algorithms (other than Shor's algorithms), and the likelihood of finding one on a much less capable platform (than the resource-unlimited, fault-tolerant quantum computer) is unlikely, but having an actual computer to experiment on could spur development. Because of the shallow depth of the computation that NISQ machines support, much effort has been focused on variational algorithms, where the quantum computer is used for rapid quantum state preparation and measurement, and the variation of experimental parameters is performed classically.

Focus will be on improving the fidelity and increasing the number of qubits. While there was significant progress on extending the lifetime of superconducting qubits in the first phase, further improvements will be challenging. Qubit fidelity affects the number of physical qubits needed for a logical qubit. There is much uncertainty in the number of physical qubits needed for a logical qubit, although estimates exist. At present, surface codes are the most promising, and about 10,000 physical qubits are needed for 1 logical qubit for physical qubits having a fidelity of 0.999 (or three nines), which is a higher fidelity than is being realized in either of the platforms. In rough terms, the inverse of the fidelity is the error rate. Three nines are record qubit fidelities for isolated qubits; typical ensemble

fidelities for collections of isolated qubits is about two nines. Systems of qubits have lower fidelities, (see Figure 5), typically 0.9–0.95, bringing the number of physical qubits to more than 100,000 per logical qubit (Markov et al. 2018). At least with trapped-ion we know that the lower fidelities stem from control and isolations issues and not qubit manufacturing issues.

Although demonstrating a logical qubit composed of physical qubits with fidelities of three nines requires a platform substantially more advanced than current NISQ platforms, realistically, fidelities from four to six nines will be required for practical quantum computing. This results in needing only about 100 physical qubits per logical qubit, but the concern is that these models assume uncorrelated noise.

Correlated noise will increase the number of physical qubits in a logical qubit. Quantum error correction is significantly more difficult when gate fidelities are low and correlated noise is present, because error detection and correction must account for the likelihood of errors. Correlated errors raise the probability of additional local errors given one error. The IARPA LogiQ is exploring the effects of correlated noise, but it is still too early in the program for insight on the nature of correlated noise.



Source: Grumbling and Horowitz (2019).

Figure 5. Theoretical Predictions of the Number of Physical Qubits Needed for a Logical Qubit as Function of Error Probability. At currently achievable error rates, logical qubits will need between 10,000 and 100,000 physical qubits per logical qubit.

Failure to establish revenue streams to sustain commercial development would likely cause private industry to lose interest. Realistically, quantum computing has about 5 years to either establish a revenue stream or, at minimum, make significant technological progress showing that viable applications are reasonably within reach. Should private industry abandon quantum computing, the government will have to substantially support development and maturation of quantum computing platforms. At present, the hope is that one of the variational algorithms will be of commercial value.

c. Fault-Tolerant Quantum Computing

The threshold for entering FTQC is the logical qubit. At present neither the trapped-ion nor the superconducting platform are anywhere close to having a logical qubit. The challenge in FTQC is increasing the depth of the computation, the number of qubits, and providing quantum memory. Quantum error correction increases the lifetime of the quantum state, but there are still limits. Quantum error correction is done in stages; the likelihood of there not being an error compounds exponentially with the number of stages, until a threshold is reached, at which point the likelihood of an error is minimal. The threshold is set in part by the required gate depth of the computation.

For example, as shown in Figure 5, the error rate was set to 1 error in 10^{12} operations. This is a little misleading, because even a qubit that just has to hold state (and not perform any gate operations) will still have to go through error correction many times per natural lifetime of the qubit. At a gate rate of 1 ns, 10^{12} operations would take 1,000 seconds. Correcting a static qubit, say, every 100 ns to stabilize the state would extend the lifetime to about 1 day. This may be sufficient for some computations, though many quantum computations are expected to take significantly longer. Longer times will require more complex logical qubits and physical qubits with improved fidelities.

Holding data in computational-type qubits is resource intensive. Quantum memory, the ability to store a quantum state in a highly isolated (extremely long lifetime) quantum system, will be needed for data-intensive quantum computing. Such long-term memory qubits or even conventional qubits can be used for QRAM (the quantum equivalent of dynamic random access memory, DRAM). QRAM is much more powerful than DRAM and is architected similarly to DRAM in the sense that bits are stored in an addressable array (Giovannetti, Lloyd, and Maccone 2008). In QRAM the memory-address register is the quantum register, and the output register contains the stored quantum states in a superposition. A QRAM to access N pieces of data consists of a branching array of $2N$ quantum switches, which must operate coherently during a memory call. In principle, such a QRAM takes time O (log2 N) to perform a memory call.

While simple demonstrations of QRAM exist, developing the component and architecture for QRAM has not been a focused effort of the research community. Without QRAM or an alternative, algorithm choice will be limited because the overhead of working

with large datasets will likely overwhelm any computational advantage of the core algorithm. This point is further discussed in the next section.

The utility of a quantum computer is expanded by having more qubits. Something that reflects the need for increasing complexity with time like a Moore's law for quantum computing, in which the number of qubits doubles every so many months, may be needed. Qubits are likely not to get smaller with successive generations, which means computers will be getting larger as the number of qubits increases.

Having more qubits also means that wiring the qubits will become more complicated. Present schemes use limited nearest neighbor coupling and, in some cases, longer range couplings. The connectivity will likely be dominated by quantum error correction considerations because these comprise most of the computation. Nevertheless, algorithms will have significantly different communications patterns, and achieving the right "general purpose" quantum computer architecture will be challenging. A quantum computer having a single algorithm of interest, such as a focus on Shor's algorithm for the Intelligence Community, results in a significantly simplified design compared with a quantum computer for general-purpose computations.

Fundamentally, FTQC is about scalability—making larger and more capable quantum computers. While nothing here is demonstrably physically impossible, the technical challenges are immense. Realistically, such development is only likely when sustained with resources from commercial sales of quantum computers. And this depends on having algorithms for key applications.

2. Applications

This section focus on application in the areas of Cryptographic, Big Data, Quantum Machine Learning, Optimization, Finance, and Simulation. The estimation of computation resources depend on the nature of the algorithm and many of the conclusion in this sections are justified in the algorithm section, which follows this section.

A number of commercial companies and venture-funded startup companies are developing NISQ computers with expectation that revenue from applications will drive continued development, as it has for other technologies, such as integrated CMOS chips. This need is further heightened by the realization that FTQC is more than a decade away, possibly as far as two to three decades before it can realize a practical quantum advantage. The time scale for the realization of a practical quantum advantage, be it with a NISQ computer or an FTQC, will have a strong effect on the level of continued participation from commercial companies in the development of quantum computers.

For sales-funded development to happen in a sustainable way, a quantum computer must offer a clear and compelling advantage over a classical computer. There's no reason to use a quantum computer to solve a problem that can be more effectively solved with a

classical computer. Furthermore, the application should be for a potentially big market, which is why much of the interest is focused on quantum machine learning and other trendy topics. Failure of a NISQ computer to gain commercial acceptance will result in reduced levels of support from commercial companies. Should quantum computers be of interest for government applications, and DoD applications in particular, then the DoD must be prepared to fund the research necessary to mature the technology, particularly if quantum computing experiences a "quantum winter," similar to the AI winter.

a. Cryptographic

The cryptographic application of quantum computing is well established. Shor's algorithm factors integers, which breaks current asymmetric crypto systems such as RSA. The oldest quantum threat to symmetric crypto systems was from Grover's algorithm, which effectively reduces the security (as measured by the number of bits in the key) in half against a brute-force search of the key space. Realistically, this is not a threat to symmetric key systems.

Of more potential concern are recent cryptanalytic attacks to symmetric key systems based on structure present in symmetric crypto systems (Kaplan et al. 2016; Santoli and Schaffner 2017; Kaplan et al. 2015; Chailloux, Naya-Plasencia, and Schrottenloher 2017; Kaplan 2014), some even demonstrating super-polynomial speedup (Kaplan et al. 2016). Many of these appear to have excessive resource requirements, such as access to cryptographic oracles that provides quantum superpositions of encrypted messages or require the collection of $2^{(n/2)}$ copies of encrypted messages, where n is the length of the key. Nevertheless, other algebraic quantum algorithms, possibly unknown at present, may be of use for cryptanalysis on symmetric ciphers.

Shor's algorithm requires an FTQC to factor a number beyond current classical capabilities. Compared with other applications requiring an FTQC, Shor's algorithm may be easier. The input requirements are minimal, and the number of qubits and gate operations are reasonable. Roughly, $3n$ logical qubits and n^3 logical gate operations are required (Shor 1994).

Although these algorithms are of possible interest to NSA, they are of little interest to the rest of the DoD. Furthermore, there is little interest outside the government in such capabilities, not so much because they would not be useful for nefarious activities, but because crypto systems are entering a post-quantum phase in which encryption will be resistant to known quantum attacks.

b. Big Data

Much of classical computing works with large datasets. This include machine learning, engineering computations, and modeling physical and other systems. The ability

to work with large datasets is extremely challenging for quantum computers. Quantum computer have been focused on computational qubits, not memory qubits or large memory access systems, such as QRAM (Giovannetti, Lloyd, and Maccone 2008). As discussed for the quantum computation of a radar cross section using quantum linear algorithm (Scherer et al. 2017), the size of the problem must become excessively large when practical consideration of working with data are included for there to be a quantum advantage. This computation required 10^{29} gate operations to reach the break-even point with the best known classical algorithms.

Although quantum computation for big data is far beyond first-generation FTQCs, it may benefit the government to get better bounds on the problem and possibly suggest some research initiatives. A good starting point may be to consider revisiting the IARPA Quantum Computer Science program intent to better understand the architectural implications of such problems (see Recommendation 3).

c. Quantum Machine Learning

With all the interest in machine learning, consideration of applying quantum computing to machine learning was inevitable, and has been a topic of interest for well over a decade (Biamonte et al. 2017; Schuld, Sinayskiy, and Petruccione 2015; Loyd, Mohseni, and Rebentrost 2013). Much of machine learning, such as principal component analysis and SVMs, relies on linear algebra. At its core, quantum mechanics is about the evolution (i.e., processing) of complex vectors in a high-dimensional linear space. Working with large training sets in their entirety on quantum computer is simply not practical for reasons previously mentioned.

