United States Government Accountability Office

Report to Congressional Addressees

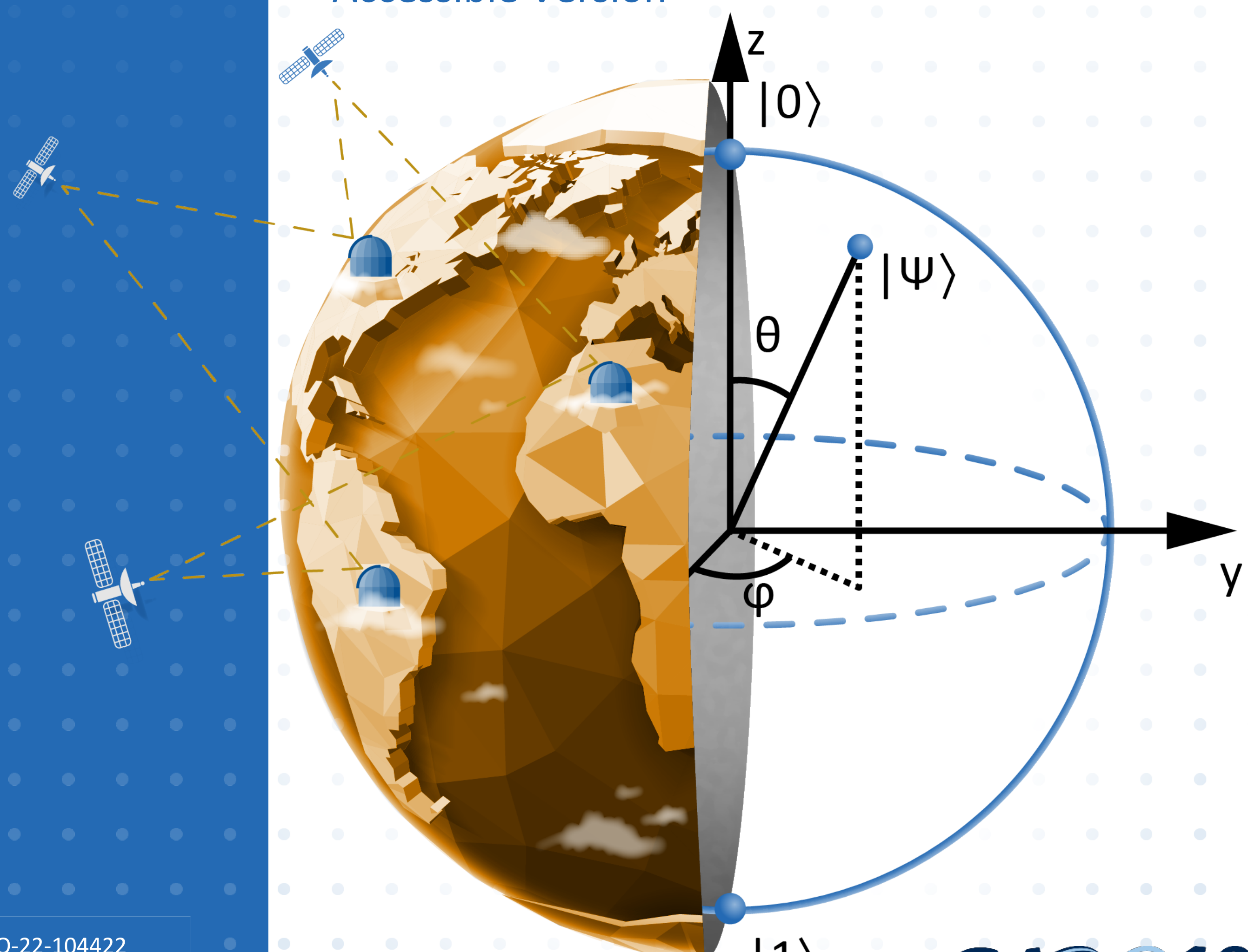
October 2021

TECHNOLOGY ASSESSMENT

Quantum Computing and Communications

Status and Prospects

Accessible Version



GAO-22-104422

A Century of Non-Partisan Fact-Based Work

The cover image displays a stylized representation of quantum computing and communications technology elements. A satellite network (left) could enable quantum communications, allowing users to exchange quantum information over long distances. The Bloch sphere (right) is a useful tool to visualize all possible states of a single qubit, the quantum equivalent of the classical bit, and the fundamental component of quantum computing and communications hardware. While a classical bit is either a 0 or a 1, a qubit can be any combination of 0 and 1 that is represented mathematically by a point on the sphere.

Image source: GAO and Kundra/stock.adobe.com. | GAO-22-104422

DRAFT

TECHNOLOGY ASSESSMENT

GAO Highlights

Highlights of GAO-22-104422, a report to congressional addressees

October 2021

Why GAO did this study

Quantum information technologies could dramatically increase capabilities beyond what is possible with classical technologies. Future quantum computers could have high-value applications in security, cryptography, drug development, and energy. Future quantum communications could allow for secure communications by making information challenging to intercept without the eavesdropper being detected.