The challenge is working with large training datasets, where the time to load the dataset into QRAM would likely overwhelm any advantage gained by the super-polynomial speedup. Internally generating the data in the quantum computer would eliminate the need to load the data from an external source. In such cases, improved performance on a quantum computer is more likely, but not guaranteed. Such an approach would almost certainly preclude working with real-world datasets (which are almost all of machine learning), and constructive datasets would likely be based on simple rules (such as games, like GO) or simple models. Regardless, there would likely have to be a significant investment in QRAM or an alternative before such applications could show capability exceeding classical approaches.

More recently, hybrid variational approaches have been explored and demonstrated for quantum SVMs (Havlíček et al. 2019). One of the advantage of these approaches is that they used samples from the training set one at time, which makes them potentially suitable for NISQ computers. To gain a quantum advantage, the quantum SVM machines not only have to be trained in a quantum computer, they also have to be run in a quantum computer after training is complete. By virtue of being variational algorithms, these approaches face

the challenges of having noisy, non-convex cost functions; stochastic optimization approaches will be needed because of quantum measurement noise. Significantly more research is needed to establish any quantum advantage of variational approaches to machine learning.

Quantum machine learning has also been proposed for training Hopfield networks and restricted Boltzmann machines. Rather than using gate-based quantum computers, these networks rely on analog simulation approaches, such as D-Wave's quantum annealer. The training of these networks adjusts the interconnections until a Boltzman-Gibbs distribution is achieved. This is exceeding difficult to do classically, but the thermalization of a quantum system, such as takes place in a quantum annealer, may speed up the process. While simple demonstrations have been performed, there are significant challenges, including that the thermalization appears to be training-sample dependent, and claims of speedup are based on an extremely few number of points close to the origin. The general discussion of these approaches is beyond the scope of this report. There are also a number of challenges associated with analog quantum computation, as discussed as in the next section.

d. Optimization

Optimization is a broad topic, and attention here is restricted to NP-hard problems that are also NP-complete. These include the traveling salesman problem and many graph algorithms, such as the max-cut problem. Although these problems are NP-hard, most of them have good heuristic approaches, particularly for applications of interest, which makes establishing a quantum advantage more difficult.

Because these are NP-complete problems, even a quantum computer is unlikely to have a super-polynomial speedup. Hence, establishing the quantum advantage will be highly application specific (likely those for which we do not have good heuristics), focused on heuristics (to establish the speedup), and the advantage will probably not be large (because exponential speedups are unlikely). For example, max-cut has heuristics that guarantee the answer is greater than 88% of the optimal (and simulated annealing can do better). That leaves less than a 12% margin for a significant reduction in algorithmic complexity as the potential quantum advantage for improved accuracy, though there is also the possibility that the quantum computer could provide a runtime improvement or electrical energy improvement.

The traditional approach has focused on Grover's algorithm. Many classical algorithms have quantum equivalents; for those that have exponential complexity, making use of Grover's algorithm cuts the exponential factor in half in many cases Such approaches require an FTQC, and for specific applications where good heuristics exist, the gain in performance is not likely to be worth the effort except for the largest of problems.

Variational approaches to optimization, such as QAOA (Farhi, Goldstone, and Gutmann 2014; Farhi, Kimmel, and Temme 2016), may offer more advantages, but they are not without significant challenges. QAOA requires the simultaneous (classical) optimization of a large number of variational parameters over an almost certainly non-convex, noisy surface. The quality of the results strongly depends on the quality of this optimization. The surface is noisy because the landscape exists in a quantum space, and the function has to be evaluated on a quantum computer. Doing so introduces quantum measurement statistics, and a point of the cost function is actually a probability distribution. QAOA approaches are also general approaches to a problem that are difficult to restrict in scope to specific application because of the inherent nature of the algorithm. This will make quantifying any quantum advantage (which necessarily must happen against the heuristics for a specific problem) challenging. Alternatively, it could be that the QAOA approach has an advantage over all optimization applications, although this seems unlikely given that they are NP-complete problems. Nevertheless, because this is one of the few algorithms that can run on a NISQ computer, it merits a deeper understanding of practical applications. However, this is not likely given the recent analysis of the QAOA algorithm by Hastings (2019) as discussed in the previous section.

e. Finance

Even finance has shown interest in quantum computing. Organizations including Goldman Sachs, Royal Bank of Scotland, and Guggenheim partners are exploring the possibilities (Clark and Saijel 2015). Quantum annealers (not the primary topic of this section) have been proposed to optimize portfolios, find arbitrage opportunities, and perform credit scoring (Orús, Mugel, and Lizaso 2019). Gate-based quantum computers have been suggested for quantum risk analysis where convergence can be increased from $O(M^{(-1/2)})$ to $O(M^{(-2/3)})$, where M is the number of samples (Woerner and Egger 2019). This is a meager speedup. Maybe Wall Street will fund the first quantum computer.

f. Simulation

Quantum simulation uses a quantum computer to understand the properties of quantum systems (Feynman 1982; Georgescu, Ashhab, and Nori 2014; Cirac and Zoller 2012; Laflorencie 2016). It was the first, and still perhaps the most promising, application for quantum computers because of the inherent intractability of using quantum theory and classical computation to understand quantum systems. The two primary applications for quantum simulation are understanding the dynamics of Hamiltonian evolution, where the Hamiltonian describes a quantum systems of interest. Gate-based quantum computers can approximate the evolution as a finite sequence of gate operations.

The other application of quantum simulation is to directly predict properties of quantum molecules and other systems, such as the ground-state energy. Two approaches

have been developed, one using quantum-phase estimation (Reiher et al. 2017), the other using variational techniques (Peruzzo et al. 2014). The QPE approach simulates the dynamics of the Hamiltonian and forces it to a low-energy state. Measurement of phase collapses the system into an energy eigenstate (not necessarily the ground state). Repeated computations will map out the low-energy states of the system under study. Achieving the required precision requires an FTQC, and for molecules such as FeMo-co (the iron molybdenum cofactor in the enzyme nitrogenase that is responsible for nitrogen fixation), the computation time has been estimated to be a few days (including error correction) on a quantum computer of 100–1,000 logical qubits (Peruzzo et al. 2014).

Variational approaches suitable for NISQ computers have been developed (McClean et al. 2016), though it will be challenging to show that there is a quantum advantage given the limited resources of NISQ machines. Nevertheless, this may be the approach with the highest likelihood of success on NISQ machines because it is the most natural match between a problem and a quantum computation. The fundamental question is how well does a variational approach work on more complex molecules.

3. Algorithms

a. Algebraic Algorithms

Much of the perceived benefit from a quantum computer is the ability to achieve super-polynomial speedup over the best known classical algorithms. In simple terms, this means that a computation that scales exponentially on a classical computer will scale polynomially (ideally, a low-order polynomial) on a quantum computer. There are many examples of super-polynomial speedups in quantum computing (Childs and Van Dam 2010), and many of these are in the algebraic area.

The best known example is Shor's algorithm for factoring integers. Shor's algorithm is a special case of the Abelian hidden subgroup problem. Other examples include finding solutions to Pell's equation, $x^2 - dy^2 = 1$, where d is an integer not divisible by any perfect square, an example of a number field problem, and the hidden shift problem (see Childs and Van Dam 2010 for details). Most of these examples are esoteric math problems that do not drive computing. The interest in Shor's algorithms is driven by the fact that factoring is computationally hard and is the basis for cyber security.

Shor's algorithm was the first quantum algorithm that had raised interest in quantum computing because it had a practical application. Shor's algorithm factors composite integers more efficiently. It is also a good example that dispels the common notion that quantum computers solve hard search problems instantaneously by simply trying all the possible solutions at once. Shor's algorithm finds the R such that $a^m \bmod N = a^{(m+R)} \bmod N$, where N is the number being factored, and a is a randomly chosen integer (that can't be coprime with N). The first stage creates a highly entangled state that contains the result in

a quantum superposition of a^m mod N for all m over a range that includes $m + R$. This induces a periodicity on the quantum register containing the state. That periodicity can be found via a quantum Fourier transform. This procedure works classically, except the difference is that the R's have to be tried one at a time; on a quantum computer all the R's can be tried simultaneously using a quantum circuit polynomial in log (N) gates. Shor's algorithm achieves exponential polynomial speedup over the best known classical factoring algorithm, the general number field sieve (Pomerance 2008).

The primary reason for going into this level of detail is to explicitly point out why Shor's algorithm is so well matched to a quantum computer. First, it does not require a large dataset. Quantum states have to be prepared for a and N. This is relatively simple compared to problems that work with large datasets. Many quantum algorithms have a much larger data requirement that is often dismissed in the analysis by using an oracle. As we will see, this dismissal results in an underestimate of the actual effort required and that in turn often removes the run-time advantage of the algorithm (Aaronson 2015).

The application of the quantum gates in the first stage of the computation creates a highly entangled state. Having a highly entangled state is a necessary condition for there to be exponential speedup, though it is not sufficient (Jozsa and Linden 2003). Finally, the quantum Fourier transform creates a condition in which there are multiple paths for the entangled states in the superposition such that the paths for the sought after answer constructively interfere while all the other states destructively interfere. This is a coherent process whereby the wave-like nature of the state is exploited.

While Shor's algorithm is simple, it's still far beyond reach of NISQ computers and requires FTQC of order 10^6 physical qubits to factor a number that is beyond reach of classical approaches. There is no consensus on when such a quantum computer will be available (Grumbling and Horowitz 2019), but there is strong agreement that one is not possible in the next decade and is likely more than two decades away.

All the algebraic algorithms are (believed to be) nondeterministic polynomial-time (NP) hard, but they are not NP-complete. This means that they all have internal structure that can be exploited, unlike a general NP-complete problem such as the traveling salesman problem. There have been some results indicating that some symmetric ciphers may be more vulnerable than previously thought (Kaplan et al. 2016) because of exploitable structure. Many algorithms (perhaps all) use the quantum Fourier transform to exploit this structure. The quantum Fourier transform is an important algorithm not only for algebraic algorithms but also for linear algebra and, perhaps most important, quantum simulation. The essential point is that it is difficult to understand a path forward for commercially supported quantum computing based solely on algebraic algorithms as these are not the drivers of computing and there is little interest except from the U.S. Government for select applications.

b. Quantum Fourier Transform and Quantum Phase Estimation

Quantum Fourier transform (QFT) and quantum phase estimation (QPE) are two critically important algorithms for the roles they play in other algorithms (Nielsen and Chuang 2010). The first version of the QFT algorithm was developed by Peter Shor as an essential element of Shor's algorithm for factoring integers (Shor 1994). The QFT is not a faster version of the classical Fourier transform. Rather, it is an algorithm that produces the Fourier transform quantum mechanical amplitudes. The QPE algorithm estimates the phase of an eigenvector, which in quantum simulation is used to predict the ground-state energy of molecules and other quantum systems. The complexity of quantum circuit depends on the required precision, which varies depending on application. Quantum simulation for predicting the ground-state energy of molecules needs high precision to be of practical value. In particular, see the supplementary information of Reiher et al. (2017) for a discussion of the resources required to realize QPE for predicting ground-state energies of molecules.

Much of the value of a quantum computer depends on having capable QPE and QFT algorithms. This is critically important for Shor's algorithm and quantum simulation of complex molecules. Achieving the required precision for practical applications will only be possible with FTQC. Hence, any quantum algorithms dependent on QFT or QPE will only be possible with the FTQC.

c. Searching (Quantum Walks)

Grover's algorithm (Grover 1996) finds the input to a function that results in a specified value. For a function having N possible input values, Grover's algorithm finds the input in $O(\sqrt{N})$ queries, whereas the classical algorithm requires $O(N)$ queries. Grover's algorithm is typically referred to as a database (or table) lookup algorithm because the values of the function are in the form of an unsorted list.

What's interesting about Grover's algorithm is the $O(\sqrt{N})$ complexity is provably optimal for an unsorted list. There is no quantum algorithm that on an unsorted list can locate a value with fewer operations. This is often used to support the conjecture that quantum computers cannot solve NP-complete problems with superpolynomial speedup. This has certainly been empirically true in that all the algorithms that have super-polynomial speed up are all NP-hard problems that are not NP-complete.

For Grover's algorithm to work on large amount of data would require an FTQC and large quantum memory to store the data. Such applications have the largest resource requirements of all quantum comping applications and are likely not practical in the foreseeable future. The application of Grover's algorithm to data generated algorithmically (as opposed to having to be loaded from external tables) may more practical, although we are unaware of any application needing such capabilities.

d. Linear Algebra (HHL algorithm and its variants)

Quantum algorithms have been developed and subsequently improved for working with large systems of linear equations. The HHL (Harrow, Hassidim, and Lloyd 2009) algorithm solves the equation $Ax = b$ for x where A is a sparse $N \times N$ matrix. The HHL algorithm has an algorithmic complexity of $O(\kappa^2 d^2 \log(N)/\varepsilon)$, where κ describe the conditioning of the matrix (ratio of the largest to the smallest eigenvalue of A), ε is the precision of the computation (typically 0.01), and d is a measure of the sparseness of the matrix A (the maximum nonzero entries are the densest row of A). The best known classical linear-system-solving algorithm based on the conjugate gradient method (Shewchuk 1994) has the run-time complexity of $O(N\kappa d \log(1/\varepsilon))$. The reduction in run-time complexity from N for the classical approach to $\log(N)$ for the quantum approach leads a super-polynomial speedup. This speedup generated much interest because of its potential application to machine learning and engineering.

Evaluating the practical utility of exponential speedup is highly application dependent. Reduced complexity will always be a significant advantage when the problem is sufficiently large. The difficult part is predicting how large is large. Algorithmic complexity is simply the limiting functional form (for large N) of the count of operations that have to be performed. Furthermore, quantum operations are not the same as the classical operations in the comparison—the classical operations are arithmetic multiplies, whereas the quantum operations are gate operations. As a result, no matter what the constants, such as the energy cost of an operation or even the time it take to perform an operation, there is some size of the problem for which the quantum computer will outperform the classical computer (in that it requires fewer operation to complete the computation). It's instructive to have a sense of for what values of N is the quantum approach is better than the classical approach.

The other complication is that as described in Harrow, Hassidim, and Lloyd (2009), the quantum algorithm is an oracle algorithm with an oracle taking the place of the matrix A and the vector b. What that means is that unit algorithmic cost is assigned to the operation of the oracle. The oracle has significant resource requirements and operational impact. If quantum random access memory existed, then A could be stored in quantum memory much as the A is stored in working memory (DRAM) in a classical computer. Having to load QRAM would be a significant impact, but the alternative of generating A as part of the computation is likely unrealistic for practical applications such as machine learning or engineering computations, both of which depend on large datasets.

As part of the IARPA Quantum Computer Science program, a more detailed estimate of the resource requirements was determined for computing the electromagnetic scattering cross section of a 2D target (Scherer et al. 2017). In that analysis, it was estimated that the crossover point where the number of quantum (gate) operations would equal the number of classical (multiply operations) was $N = 332{,}020{,}680$. Assuming an algorithmic precision

of $\varepsilon = 0.01$, the computation required a circuit width of order 10^8 and a circuit depth of 10^{29} when resource requirements for oracle were taken into consideration, whereas the circuit width and depth were 340 and 10^{25}, respectively, when A was represented as an oracle. At an execution rate of 1 ns per gate, the sequential computation would require 10^{20} seconds, which is about the age of the universe (4×10^{20} seconds). Using parallel computing resources could reduce the duration of the computation by no more than the width of the computation, likely less. This gives a lower bound on the computation of 30,000 years. These estimates are for logical operations. One should expect a several order-of-magnitude increase to the duration of the computation and the number of qubits and their duration. Such computations are clearly not practical, barring significant improvements in algorithm or quantum technology.

e. Variational Quantum Eigensolver for Optimization

Variational methods make use of a quantum computer to evaluate the objective function via the measurement on a variationally generated quantum state. These methods have garnered increasing interest, particularly for use on NISQ-generation quantum computers. The idea is simple: The quantum computer is used to prepare a state that is determined by a set of continuously variable experimental parameters that can be controlled through a sequence of quantum gates. An objective function dependent on a measured value of the quantum state is minimized. Often evaluation of the objective function has to be repeated multiple times to build up sufficient precision and confidence in the value. A classical optimization routine updates the experimental parameters that determine a new quantum state and, ideally, will decrease the value of the objective function. The process is continued until a minimum (possibly a local minimum) is reached.

The method was originally developed as an alternative to QPE to find the ground-state energy of molecules, where the quantum state describes the electron configuration (Peruzzo et al. 2014). Practical QPE requires long-depth circuits (suitable for an FTQC but not a NISQ computer). The primary advantage of the variational approach along with its interest for use on NISQ computers is that the generation of the quantum state from a simple reference state (i.e., the application of a short network of parametrized quantum gates) and the measurement of the objective function can be performed within the coherence time of the NISQ physical qubits. The disadvantage of this approach is that to achieve precision p, $O(p^{-2})$ iterations of the state preparation/measurement cycle will have to be performed whereas $O(p^{-1})$ are required for QPE (McClean et al. 2016). Additional iterations of this process (with an updated set of parameters) are needed to find the minimum. The trade-off is the long coherent evolution required for QPE is replaced with quadratically more operations (but within the coherence time of the qubits) for the variational approach.

The quantum computer is used solely to compute the objective function. This has an advantage if the objective function is hard to compute classically. Classical approaches to

quantum chemistry rely on methods such as (electron) density functional theory and unitary coupled cluster theory. Classical approaches give reasonably approximate answers (though not sufficient to predict experimental measurements) in many cases, though ultimately they are limited by computational resources. Classical approaches do not fully account for the energy of exchange interaction in fermionic systems, which is a unique quantum effect and one that is computationally intractable classically because of the combinatorics. Classical computations of electronic structure are still used in these quantum variational estimation approaches because they serve as the basis for the second quantization formulation of the Hamiltonian describing the molecule. The quantum variational estimation approach applied to quantum chemistry problems starts from a close state (the closer, the better), and the closer the state is the faster the rate of convergence to a global minimum (McClean et al. 2016).

With the expectation that variational approaches are well matched for NISQ computers, variational approaches have been extended to more conventional computation problems, including approximate optimization and machine learning. In generalizing variational approaches from quantum chemistry to other applications, two observations are warranted. First, the quantum state needs to capture an aspect of the problem that is intrinsically computationally hard. Without doing this, there is no speedup from the quantum computer. In quantum chemistry this is the exchange interaction. Second, there should be a starting point that is "close" to the correct answer so that the variation is really a perturbation about an approximate solution. As we will see, the closeness of the starting point can be somewhat relaxed, but as it is, it becomes less clear what the quantum advantage is.

The quantum adiabatic optimization algorithm (QAOA), although not a variational quantum eigensolver, uses the variational approach to find approximate solutions to NP-hard problems (Farhi, Goldstone, and Gutmann 2014). It is an approximate algorithm that, as originally formulated, proceeds through a series of stages of alternating applications of a mixing Hamiltonian and the problem Hamiltonian. The applications of these gates are stages using parameters β_i and γ_i angles, which are constants over all the qubits in the system for stage i. The two vector experimental parameters, $\boldsymbol{\gamma}$ and $\boldsymbol{\beta}$, are determined and optimized classically using a measured cost function on the quantum state.