GAO conducted a technology assessment on (1) the availability of quantum computing and communications technologies and how they work, (2) potential future applications of such technologies and benefits and drawbacks from their development and use, and (3) factors that could affect technology development and policy options available to help address those factors, enhance benefits, or mitigate drawbacks.

To address these objectives, GAO reviewed key reports and scientific literature; interviewed government, industry, academic representatives, and potential end users; and convened a meeting of experts in collaboration with the National Academies of Sciences, Engineering, and Medicine. GAO is identifying policy options in this report.

View GAO-22-104422. For more information, contact Karen L. Howard at (202) 512-6888 or howardk@gao.gov.

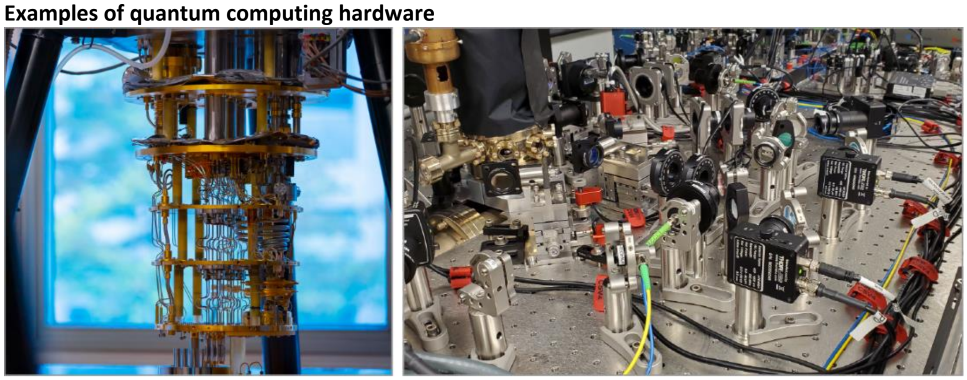
Quantum Computing and Communications

Status and Prospects

What GAO found

Quantum information technologies aim to use the properties of nature at atomic scales to accomplish tasks that are not achievable with existing technologies. These technologies rely on *qubits*, the quantum equivalent of classical computer bits. Scientists are creating qubits from particles, such as atoms or particles of light, or objects that mimic them, such as superconducting circuits. Unlike classical bits, qubits can be intrinsically linked to each other and can be any combination of 0 and 1 simultaneously. These capabilities enable two potentially transformational applications—quantum computing and communications. However, quantum information cannot be copied, is fragile, and can be irreversibly lost, resulting in errors that are challenging to correct.

Examples of quantum computing hardware



Many different types of quantum computers are being developed. The left image shows superconducting quantum computer hardware. The right image shows trapped ion quantum computer hardware.

Source: ©Intel Corporation (left photo); Chris Seck, Oak Ridge National Laboratory (right photo). | GAO-22-104422

Some quantum computing and communications technologies are available for limited uses, but will likely require extensive development before providing significant commercial value. For example, some small error-prone quantum computers are available for limited applications, and a quantum communications technology known as quantum key distribution can be purchased. According to agency officials and stakeholders, additional quantum technology development may take at least a decade and cost billions, but such estimates are highly uncertain. Quantum computing and communications technologies will likely develop together because of some shared physics principles, laboratory techniques, and common hardware.

Quantum computers may have applications in many sectors, but it is not clear where they will have the greatest impact. Quantum communications technologies may have uses for secure communications, quantum networking, and a future quantum internet. Some applications—such as distributed quantum computing, which connects multiple quantum computers together to solve a problem—require both quantum computing and communications technologies. Potential drawbacks of quantum technology include cost, complexity, energy consumption, and the possibility of malicious use.

GAO identified four factors that affect quantum technology development and use: (1) collaboration, (2) workforce size and skill, (3) investment, and (4) the supply chain. The table below describes options that policymakers—legislative bodies, government agencies, standards-setting organizations, industry, and other groups—could consider to help address these factors, enhance benefits, or mitigate drawbacks of quantum technology development and use.

Policy Options to Help Address Factors that Affect Quantum Technology Development and Use, or to Enhance Benefits or Mitigate Drawbacks