Analysis contained in the original paper (Farhi, Goldstone, and Gutmann 2014) and other sources (Hadfield 2018) established that this approach (of terminating the approximation at a single stage) only accounts for contributions from nearest neighbors in a graph algorithm, for example. Contributions from non-nearest neighbors can be included by incorporating additional stages of rotations. Incorporating a second stage introduces β_2 and γ_2, and all four parameter would be subject to optimization. It has been proved that as the number of stages increases, the approximation improves and in the limit of an infinite

number of stages, the solution becomes exact. This is assuming that optimal values for $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ can be determined by the variational approach.

To be more specific, the original formulation of QAOA was applied to the constraint-satisfaction problem (Farhi, Goldstone, and Gutmann 2014; Farhi, Kimmel, and Temme 2016), where the goal was to satisfy all the constraints. Because the NP-hard problems considered are also NP-complete, in some sense all these problems are equivalent (though maybe not practically so). The objective function counts the number of constraints satisfied, where an exact solution would have all the constraints satisfied. QAOA does produce an entangled state and is therefore computationally hard to classically compute. QAOA works by finding a sequence of γ's and β's that cause the (more) optimal solution to constructively interfere and the less optimal solutions to destructively interfere.

QAOA is a Trotterized version of quantum annealing (e.g., a D-Wave machine). But unlike a D-Wave machine, QAOA does have the ability to find a global minimum, though the hardness of finding that global minimum is in classical optimization of the quantum parameters, for which a general procedure likely doesn't exist because of the complexities of the landscape of the objective function. The challenging hard work is in the classical computation of the $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$. QAOA will likely not work with any performance advantages when the classical optimization routines have to cope with highly non-convex surfaces, which are the same problem instances for which many classical heuristics also fail to find good approximate solutions.

It has recently been shown that QAOA is likely to be limited in its performance (Hastings 2019) and that classical algorithms can often outperform the QAOA. Hastings (2019) showed that QAOA appears to be a quantum circuit that in actuality is quite similar to simple classical algorithms that are based on local choices. Furthermore, for cases in which these simple classical algorithms break down, the quantum approach is likely also to break down and slowly converge. There is no general explanation as to why the quantum circuit should outperform classical algorithms.

Variational approaches have also been applied to machine learning (Havlíček et al. 2019). For example, the Hilbert space describing a quantum n-qubit register is an exponentially large linear space in which data can be embedded and classified by using a hyperplane-like construct to partition the space. The quantum equivalent of a support vector machine (SVM), this construct was recently demonstrated on a 5-bit quantum computer (Havlíček et al. 2019) (although only 2 of the 5 bits were used in the demonstration). In this demonstration real-valued vectors of two dimensions were nonlinearly transformed into a 2-qubit quantum registers one at a time. For each sample from the training set an objective function that measured the classification error was computed, and the quantum classification operator was variationally adjusted to minimize the classification error.

Using constructed data having perfect classification for a predetermined nonlinear embedding, the procedure was able to achieve error-free classification in two out of three attempts. The generalization of these results with regard to the utility of using a quantum computer for machine learning raises a few issues. First, while demonstrating the algorithm on an actual quantum computer is impressive, the approach had a significant advantage in that even before training, both the form of the nonlinear embedding and the partition that the variational procedure found were known to exist in the dataset by its construction. This would not be known for a real-world dataset, and the number of nonlinear embedding options that could be chosen when working with a real dataset is practically unlimited. No sensitivity analysis was performed. If a controlled amount of noise were added to the training set, would the variational procedure still find a useful classification discriminator?

Second, the nonlinear embedding chosen was claimed to be computationally intractable on a classical computer. There is no reason why such an embedding is better than one that could be computed on a conventional computer; nonlinear embeddings are common for classical SVMs.

Finally, the classification function must be run on a quantum computer; the partition cannot be measured after the training is completed and be run on a conventional computer. In the example given, each classification from the test set required 10,000 runs of the quantum computer to build up sufficient statistics for confidence in the classification. The essential point is not that quantum systems do provide an exponentially large linear state spaces, but it is not obvious how they can be used for computational advantage on practical problems without a significant amount of further research.

4. Other Approaches to Quantum Computing

Digital quantum computing uses a sequence of discrete quantum gates to evolve the state of the computation. This section presents other approaches to quantum computing, all of which are based on analog (or continuous) evolution of the quantum computational state.

Analog quantum computing evolves the state in a continuous manner starting from a defined ground state to the final state. Measurement of the final state provides the result of the computation. Analog and digital computation refers to the evolution of the state. Both analog and digital quantum computation are still digital in the sense that the input state and the measurement of the output state are strings of 0’s and 1’s. There are no solely analog quantities, such as a voltage, in the computation that are measured classically. The two dominant forms of analog quantum computing are the adiabatic quantum computer and its descendant, the quantum annealing machine, and the coherent Ising machine.

Adiabatic quantum computing is based on the adiabatic theorem of quantum mechanics (Born and Fock 1928), which states that a system starting in a ground state of one Hamiltonian will remain in that ground state as the Hamiltonian is slowly changed.

The initial Hamiltonian is a simple Hamiltonian with an easily prepared ground state, and the final Hamiltonian represents the computation. The solution to NP-complete problems, such as the traveling salesman problem, is the ground state of Hamiltonian (Farhi et al. 2000). The perceived advantage of adiabatic quantum computing is that it only uses physical qubits and, in principle, should be able to efficiently solve large instances of problems as long as the evolution between the initial and final state is sufficiently slow. And that's the catch. Sufficiently slow is challenging to define in a problem-independent way. In most cases the speed has to slow exponentially with problem size. Failure to do so will cause the system to end up in an excited state, which may be an approximate solution to the problem, but this is not guaranteed.

The best example of an analog quantum computer is the original D-Wave machine. Failure to keep the computation reliable in the ground state and the lack of any demonstrable speedup with problem size caused D-Wave to abandon this approach and use the machine as a quantum annealer. A quantum annealer, which is the quantum version of simulated annealing (Amin 2015), relies on quantum mechanical tunneling through potential barriers to explore a complex landscape and ideally find a global minimum. The advantage of a quantum annealer over classical approaches has not been verified for a variety of reasons that are well-explained in the literature.

A final example of analog quantum computing is the coherent Ising machine (Wang et al. 2013). Ising machine comprise a collection of coupled bistable systems that are driven through a phase transition. The phase transition drives the system from an entangled quantum state to a classical state, and the state of each of the bistable systems is read out. This is the result of the computation. Coherent Ising machines have been demonstrated to solve large coupled systems of more than 2,000 variables (Inagaki et al. 2016). While these results are impressive, noise issues make the final state not the ground state; the answer is only an approximation.

The fundamental challenge with all these analog approaches is quantifying the role of noise. Noise causes errors, and it has proved to be exceedingly difficult to have a general theory of noise to guide the scalability of analog quantum computing. The basic approach is to build a sequence of larger machines and measure their performance. Of course, there is innovation at each stage, but this is fundamentally a different approach than digital computing, be it classical or quantum digital computing,

In digital computing, noise manifests itself as discrete errors. That is, classically a 1 has become a 0 or vice versa. In quantum computing this would be described as a spin-flip error. In digital computing an error can be detected and corrected; this ability to fix discrete errors is the basis for scalability. In analog computing, noise distorts the computational state. Classically, the distortion is continuous, whereas it is discrete for a quantum system. This makes the noise difficult to detect and correct.

The primary advantage of analog quantum computing is that the computer is much simpler than a digital quantum computer, at least in principle. The disadvantage is that the analog quantum computer works for a small set of problems, whereas the digital quantum computer is universal in the sense that a Turing machine is universal for classical computing. The primary advantage of digital computing over analog computing is that once the enabling technology reaches a desired level of performance, the scale or size of the computer is limited by the available resources, although there are still issues with the overall error rate when the machine becomes large. For these reasons, DoD investment in analog quantum computing is not recommended.

5. Recommendations

> Recommendation 1: The DoD must be prepared to play a significant role in quantum computing, particularly throughout the (decade long) NISQ transitional phase, if it is concerned with quantum computing being a technology that significantly contributes to a shift in the balance of power.

Although a NISQ phase is critically important for the maturation of quantum computing technology, its promotion as a computational capability is largely a marketing effort by commercial companies to establish a revenue-generating product to support continuing R&D efforts. The primary concern for the DoD is that a failure of commercial companies to generate revenue through sales will cause these entities to significantly reduce R&D efforts and the U.S. lead in quantum computing will thereby vanish. Should this happen, the significant investment by the governments of other countries, notably China, will only serve to accelerate their progress and diminish the U.S. lead. The impact of this risk can be lessened by the U.S. Government, and the DoD in particular, having a significant effort in place to contribute to hardware development.

The primary motivation for this concern stems from the limited computational capability of NISQ machines and the expected decade-long duration of the NISQ era. The most powerful quantum algorithms, specifically Shor's algorithm and quantum simulation, are not within the capability of NISQ machines. Even though demonstration of these algorithms on toy problems is possible, there are insufficient computational resources on NISQ machines for them to have a quantum advantage over classical computational approaches. Working with large amounts of data in aggregate will not be possible with NISQ computers nor will it be likely with first-generation, fault-tolerate quantum computers. Much of the hope for NISQ computers lies in hybrid variational algorithms, although their practical utility is not clear.

> Recommendation 2: Portfolio- and project-level investment decisions by the DoD should reflect the strategic importance of quantum computing and simulation and not be based solely on applications that directly lead to new or improved military capabilities. At present, such applications for the DoD are unclear despite over 30 years of quantum computing algorithm research.

There is no clear and compelling strategic importance of quantum computing to the DoD at present. This is not the case for the Intelligence Community, where the existence of Shor's algorithm, even without a practical quantum computer for its execution, has major strategic concerns that are being addressed. Shor's algorithm is more than 20 years old, and there has been a robust search for other quantum algorithms, though none, with the possible exception of quantum simulation, has the same impact.

It is challenging for the DoD to support quantum computing based on an application well matched to the unique capabilities of a quantum computer. The support for quantum computing should be based, in part, on its importance as a strategic technology for the DoD. Whether or not quantum computing is in actuality a strategic technology for the DoD is unclear given the current state of its development and lack of key algorithms relevant to the DoD.

Much of the current algorithmic research is focused on hybrid algorithms for NISQ machines. These are variational approaches where the quantum computer is used to quickly prepare and measure a quantum state, and its optimization (for the intended application) is performed classically. Simple problems have been demonstrated on quantum computers for quantum simulation (the binding energy of H_2) and machine learning (binary classification using a SVM). There has also been interest in using a variational algorithm for approximate solutions to NP-complete problems. It is not clear if any of these approaches will have a quantum advantage, particularly on a NISQ machine.

Ultimately, quantum simulation may be the most important application for a quantum computer. Quantum simulation is the ability to predict the properties of quantum systems, such as ground-state energy of molecules and the temporal evolution of quantum states. Properties of quantum systems are difficult to predict because of the correlation present when systems are in entangled states, which are naturally accounted for when computed on a quantum computer. Because of its importance and long-term focus, the DoD should have a committed and sustained effort in quantum simulation, which will have the added benefit of maturing the enabling technology for other quantum computing applications.

> Recommendation 3: Develop a practical understanding of practical quantum computing based on engineering and benchmarking to improve on preliminary analysis arguing for the advantage of quantum computers based on algorithmic complexity.

Much of the quantum computing's perceived benefit is based on algorithmic complexity arguments, which give limiting forms of scaling of the number of (gate) operations as a function of the problem size. The use of oracles in algorithms further obscures any quantum advantage. The speedup of a quantum algorithm is the comparison complexity of the quantum algorithm to that of the best classical algorithm. These are operational counts and give no indication of the actual runtime of the algorithm.

Furthermore, operations can also be queries to an oracle that hides even more of the detail necessary for predicting actual runtimes.

For example, Shor's algorithm gives a superpolynimial speedup for factoring integers. That is, the best classical algorithm requires an exponential number of operations, but the quantum algorithm only requires a third-order polynomial number of (logical) gate operations. Such an analysis has little to say regarding the size an integer should be for which a quantum computer has an advantage over using a classical computer. It is clear that for a very large integer, the superpolynomial speedup will dominate all other considerations, but just how large must that number be for this to be so?

A more realistic understanding of practical quantum computing based on detailed considerations that include all operations for a computation on an appropriate model of a quantum computer is needed. This should include all I/O aspects of data, logic for quantum error correction, and logic for the problem. Such a program should be specific to platforms (e.g., trapped ion), error-correcting codes (e.g., surface codes), and working quantum memory. Such a program would have to develop practical and innovative approaches to issues. It would identify bottlenecks to performance and provide critical recommendations for advanced research on quantum computing. The level of analysis and the understanding it provides are absolutely essential for fault-tolerant quantum computing to become practical. While there is likely little benefit from this analysis for NISQ computing, starting it now, while practical FTQC is more than a decade away, would be highly beneficial in preventing surprise from other countries engaged in quantum computing research.

> Recommendation 4: Do not invest in other approaches to quantum computing until the benefits of computing are better characterized.

There are other approaches to quantum computing besides gate-based quantum computing, including adiabatic quantum computing, quantum annealing, and coherent Ising machines. All these approaches are analog in nature, as opposed to gate-based quantum computing (or, more simply, digital quantum computing), which is the primary focus of this section. The primary challenge with all these alternative forms of quantum computing is the role of noise and its effect on the computation. In analog computing, noise manifests itself as a distortion of the state between the intended state and the realized state. This is hard to correct, often dependent on the problem being computed, and, most important, limits scalability in unpredictable ways. Noise in gate-based quantum computing manifests itself as discrete gate errors, which can be corrected, at least in principle.

Adiabatic quantum computing has largely been abandoned because of these noise issues. There is strong consensus that there is no speedup offered by its successor, quantum annealing, unless the interaction is non-stoquastic, which significantly complicates the hardware, likely in a problem-dependent way. In more recent approaches, such as the

coherent Ising machine, the computation often ends up in a nearby state, which is only an approximate solution to the problem. The primary advantage of these approaches is that they use only physical qubits and consequently have the potential to need many fewer qubits for a computation. But that comes with price of not being able to control the noise. In addition, the range of computational problems accessible to an analog quantum computer is much more limited.

In light of the limited applications of analog quantum computing, fundamental concerns regarding scalability, and division of effort over the range of approaches to quantum computing, investment by the DoD in analog quantum computing should not be prioritized. Results and conclusions from IARPA's quantum enhanced optimization effort, which is exploring many of these issues, should provide sufficient information in several years to reevaluate a recommendation for the DoD not to fund other forms of quantum computing.

> Recommendation 5: The impact of quantum computing and simulations will be strategic and long term. The likelihood of technology surprise affecting military capabilities is low. The best way of avoiding surprise is with an open, long-term commitment to the development of quantum computing.

Credible sources estimate that a capable fault-tolerant computer is at least a decade away (Grumbling and Horowitz 2019). Most likely, quantum computing is more than a decade away, although it is difficult to reach any meaningful consensus on just how far away it is. Hence, technological surprise is unlikely.

The challenge with avoiding surprise in the long term is staying actively engaged in quantum computing research and development. Such a commitment will be challenging if practical applications having a clear quantum advantage are not developed during the NISQ phase. The most powerful algorithms for a quantum computer, specifically the mathematical algorithms (e.g., Shor's algorithm) and simulation algorithms, are far beyond the reach of NISQ phase computer. Many of these variational algorithms are unproven and are primarily being explored because there are no other algorithms having potential value for a NISQ computer.

Should quantum computing experience a "Quantum Winter" much as AI did in the mid-1970s and then later in late-1980s, leadership in the field is likely to be with the country or organization that remains actively engaged in research and development. The DoD is most likely to find itself being surprised should it focus on the utility of quantum computing during the NISQ phase at the expense of committing to a long-term effort. While searching for NISQ applications merits effort, it may be more important for the DoD to have a committed support on quantum simulation, for example, for the purpose of computing physical properties of quantum systems. Such an effort could be justified as developing a more foundational understanding of materials for advanced applications. For

example, research on room-temperature superconductivity could support the development of superconducting electromagnetic catapults for aircraft carriers. The value of other applications outside the mathematical and simulation areas is not clear.

Given the extent, cost, and long-term nature of developing a fault-tolerant quantum computer, collaborative research should be emphasized, keeping classified research to a minimum. This effort could be supported as part of the quantum computer science and engineering effort (see Recommendation 3).

5. Conclusions

A. Quantum Sensing and Metrology

Quantum sensing and metrology are very active directions for quantum science and technology, as described in Chapter 4. A large number of fields—such as magnetic, electric, photon, electromagnetic—can be sensed and measured with better precision than classical sensors. In addition, time, position, and acceleration can also be measured more precisely using quantum systems with both single and multiple qubits. A number of applications have been proposed. However, no reliable demonstrations have occurred yet (e.g., quantum radar). Although this is definitely a growth area for quantum science and technology, the DoD needs to clearly understand the potential capabilities and what impact they can have.

We note that these technologies are not expected to be disruptive changes in the state of the art. Consequently, the rise of China in this field is not expected to lead to any dire strategic disadvantages. Although advanced quantum sensors can provide significant improvements in terms of SWaP and performance in a number of different missions, future advances in this area by China and others are not expected to lead to a quantum surprise.

B. Quantum Cryptography and Communication

QKD and quantum communication via "teleportation" using quantum repeaters have been very active areas of research and development, starting with the landmark work by Bennett and Brassard (BB84) and the experimental demonstration of atom teleportation by Blatt in 2004. This direction has become quite mature; several companies are producing hardware that can be used for QKD over kilometer-scale distances.

It is clear from the results discussed in Section 4.B.3 that China is a dominant player in QKD technologies—China demonstrated QKD over a satellite link. But there are several challenges inherent in QKD (e.g., authentication) that currently preclude its use in practical applications. Although overcoming these challenges might be considered a "quantum-leap" in capability, there are several non-quantum alternatives to QKD for achieving secure communication. There is not much incentive to continue government support for this technology.

C. Quantum Computing

Given the broad prevalence of encryption methods that rely on prime factorization to secure communications, the rapid or sudden development of a working quantum computer

that can implement Shor's algorithm to factor large numbers would constitute a quantum surprise. This particular concern is well known and is under close watch by the Intelligence Community. Other potential surprises that may be of particular concern to DoD are not obvious. To date, only a small number of niche problems have been identified in the literature where fault-tolerant quantum computing provides a clear advantage over traditional methods. This may change over time as researchers gain more experience in NISQ computers, and it is worthwhile for DoD to monitor this area. Nevertheless, besides the potential impact on encryption, there is no clear strategic consequence to the rise of China and others in this field.