Policy options and potential implementation approaches	Opportunities	Considerations
Collaboration (report p. 37) Policymakers could encourage further collaboration in developing quantum technologies, such as collaboration among: • Scientific disciplines • Sectors • Countries	• Collaboration among disciplines could enable technology breakthroughs. • Collaboration could help accelerate research and development, as well as facilitate technology transfer from laboratories to the private sector, federal agencies, and others. • International collaboration could bring mutual benefits to the U.S. and other countries by accelerating scientific discovery and promoting economic growth.	• Intellectual property concerns could make quantum technology leaders reluctant to collaborate. • Institutional differences could make collaboration difficult. • Export controls may complicate international collaboration, but are also needed to manage national security risks.
Workforce (report p. 39) Policymakers could consider ways to expand the quantum technology workforce by, for example: • Leveraging existing programs and creating new ones • Promoting job training • Facilitating appropriate hiring of an international workforce who are deemed not to pose a national security risk	• Educational programs could provide students and personnel with the qualifications and skills needed to work in quantum technologies across the private sector, public sector, and academia. • Training personnel from different disciplines in quantum technologies could enhance the supply of quantum talent. • International hiring could allow U.S. quantum employers to attract and retain top talent from other countries.	• Efforts to increase the quantum technology labor force may affect the supply of expertise in other technology fields with high demand. • It may be difficult to adequately develop workforce plans to accommodate quantum technology needs. • International hiring could be challenging because of visa requirements and export controls, both in place for national security reasons.
Investment (report p. 41) Policymakers could consider ways to incentivize or support investment in quantum technology development, such as: • Investments targeted toward specific results • Continued investment in quantum technology research centers • Grand challenges to spur solutions from the public	• More targeted investments could help advance quantum technologies. These may include investments in improving access to quantum computers and focusing on real-world applications. • Quantum technologies testbed facility investments could support technology adoption, since testbeds allow researchers to explore new technologies and test the functionality of devices. • Grand challenges have shown success in providing new capabilities and could be leveraged for quantum technologies.	• It may be difficult to fund projects with longer-term project timeframes. • A lack of standards or, conversely, developing standards too early, could affect quantum technology investments. Without standards, businesses and consumers may not be confident that products will work as expected. • Developing standards too early may deter the growth of alternative technology pathways.
Supply Chain (report p. 43) Policymakers could encourage the development of a robust, secure supply chain for quantum technologies by, for example: • Enhancing efforts to identify gaps in the global supply chain • Expanding fabrication capabilities for items with an at-risk supply chain	• A robust supply chain could help accelerate progress and mitigate quantum technology development risks by expanding access to necessary components and materials or providing improved economies of scale. • Quantum material fabrication capabilities improvements could ensure a reliable supply of materials to support quantum technology development. • Facilities dedicated to producing quantum materials could help support scalable manufacturing of component parts needed for quantum technology development.	• The current quantum supply chain is global, which poses risks. For example, it is difficult to obtain a complete understanding of a component's potential vulnerabilities. • Some critical components, such as rare earths, are mined primarily outside of the U.S., which may pose risks to the supply chain that are difficult to mitigate. • Quantum manufacturing facilities take a long time to develop and can be costly.

Source: GAO. | GAO-22-104422

Table of Contents

Abbreviations

DOD	Department of Defense
DOE	Department of Energy
EAR	Export Administration Regulations
ITAR	International Traffic in Arms Regulations
National Academies	National Academies of Sciences, Engineering, and Medicine
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSF	National Science Foundation

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Introduction

October 19, 2021

Congressional Addressees

Quantum information technologies build on the study of quantum physics to collect, generate, and process information in ways not achievable with existing technologies.[1] One such technology, a quantum computer, could address some problems that are intractable on any possible classical computers, including the most powerful supercomputers.[2] Future quantum computing could break cryptographic schemes by factoring the large numbers used in encryption, as well as simulate chemical reactions that are critical to drug development, energy storage, and other high-value commercial applications.

A related category of technology, quantum communications, could allow for more secure communications by making information challenging to intercept without the eavesdropper being detected.[3] Quantum communications networking could revolutionize aspects of information transmission, and some people consider building and scaling such networks to be among the most important technological frontiers of the 21st century.[4]

The National Science and Technology Council has reported that the United States could improve its industrial base, create jobs, and realize economic and national security benefits through quantum technology development.[5] In 2018, Congress passed the National Quantum Initiative Act, providing for a coordinated federal program to accelerate quantum research and development for the economic and national security of the United States.[6] The 2019 National Defense Authorization Act (NDAA) authorized the creation of a defense quantum information

[1]Quantum technologies broadly include quantum computing, quantum communications, and quantum sensing. For this technology assessment, we focus on quantum computing and communications technologies.

[2]National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, D.C.: National Academies Press. 2019). Computers that process information according to the laws of classical physics are "classical computers." Quantum computers rely on the laws of quantum physics to process information.

[3]The Department of Defense (DOD) considers quantum communications to be a subset of quantum networks and defines a quantum network as a set of interconnected devices or nodes that function together to achieve overarching goals.

[4]K. Kleese van Dam, *From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop,* BNL-216179-2020-FORE (Department of Energy, Office of Science, July 2020).

[5]National Science and Technology Council, Subcommittee on Quantum Information Science, *National Strategic Overview for Quantum Information Science* (September 2018).

[6]National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092-5103 (2018).

science and technology research and development program.[7] Companies and other countries have also prioritized quantum technology development.

We prepared this report under the authority of the Comptroller General to assist Congress with its oversight responsibilities, in light of the broad congressional interest in and crosscutting nature of quantum technologies. We examined (1) the availability of quantum computing and communications technologies and how they work, (2) potential future applications of such technologies and the potential benefits and drawbacks from their development and use, and (3) factors that could affect the development and use of such technologies and the policy options available to help address those factors, enhance benefits, or mitigate drawbacks. See Appendix I for a detailed description of our objectives, scope, and methodology.

To conduct our work, across all three objectives, we:

- Interviewed officials from the Department of Defense (DOD), Department of Energy (DOE), Intelligence Advanced Research Projects Activity, National Aeronautics and Space Administration (NASA), National Institute of Standards and Technology (NIST), National Science Foundation (NSF), and Office of Science and Technology Policy, and a non-generalizable sample of stakeholders from academia, industry, and trade groups. Our interviews focused on quantum computing and communications activities, technology uses, potential future applications, and the potential benefits, drawbacks, and considerations related to developing such technologies. We selected stakeholders based on expertise in quantum computing or communications technologies, understanding of potential applications, or understanding of the effects of those applications.
- Interviewed potential end users about plans to use a quantum computer and the technology's benefits and drawbacks. We selected a non-generalizable sample of six potential end users from multiple sectors including the pharmaceutical and finance sectors, based on continued company interest in quantum computing, press releases or published articles, collaborations with quantum computing companies, and being a potential end user not directly involved with the creation of a quantum computer.
- Reviewed agency documents and documents suggested during interviews or identified by GAO to provide insights into the maturity of quantum computing and communications technologies, their applications, the potential benefits and drawbacks of their usage, and policy options. A GAO librarian also conducted a legal literature search in topic areas such as quantum computing and communications encryption, privacy, and standards to help provide insights into the legal landscape that may affect the development and use of quantum computing and communications technologies.

---

[7] John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, Pub. L. No. 115-232, div. A, tit. II, § 234, 132 Stat. 1636, 1692-93 (2018), as amended by Pub. L. No. 116-92, div. A, tit. II, § 220, 133 Stat. 1198, 1260-61 (2019) and Pub. L. No. 116-283, div. A, tit. II, § 214, 134 Stat. 3388, 3458 (2021).

- Convened a one-and-a-half day meeting of experts from academia, government, and industry. We invited these experts with assistance from the National Academies of Sciences, Engineering, and Medicine (National Academies)—based on expertise in quantum computing, quantum communications, quantum applications, and the economic, social, or legal implications of quantum computing and communications technologies—to obtain a range of perspectives on the maturity of quantum computing and communications technologies, challenges, factors that could affect technology development and use, applications, and policy options. See Appendix II for a list of experts who participated in our meeting.

For objective 3, in addition to the steps above, we identified policy ideas from the above evidence. These policy ideas were developed into policy options by combining similar ideas and removing those that were duplicative, could be grouped into a higher-level policy option, were examples of how to implement a policy option, or did not fit into our scope.

We conducted our work from July 2020 to October 2021 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

1 Background

1.1 Introduction to quantum computing and communications technologies

Two characteristics distinguish quantum information technologies from classical information technologies.[8] First, they rely on quantum physics: the sometimes counterintuitive properties of nature at atomic scales.[9] Second, measuring or observing a quantum system fundamentally changes quantum information. These two characteristics cause quantum technologies to process information in a way that is fundamentally different from classical technologies.[10] The difference in processing information begins at the smallest level—a quantum bit, or qubit, which is analogous to a bit in a classical computer.[11] Quantum computers can, for some problems, dramatically increase processing speed compared to a classical computer. Quantum communications technologies can transmit qubits while maintaining their quantum properties, which is needed to achieve certain security protocols and connect quantum devices.

One way quantum technologies process and send information differently is by using *superposition*–a property of quantum physics that allows qubits to be in a combination of states simultaneously. Whereas a classical bit can be in a state of 0 or 1, a qubit can be in some combination 0 and 1 at the same time; upon measurement, a qubit will resolve to one of the states composing the superposition, destroying the superposition (see app. III for selected definitions). Quantum technologies also use *entanglement*, where qubits are intrinsically linked so that when one qubit is acted upon—such as through measurement—it can reveal information about the other qubits, something that does not occur with classical bits.[12] Superposition and entanglement, among other things, give rise to the potentially transformational applications of quantum computing and communication.

Scientists are working to create quantum technologies by creating physical qubits from a variety of systems including:

- Particles such as atoms, ions, and particles of light, known as *photons*.
- Objects that mimic particles, such as *superconducting circuits* (i.e., electronic circuits without electrical resistance), *quantum dots* (small semiconducting crystals that resemble transistors), and defects in a crystal (e.g., a nitrogen atom within a diamond's carbon lattice, known as a *color center*).

[8]Quantum sensing is another quantum technology, but it is outside the scope of this technology assessment.

[9]Quantum physics explains the behavior and interactions of small particles such as atoms, molecules, electrons, and photons.

[10]Classical information technologies follow the laws of classical physics and consist of methods for information transfer and information processing, including supercomputers, the internet, and personal computing devices.