In summary, research in quantum computing can be divided into three distinct directions that depend on the type of problems addressed. They differ significantly in the resources needed to provide "quantum supremacy" (the ability to solve a problem faster than any classical computer or to solve a problem intractable for a classical computer):

1. Fully fault-tolerant error-corrected quantum processor—This implementation, which requires fully error-corrected logical qubits made up of many physical qubits, can implement Shor's algorithm to factor very large numbers in polynomial time. It was Shor's algorithm that triggered much of the first few decades of research into the requirements for such a processor and produced some processors with a handful of qubits. There has been much progress and significant investment, but a fully error-corrected quantum machine that can factor numbers used in current encryption protocols is still at least one to two decades away. There is still hope that other algorithms that can tackle many NP-hard or other hard problems can be found and thus drive the development of this type of processor. There are still significant investments in the United States and worldwide in this type of processor, including significant industry participation
2. Noisy intermediate-scale quantum processor—This implementation does not require fault-tolerant qubits, and there already are paths to build rather large numbers of these physical qubits. There are proposals to use this type of processor to solve some NP-hard optimization problems like the traveling salesman problem or other problems (not yet defined) where quantum supremacy can be demonstrated. Although the range of applications for such a processor is not currently clear, it is an area where significant progress can be made in a few years rather than in a few decades. DoD has to assess what capabilities can be enabled by supporting these efforts.
3. Adiabatic quantum computing and quantum annealing—Quantum processors that use qubits that have minimal entanglement but reasonable coherence have been built with up to several thousand qubits. They have been shown to solve problems like the Ising model or can evolve a given Hamiltonian. They have been proposed to be able to solve some optimization algorithms but the verdict

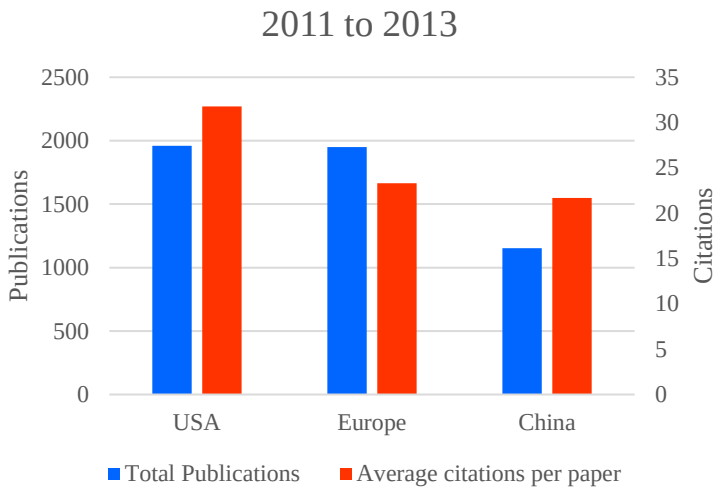
is out on whether they can exhibit quantum advantage.. Work on this type of processor has contributed to the infrastructure necessary for both the error-corrected and noisy quantum processors and thus is still very valuable research.

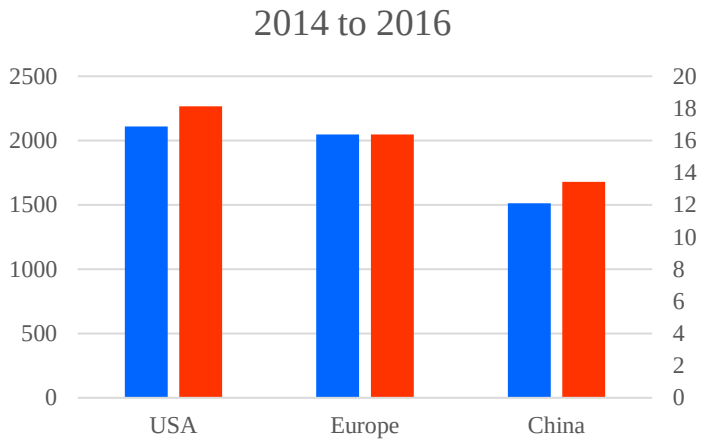
D. Overall

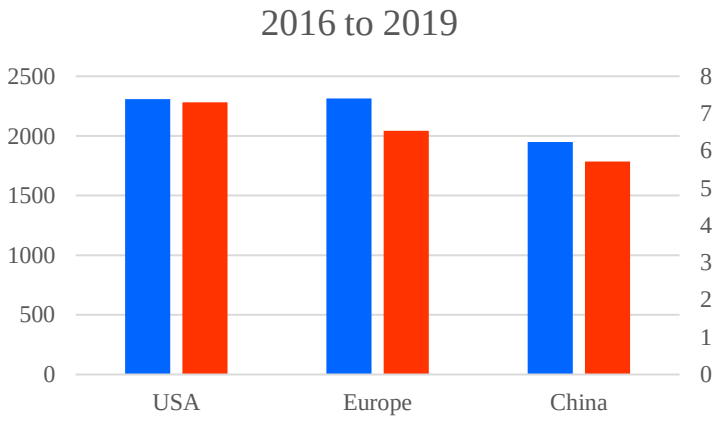
Overall, we recommend that DoD support for quantum information continue, although in a focused manner to heavily support those areas where applications important for the DoD have been identified or where some key capability is envisioned. Some specific areas that we feel are particularly important are those for precision navigation (time and position), magnetic field, electric field, and electromagnetic field sensing (quantum reciever), and development of noisy intermediate- and large-scale quantum processors that can be heavily exercised to find what problems they can tackle that are difficult or impossible for classical processors.

Appendix A.
Trends in Superconductivity and Magnetism Research

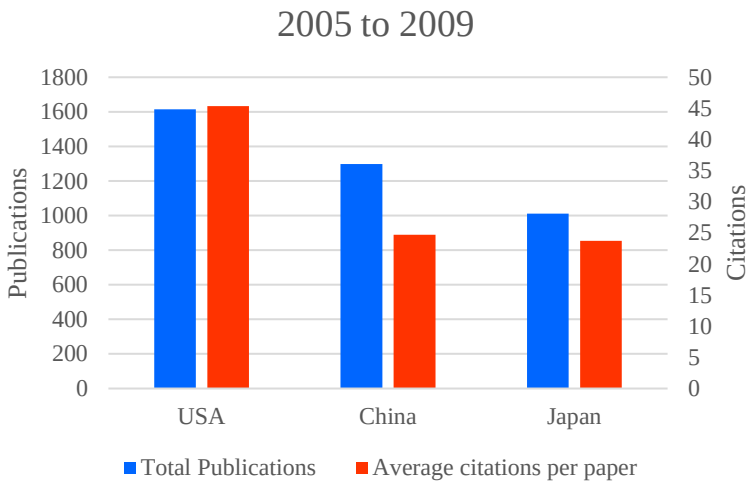
We also observed trends in related fields such as superconductivity and magnetism. The charts that follow show the increase in superconductivity research from 2011 to 2019 in China relative to the United States and Europe. The data in the first time interval of this trend analysis (2011–2013) show that China lagged the United States and Europe in both total publications and average citations per paper. In the most recent time interval (2016–2019), however, China gained significant ground in both metrics.

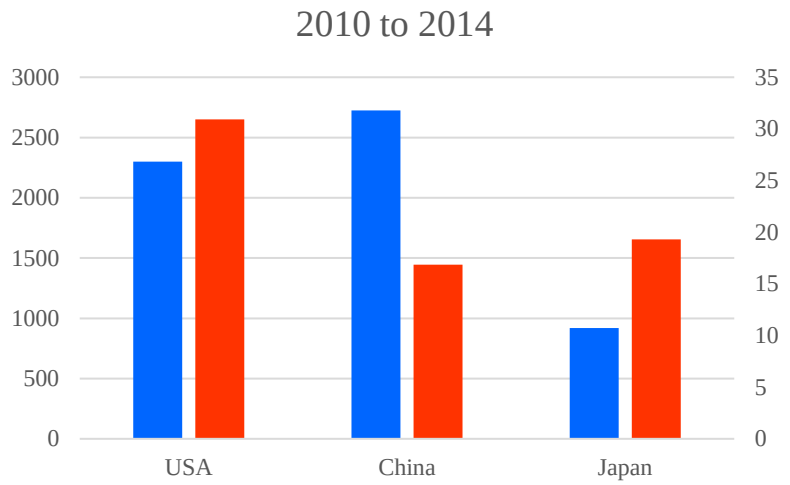


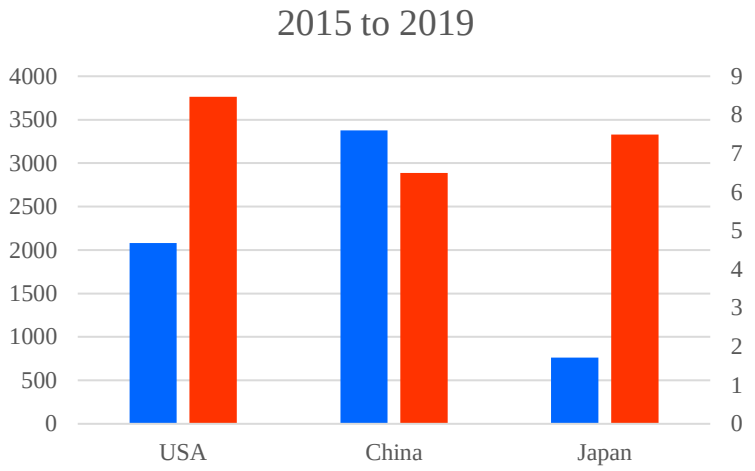




Similar trends are observed in magnetism research. The charts below show China surpassing the United States in magnetism research, in terms of total number of publications, in the 2005–2019 time period.







While these trends in superconductivity and magnetism research are not directly related to China's progress in quantum research, they do indicate that China has the

capability to make advancements in related research areas within a relatively short time frame. This further points to the need for the United States and its allies to continue making investments in quantum research and to stay abreast of the technological and research advances made by China and other adversaries.

References

Aaronson, Scott. 2015. “Read the Fine Print.” *Nature Physics* 11, no. 4: 291. https://doi.org/10.1038/nphys3272.

Aasen, David, Michael Hell, Ryan V. Mishmash, Andrew Higginbotham, Jeroen Danon, Martin Leijnse, Thomas S. Jespersen et al. 2016. “Milestones toward Majorana-based Quantum Computing.” *Physical Review X* 6, no. 3: 031016. https://doi.org/10.1103/PhysRevX.6.031016.

Amin, Mohammad H. 2015. “Searching for Quantum Speedup in Quasistatic Quantum Annealers.” *Physical Review A* 92, no. 5: 052323. https://doi.org/10.1103/PhysRevA.92.052323.

Anderson, David A, Rachel E Sapiro, and Georg Raithel. 2018. “An Atomic Receiver for AM and FM Radio Communication.” Preprint, submitted August 26, 2018. https://arxiv.org/abs/1808.08589.

Barrett, B., A. Bertoldi, and P. Bouyer. 2016. “Inertial Quantum Sensors Using Light and Matter.” *Physica Scripta* 91 (5): 053006.

Biamonte, Jacob, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. 2017. “Quantum Machine Learning.” *Nature* 549, no. 7671: 195. https://doi.org/10.1038/nature23474.

Biercuk, Michael J., Hermann Uys, Joe W. Britton, Aaron P. VanDevender, and John J. Bollinger. 2010. “Ultrasensitive Detection of Force and Displacement Using Trapped Ions.” *Nature Nanotechnology* 5:646. doi: 10.1038/nnano.2010.165.

Blatt, Rainer, and David Wineland. 2008. “Entangled States of Trapped Atomic Ions.” *Nature* 453, no. 7198: 1008. https://doi.org/10.1038/nature07125.

Born, M., and V. A. Fock. 1928. “Beweis des Adiabatensatzes.” *Zeitschrift für Physik A.* 51 (3–4): 165–80. https://doi.org/doi:10.1007/BF01343193.

Chailloux, André, María Naya-Plasencia, and André Schrottenloher. 2017. “An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography.” In *Advances in Cryptology – ASIACRYPT 2017*, edited by T. Takagi and T. Peyrin, 211–40, Springer, Cham. http://dx.doi.org/10.1007/978-3-319-70697-9_8.

Childs, Andrew M., and Wim Van Dam. 2010. “Quantum Algorithms for Algebraic Problems.” *Reviews of Modern Physics* 82, no. 1: 1. https://doi.org/10.1103/RevModPhys.82.1.

Cirac, J. Ignacio, and Peter Zoller. 2012. “Goals and Opportunities in Quantum Simulation.” *Nature Physics* 8, no. 4: 264. https://doi.org/10.1038/nphys2275.

Clark, Jack, and Kishan Saijel. 2015. “Quantum Computers Entice Wall Street Vowing Higher Returns.” Bloomberg. https://www.bloomberg.com/news/articles/2015-12-09/quantum-supercomputers-entice-wall-street-vowing-higher-returns.

Clarke, John, and Frank K. Wilhelm. 2008. “Superconducting Quantum Bits.” *Nature* 453, no. 7198: 1031. https://doi.org/10.1038/nature07128.

Cox, Kevin C., David H. Meyer, Fredrik K. Fatemi, and Paul D. Kunz. 2018. “Quantum-Limited Atomic Receiver in the Electrically Small Regime.” *Physical Review Letters* 121 (11): 110502. doi: 10.1103/PhysRevLett.121.110502.

Dang, H. B., A. C. Maloof, and M. V. Romalis. 2010. “Ultrahigh Sensitivity Magnetic Field and Magnetization Measurements with an Atomic Magnetometer.” *Applied Physics Letters* 97 (15): 151110. doi: 10.1063/1.3491215.

Degen, C. L, F. Reinhard, and P. Cappellaro. 2017. “Quantum Sensing.” *Reviews of Modern Physics* 89 (3):035002. doi: 10.1103/RevModPhys.89.035002.

Deutsch, David. 1985. “Quantum Theory, the Church–Turing Principle and the Universal Quantum Computer.” *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400, no. 1818: 97–117. https://doi.org/10.1098/rspa.1985.0070.

Diddams, S. A., Th. Udem, J. C. Bergquist, E. A. Curtis, R. E. Drullinger, L. Hollberg, W. M. Itano, W. D. Lee, C. W. Oates, K. R. Vogel, and D. J. Wineland. 2001. “An Optical Clock Based on a Single Trapped ¹⁹⁹Hg⁺ Ion.” *Science* 293 (5531):825-828. doi: 10.1126/science.1061171.

Facon, Adrien, Eva-Katharina Dietsche, Dorian Grosso, Serge Haroche, Jean-Michel Raimond, Michel Brune, and Sébastien Gleyzes. 2016. “A Sensitive Electrometer Based on a Rydberg Atom in a Schrödinger-Cat State.” *Nature* 535:262. doi: 10.1038/nature18327.

Farhi, Edward, Jeffrey Goldstone, and Sam Gutmann. 2014. “A Quantum Approximate Optimization Algorithm.” Preprint, submitted November 14, 2014. https://arxiv.org/abs/1411.4028.

Farhi, Edward, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. 2000. “Quantum Computation by Adiabatic Evolution.” Preprint, submitted January 28, 2000. https://arxiv.org/abs/quant-ph/0001106.

Farhi, Edward, Shelby Kimmel, and Kristan Temme. 2016. “A Quantum Version of Schöning’s Algorithm Applied to Quantum 2-SAT.” Preprint, submitted March 22, 2016. https://arxiv.org/abs/1603.06985.

Feynman, Richard P. “Simulating Physics with Computers.” *International Journal of Theoretical Physics* 21, no. 6 (1982): 467–88. https://doi.org/10.1007/BF02650179.

Figliola, Patricia Moloney. 2018. “Federal Quantum Information Science: An Overview.” *In Focus.* Washington, DC: Congressional Research Service. https://fas.org/sgp/crs/misc/IF10872.pdf.

Flamini, Fulvio, Nicolò Spagnolo, and Fabio Sciarrino. 2018. “Photonic Quantum Information Processing: A Review.” *Reports on Progress in Physics* 82 (1):016001. doi: 10.1088/1361-6633/aad5b2.

Georgescu, Iulia M., Sahel Ashhab, and Franco Nori. 2014. “Quantum Simulation.” *Reviews of Modern Physics* 86, no. 1: 153. https://doi.org/10.1103/RevModPhys.86.153.

Giovannetti, Vittorio, Seth Lloyd, and Lorenzo Maccone. 2008. “Quantum Random Access Memory.” *Physical Review Letters* 100, no 16:. 1060501. DOI: 10.1103/PhysRevLett.100.160501.

Gisin, Nicolas, and Rob Thew. 2007. “Quantum Communication.” *Nature Photonics* 1:165. doi: 10.1038/nphoton.2007.22.

Grover, Lov K. 1996. “A Fast Quantum Mechanical Algorithm for Database Search.” Preprint, submitted November 19, 1996. https://arxiv.org/abs/quant-ph/9605043v3.

Grumbling, Emily, and Mark Horowitz, eds. 2019. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press.

Grumbling, Emily, and Mark Horowitz, eds. 2019. *Quantum Computing: Progress and Prospects.* Consensus Study Report of the National Academies of Sciences, Engineering, and Medicine. Washington, DC: National Academies Press. https://doi.org/10.17226/25196.

Hadfield, S. 2018. “Quantum Algorithms for Scientific Computing and Approximate Optimization.” Preprint, submitted May 8, 2018. https://arxiv.org/abs/1805.03265.

Harrow, Aram W., Avinatan Hassidim, and Seth Lloyd. 2009. “Quantum Algorithm for Linear Systems of Equations.” *Physical Review Letters* 103, no. 15: 150502. https://doi.org/10.1103/PhysRevLett.103.150502.

Hastings, Matthew B. 2019. “Classical and Quantum Bounded Depth Approximation Algorithms.” Preprint, submitted May 16, 2019. arXiv preprint arXiv:1905.07047.

Havlíček, Vojtěch, Antonio D. Córcoles, Kristan Temme, Aram W. Harrow, Abhinav Kandala, Jerry M. Chow, and Jay M. Gambetta. 2019. “Supervised Learning with Quantum-Enhanced Feature Spaces.” *Nature* 567, no. 7747: 209. https://doi.org/10.1038/s41586-019-0980-2.

Herman, Arthur. 2018. “Winning the Race in Quantum Computing.” *American Affairs Journal*, May 21, 2018. Hudson Institute. https://www.hudson.org/research/14346-winning-the-race-in-quantum-computing.

Heshami, Khabat, Duncan G. England, Peter C. Humphreys, Philip J. Bustard, Victor M. Acosta, Joshua Nunn, and Benjamin J. Sussman. 2016. “Quantum Memories: Emerging Applications and Recent Advances.” *Journal of Modern Optics* 63 (20): 2005–28. doi: 10.1080/09500340.2016.1148212.

Inagaki, Takahiro, Yoshitaka Haribara, Koji Igarashi, Tomohiro Sonobe, Shuhei Tamate, Toshimori Honjo, Alireza Marandi et al. 2016. “A Coherent Ising Machine for 2000-node Optimization Problems.” *Science* 354, no. 6312: 603–6. https://doi.org/10.1126/science.aah4243.

Ivanov, Peter A., Nikolay V. Vitanov, and Kilian Singer. 2016. “High-Precision Force Sensing Using a Single Trapped Ion.” *Scientific Reports* 6:28078. doi: 10.1038/srep28078.

Jozsa, Richard, and Noah Linden. 2003. “On the Role of Entanglement in Quantum-Computational Speed-Up.” *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 459, no. 2036 (2003): 2011–32.

Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. 2016. “Breaking Symmetric Cryptosystems Using Quantum Period Finding.” In *Advances in Cryptology – CRYPTO 2016*, edited by M. Robshaw and J. Katz, 207–37, Berlin, Heidelberg: Springer.

Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. 2015. “Quantum Differential and Linear Cryptanalysis.” Preprint, submitted October 20, 2015. https://arxiv.org/abs/1510.05836.

Kaplan, Marc. “Quantum Attacks against Iterated Block Ciphers.” 2014. Preprint, submitted October 6, 2014. https://arxiv.org/abs/1410.1434.