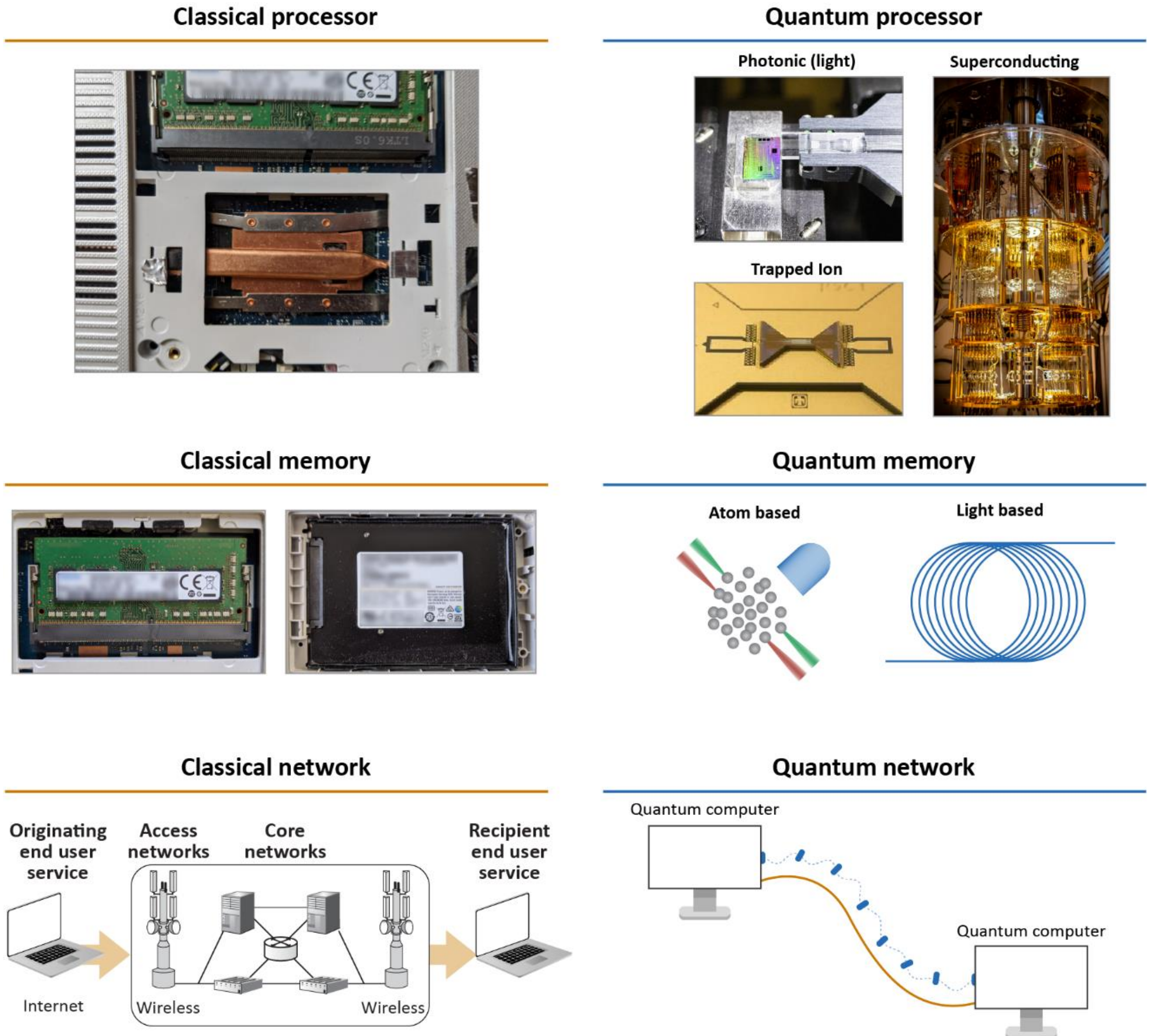
[11]A bit, or binary digit, is the most elementary unit of classical computing and communications information; it is represented by either a 0 or a 1.

[12]Quantum entanglement does not allow for information transfer at speeds faster than the speed of light.

To create quantum technologies from these qubits, scientists manipulate the quantum properties of each qubit and entangle multiple qubits with one another. These manipulations are accomplished with lasers, microwaves, electric or magnetic fields, and other ways to control qubits. However, quantum technologies have not yet been perfected. Quantum information is fragile and can be irreversibly lost through interactions with the environment, in a process called *decoherence*. The *quantum coherence time* is how long a qubit maintains a superposition or entangled state before decoherence, a factor that limits how long a qubit can be used for an operation. Classical information can also be lost to the environment, but classical computers employ automatic error detection or correction techniques to mitigate the effects of information loss by, for example, copying the state of the system so that subsequent errors can be detected and corrected. However, quantum information cannot be copied, and measurement disrupts the information, preventing the implementation of classical error correction techniques. Quantum error correction techniques have been proposed and demonstrated but are challenging to implement. Quantum error correction procedures use many error-prone physical qubits working together and with classical processing to create a system that mimics a robust and stable single qubit—known as a *logical qubit*.

Quantum information technologies may add new functionalities to supplement and enhance classical information technologies but will use different hardware to do so (see fig. 1).

Figure 1: Examples of classical and quantum technology hardware



Sources: GAO; GAO analysis of communications sector data and peer-reviewed journals; Oak Ridge National Laboratory, U.S. Dept. of Energy, Carlos Jones, ORNL Photographer (Photonic image); © 2020 Akel Hashim (Superconducting image); Peter Maunz, formerly of Sandia National Laboratories (Trapped ion image); Júlia Fort Muñoz for TU Delft (Quantum network image). | GAO-22-104422

1.2 History of quantum technologies

After the field of quantum physics was developed in the early 20th century, researchers began to explore its application to quantum technologies. In 1959, researcher Richard Feynman suggested it may be possible to manipulate matter at an atomic scale, implying certain types of calculations could be completed more efficiently on quantum systems than on classical technologies.[13] At the first conference on the physics of computation, in 1981, researchers observed that it may be impossible to

[13] Feynman delivered a talk on manipulating and controlling things on a small scale, later published in the February 1960 issue of *Engineering and Science* Magazine. R.P. Feynman, "There's Plenty of Room at the Bottom: An invitation to enter a new field of physics," *Engineering and Science*, (Feb. 1960) pp. 22-36.

efficiently simulate a quantum system's evolution on a classical computer, and proposed a basic model for quantum computing. Meanwhile, researchers began to build off classical information theory to develop an understanding of quantum information, such as the understanding that quantum information could not be copied the way classical information could be.

The late 20th century marked other advances in quantum theory, including:

- In 1984, researchers described a quantum key distribution scheme in which an eavesdropper would have a high probability of being detected when attempting to spy on an encrypted key exchange that uses qubits to transmit information. This scheme, commonly called BB84, is regarded as the first quantum cryptography protocol.[14] In 1991, researchers expanded on the BB84 protocol and introduced a different approach to quantum key distribution that incorporates entanglement.[15]
- In 1994, Peter Shor, a researcher at Bell Labs, introduced Shor's algorithm, an algorithm that could factor very large numbers if a quantum computer were to be developed.[16] This algorithm has the potential to crack current encryption schemes used in secure transactions, some of which are based on the assumption that factoring large numbers is impractical.

The first experimental achievements in quantum technologies also came in the late 20th century:

- In 1972, researchers showed that measurements of one qubit can affect the measurement of other qubits, demonstrating entanglement for the first time.[17]
- In 1987, researchers measured the time intervals between two photons and found that they were indistinguishable from one another, a property necessary for photon entanglement.[18]
- In 1995, researchers demonstrated the first quantum logic gate based on individual qubits.[19]
- In 1998, researchers demonstrated through a proof of principle experiment that quantum error correction is possible, which is necessary for cost-effective

[14] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *International Conference on Computers, Systems, and Signal Processing, 1984,* (December 1984): pp. 175-179. According to an expert, BB84 was based on a scheme for quantum money that is, in principle, impossible to counterfeit, as proposed by Stephen Wiesner in 1970.

[15] A. K. Eckert, "Quantum Cryptography Based on Bell's Theorem." *Physical Review Letters*, vol. 67, no. 6, (Aug. 5, 1991), pp. 661-663.

[16] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *35th Annual Symposium on Foundations of Computer Science*, (November 1994): pp. 124-134.

[17] S. J. Freedman and J. F. Clauser, "Experimental Test of Local Hidden-Variable Theories," *Physical Review Letters*, vol. 28, no. 14, (Apr. 3, 1972), pp. 938-941.