Kloeffel, Christoph, and Daniel Loss. 2013. “Prospects for Spin-based Quantum Computing in Quantum Dots.” *Annu. Rev. Condens. Matter Phys.* 4, no. 1: 51-81. https://doi.org/10.1146/annurev-conmatphys-030212-184248.

Kominis, I. K., T. W. Kornack, J. C. Allred, and M. V. Romalis. 2003. “A Subfemtotesla Multichannel Atomic Magnetometer.” *Nature* 422:596. doi: 10.1038/nature01484.

Ladd, Thaddeus D., Fedor Jelezko, Raymond Laflamme, Yasunobu Nakamura, Christopher Monroe, and Jeremy Lloyd O’Brien. 2010. “Quantum Computers.” *Nature* 464, no. 7285: 45. https://doi.org/10.1038/nature08812.

Laflorencie, Nicolas. 2016. “Quantum Entanglement in Condensed Matter Systems.” *Physics Reports* 646: 1–59. https://doi.org/10.1016/j.physrep.2016.06.008.

Ledbetter, M. P., K. Jensen, R. Fischer, A. Jarmola, and D. Budker. 2012. “Gyroscopes Based on Nitrogen-Vacancy Centers in Diamond.” *Physical Review A* 86 (5): 052116. doi: 10.1103/PhysRevA.86.052116.

Lloyd, Seth, Masoud Mohseni, and Patrick Rebentrost. 2013. “Quantum Algorithms for Supervised and Unsupervised Machine Learning.” Preprint, submitted November 4, 2013. https://arxiv.org/abs/1307.0411.

Lloyd, Seth. 2008. “Enhanced Sensitivity of Photodetection via Quantum Illumination.” *Science* 321 (5895): 1463–65. doi: 10.1126/science.1160627.

Markov, Igor L., Aneeqa Fatima, Sergei V. Isakov, and Sergio Boixo. 2018. “Quantum Supremacy Is Both Closer and Farther Than It Appears.” arXiv preprint arXiv:1807.10749, submitted 2018. https://arxiv.org/abs/:1807.10749.

McClean, Jarrod R., Jonathan Romero, Ryan Babbush, and Alán Aspuru-Guzik. 2016. “The Theory of Variational Hybrid Quantum-Classical Algorithms.” *New Journal of Physics* 18, no. 2: 023023.

Montanaro, Ashley. 2016. “Quantum Algorithms: An Overview.” *npj Quantum Information* 2: 15023. https://doi.org/10.1038/npjqi.2015.23.

Nielsen, Michael A., and Isaac L. Chuang. 2010. *Quantum Computation and Quantum Information.* Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/CBO9780511976667.

Orús, Román, Samuel Mugel, and Enrique Lizaso. 2019. “Quantum Computing for Finance: Overview and Prospects.” *Reviews in Physics*: 100028. https://doi.org/10.1016/j.revip.2019.100028.

Peruzzo, Alberto, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O’brien. 2014. “A Variational Eigenvalue Solver on a Photonic Quantum Processor.” *Nature communications* 5: 4213. https://doi.org/10.1038/ncomms5213.

Pla, Jarryd J., Kuan Y. Tan, Juan P. Dehollain, Wee H. Lim, John JL Morton, David N. Jamieson, Andrew S. Dzurak, and Andrea Morello. 2012. “A Single-Atom Electron Spin Qubit in Silicon.” *Nature* 489, no. 7417: 541. https://doi.org/10.1038/nature11449.

Pomerance, Carl. 2008. “A Tale of Two Sieves.” *Biscuits of Number Theory* 85: 175. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.80.9198.

Prawer, Steven, and Andrew D. Greentree. 2008. “Diamond for Quantum Computing.” *Science* 320, no. 5883: 1601–2. https://doi.org/10.1126/science.1158340.

Preskill, John. 2018. “Quantum Computing in the NISQ Era and Beyond.” *Quantum* 2: 79. https://doi.org/10.22331/q-2018-08-06-79.

Reiher, Markus, Nathan Wiebe, Krysta M. Svore, Dave Wecker, and Matthias Troyer. 2017. “Elucidating Reaction Mechanisms on Quantum Computers.” *Proceedings of the National Academy of Sciences* 114, no. 29: 7555–60. https://doi.org/10.1073/pnas.1619152114.

Rudolph, Terry. 2017. “Why I am Optimistic about the Silicon-Photonic Route to Quantum Computing.” *APL Photonics* 2, no. 3: 030901. https://doi.org/10.1063/1.4976737.

Santoli, Thomas, and Christian Schaffner. 2017. “Using Simon’s Algorithm to Attack Symmetric-Key Cryptographic Primitives.” Preprint, submitted January 31, 2017. https://arxiv.org/abs/1603.07856v3.

Scherer, Artur, Benoît Valiron, Siun-Chuon Mau, Scott Alexander, Eric Van den Berg, and Thomas E. Chapuran. 2017. “Concrete Resource Analysis of the Quantum Linear-System Algorithm Used to Compute the Electromagnetic Scattering Cross Section of a 2D Target.” *Quantum Information Processing* 16, no. 3: 60. https://doi.org/10.1007/s11128-016-1495-5.

Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. 2015. “An Introduction to Quantum Machine Learning.” *Contemporary Physics* 56, no. 2: 172–85. https://doi.org/10.1080/00107514.2014.964942.

Shewchuk, Jonathan Richard. 1994. “An Introduction to the Conjugate Gradient Method without the Agonizing Pain.” Pittsburgh, PA: Carnegie Mellon University. https://www.cs.cmu.edu/~quake-papers/painless-conjugate-gradient.pdf.

Shor, Peter W. 1994. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–34. https://doi.org/10.1109/SFCS.1994.365700.

Taylor, J. M., P. Cappellaro, L. Childress, L. Jiang, D. Budker, P. R. Hemmer, A. Yacoby, R. Walsworth, and M. D. Lukin. 2008. “High-Sensitivity Diamond Magnetometer with Nanoscale Resolution.” *Nature Physics* 4:810. doi: 10.1038/nphys1075.

Wang, Zhe, Alireza Marandi, Kai Wen, Robert L. Byer, and Yoshihisa Yamamoto. 2013. “Coherent Ising Machine Based on Degenerate Optical Parametric Oscillators.” *Physical Review A* 88, no. 6: 063853. https://doi.org/10.1103/PhysRevA.88.063853.

Wasilewski, W., K. Jensen, H. Krauter, J. J. Renema, M. V. Balabas, and E. S. Polzik. 2010. “Quantum Noise Limited and Entanglement-Assisted Magnetometry.” *Physical Review Letters* 104 (13): 133601. doi: 10.1103/PhysRevLett.104.133601.

Weiss, David S., and Mark Saffman. 2017. “Quantum Computing with Neutral Atoms.” *Phys. Today* 70, no. 7: 44. http://dx.doi.org/10.1063/PT.3.3626.

Woerner, Stefan, and Daniel J. Egger. 2019. “Quantum Risk Analysis.” *npj Quantum Information* 5, no. 1: 15. https://doi.org/10.1038/s41534-019-0130-6.

Zhang, Zheshen, Sara Mouradian, Franco N. C Wong, and Jeffrey H. Shapiro. 2015. “Entanglement-Enhanced Sensing in a Lossy and Noisy Environment.” *Physical Review Letters* 114 (11): 110506. doi: 10.1103/PhysRevLett.114.110506.

Abbreviations

ACES	Atomic Clock with Enhanced Stability
AMBIIENT	Atomic Magnetometer for Biological Imaging In Earth's Native Terrain
CMOS	complementary metal oxide semiconductor
CQC	component quantum computing
DARPA	Defense Advanced Research Projects Agency
DRAM	dynamic random access memory
EPR	Einstein, Podolsky, and Rosen
FeMo-co	iron molybdenum cofactor (in the enzyme nitrogenase)
FTQC	fault-tolerant quantum computing
GPS	Global Positioning System
HHL	Harrow, Hassidim, and Lloyd
IARPA	Intelligence Advanced Research Projects Activity
NISQ	noisy intermediate-scale quantum
NP	nondeterministic polynomial time
NSA	National Security Agency
QAOA	quantum adiabatic optimization algorithm
QFT	quantum Fourier transform
QKD	quantum key distribution
QPE	quantum phase estimation
QuASAR	Quantum-Assisted Sensing and Readout
QUESS	Quantum Experiments at Space Scale
RSA	Rivest–Shamir–Adleman (public-key cryptosystem)
SVM	support vector machine
SWaP	size, weight, and power

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From–To)*
June 2019	FINAL	

4. TITLE AND SUBTITLE

Overview of the Status of Quantum Science and Technology and Recommendations for the DoD

5a. CONTRACT NUMBER
HQ0034-14-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Wolf, Stuart A.
Joneckis, Lance G.
Waruhiu, Steven
Biddle, John C.
Sun, Olivia S.
Buckley, Leonard J.

5d. PROJECT NUMBER
AI-2-4462

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document D-10709

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Basic Research Office
Office of the Assistant Secretary of Defense for Research and Engineering
4800 Mark Center Drive, Suite 17C08
Alexandria, VA 22350

10. SPONSOR/MONITOR'S ACRONYM(S)

ASD(R&E)/BRO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited (22 November 2019).

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Within the last few decades, quantum science and technology have become areas of tremendous worldwide interest, and have thus, garnered significant investment. We analyzed areas of quantum technology with the potential to change the way we sense, communicate, and compute. The focus of this report is on quantum sensing and metrology, quantum communication, and quantum computing, and what investments DoD should make to ensure the United States is not a victim of technological surprise.

15. SUBJECT TERMS

Quantum Computing, Quantum Communication, Quantum Sensing, Quantum Information

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Bindu Nair
Uncl.	Uncl.	Uncl.	SAR	71	19b. TELEPHONE NUMBER *(include area code)* (571) 372-6460

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18