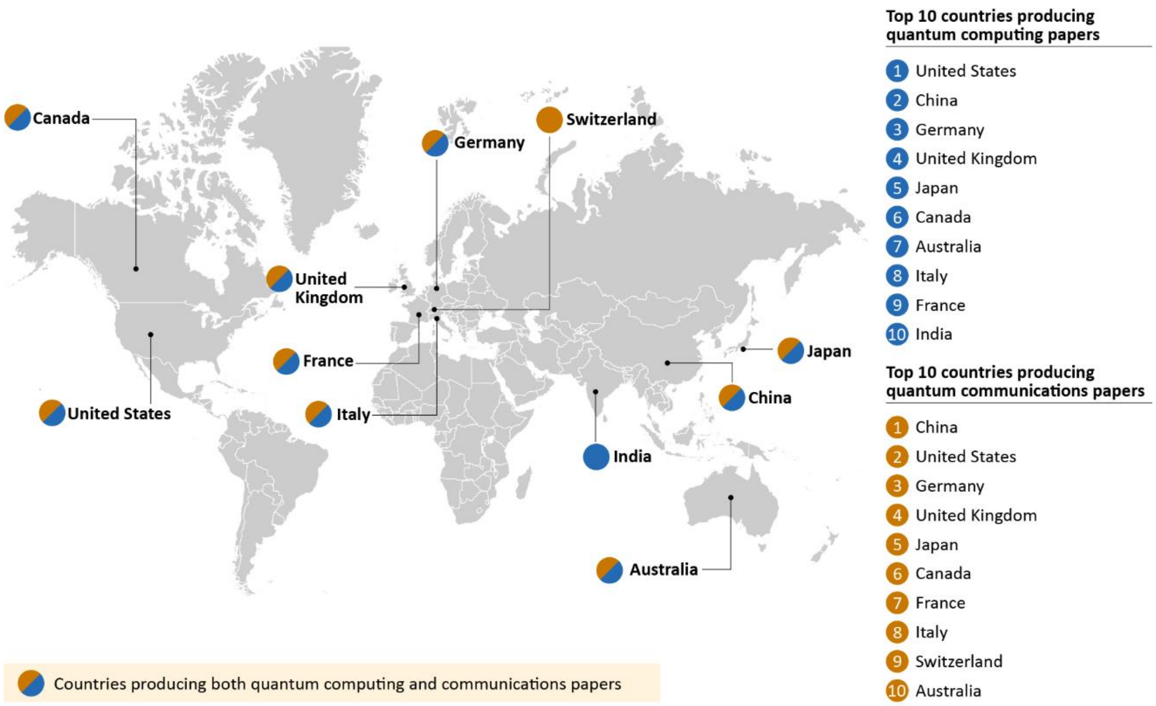
[18] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of Subpicosecond Time Intervals between Two Photons by Interference, " *Physical Review Letters,* vol. 59, no. 18, (Nov. 2, 1987), pp. 2044- 2046.

[19] Logic gates are the building blocks for processing information (bits) in classical computation. Engineers can arrange logic gates in a circuit and create a flowchart that enables computers to carry out several kinds of logical operations, such as mathematical calculations. A quantum logic gate is similar, but uses qubits instead of traditional bits.

quantum computing and communication because excess noise destroys quantum information.[20]

Quantum technologies continue to improve. Demonstrations range from a 3-qubit magnetic resonance machine in 1998, a 14-qubit entangled state using a trapped ion quantum computing system in 2010, a 53-qubit superconducting quantum computing system in 2019, and a 76-qubit, photon-based system in 2020.[21] One company plans to build a 1,000-plus qubit device by 2023. Because of a quantum computer's potential uses, academics, companies, and governments are pursuing research and development in quantum technologies (see fig. 2).[22] Quantum communications improvements include advancements in quantum repeater research, a quantum network testbed that uses

Figure 2: Top ten countries producing quantum computing and communications research papers from 1996 to 2016



Source: GAO analysis of data from Jacob Farinholt, Trends in Quantum Computing, (October 2019). | GAO-22-104422

[20]In a quantum computer, noise—measured by error rates and qubit coherence times—limits the complexity of the problems that the computer can solve. Error correction algorithms are intended to create a noise-free quantum computer.

[21]J. A. Jones, "Quantum computing and nuclear magnetic resonance," *PhysChemComm,* vol. 11 (June 11, 2001) pp. 1-8; T. Monz et al., "14-Qubit Entanglement: Creation and Coherence," *Physical Review Letters*, vol. 106 (April 1, 2011 p.130506; F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574 (Oct. 24, 2019) pp. 505-510; H. S. Zhong, et al., "Quantum computational advantage using photons," *Science*, vol. 370, (Dec. 18, 2020) pp. 1460-1463.

[22]We previously reported on quantum computing research conducted at federal agencies and within select nonfederal groups. See GAO, *Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas*, GAO-18-656, (Washington, D.C.: Sept. 26, 2018).

portable quantum entanglement sources, and a 2020 roadmap for building the first nationwide quantum internet in the U.S.[23]

1.3 Applicable laws on quantum information science

Since 2018, Congress has passed laws authorizing the establishment of quantum information science research and development programs.

- In 2018, Congress passed the National Quantum Initiative Act to establish a whole-of-government approach to quantum information science.[24] It established a 10 year national quantum initiative program to accelerate development of quantum information science and technology applications, invest in workforce development, and improve coordination of federal quantum information science research, among other things. The National Quantum Coordination Office, established pursuant to the Act, is responsible for overseeing interagency coordination of the program and serving as the point of contact on Federal civilian quantum information science and technology activities for entities including Federal departments and agencies, state governments, industries and universities, among other responsibilities. The Act also directed the establishment of a consortium and multiple centers. The Act required NIST to establish a quantum consortium to identify future measurement, standards, cybersecurity, and other needs for supporting the development of a robust quantum technology industry.[25] In addition, NSF established five multidisciplinary centers for quantum research and education and DOE established five national quantum information science research centers in response to National Quantum Initiative Act requirements to establish at least two, and no more than five, of each type of center.
- The 2019 NDAA authorized DOD's Quantum Information Science and Technology Research and Development Program to, among other things, establish, support, and coordinate DOD quantum information science research and development, and to accelerate quantum information science concept and technology transition and deployment into the Armed Forces.[26] Amendments to the program, contained in the fiscal year 2020 NDAA include requirements for creating quantum information science workforce development plans, enhancing awareness of the field, reducing the risk of cybersecurity threats posed by quantum information science, and developing

[23] Kleese van Dam, *From Long-distance Entanglement to Building a Nationwide Quantum Internet*.

[24] National Quantum Initiative Act, Pub. L. No. 115-368, 132 Stat. 5092-5103 (2018).

[25] The Quantum Economic Development Consortium is a consortium of stakeholders that aims to enable and grow the U.S. quantum industry. It is focused on identifying workforce needs, identifying technology gaps, supporting standards development, and engaging with U.S. government agencies. It was established with support from NIST as part of the federal strategy for advancing quantum information science and as called for by the National Quantum Initiative Act.

[26] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, div. A, tit. II, § 234, 132 Stat. 1636, 1692-93 (2018), as amended by Pub. L. No. 116-92, div. A, tit. II, § 220, 133 Stat. 1198, 1260-61 (2019) and Pub. L. No. 116-283, div. A, tit. II, § 214 134 Stat. 3388, 3458 (2021).

ethical guidelines for the use of technologies; and establishing at least one quantum information science research center. Additional amendments to the program contained in the fiscal year 2021 NDAA require programs for small- and medium-sized businesses to provide functional quantum computing capabilities to government, industry, and academic researchers; and development of an annually updated list of technical problems and research challenges likely addressable by quantum computers available for use in the next 1 to 3 years.

2 Some Quantum Technologies Could Take at Least a Decade to Mature

Some quantum technologies are available for limited uses. Nevertheless, it will likely take at least a decade and cost billions to develop quantum technologies for more complex uses, according to stakeholders and agency officials. However, such estimates are highly uncertain. Regarding quantum computing and quantum communications technologies, they are interconnected and likely to develop together.

2.1 Some quantum technologies are available for limited uses

2.1.1 Quantum computing

There are two main quantum computing methods. The first is analog quantum computing, which works by preparing an initial set of qubits representing all possible solutions to a problem and exploiting the properties of superposition and entanglement, such that the set of qubits evolves and identifies an optimal solution. The most mature version of an analog quantum computer is a *quantum annealing machine*. Quantum annealing machines are available for purchase or for limited applications over the internet (see text box). Other analog quantum computing technologies include adiabatic quantum computing and quantum simulation.

Quantum annealing machines

Quantum annealing machines, a type of analog quantum computer, are designed to solve certain optimization problems. With these problems, the number of possible solutions increases exponentially, meaning it grows more rapidly with increasing problem size. This makes many optimization problems impractical to solve with a classical computer. A quantum annealing machine places a system of qubits in an initial state representing all possible solutions to a problem. The set of qubits then evolves and identifies an optimal solution using the quantum physics properties of superposition and entanglement. Quantum annealing machines provide a method for designing an approach to solve a specific problem without performing computations on individual qubits and may have uses in optimizing drug design, donor matching, traffic flows, and transportation routes.

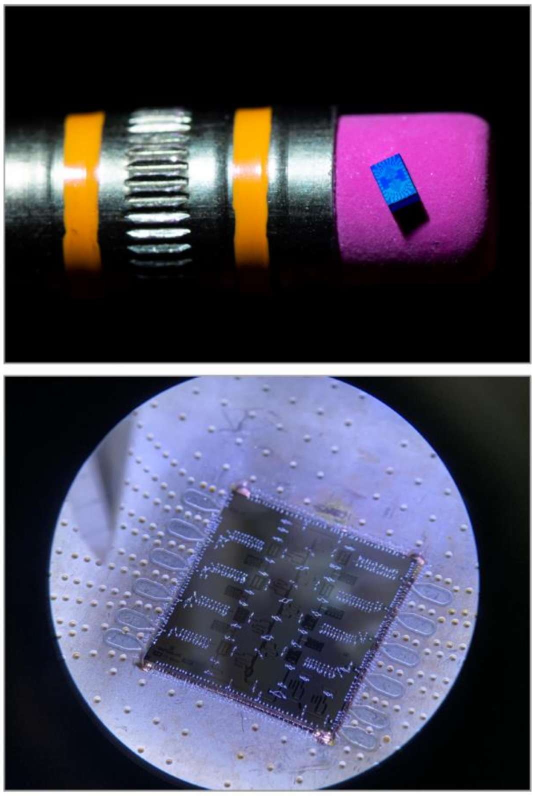
Source: Center for Data Innovation, *Why the United States Needs to Support Near-Term Quantum Computing Applications.* (April 27, 2021), and National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, D.C.: National Academies Press. 2019). | GAO-22-104422

The second method is gate-based quantum computing, which breaks a problem down into a sequence of basic operations, or gates.[27] These gates are similar to logic gates, the building blocks of a classical computer, which perform operations on bits or store bit values. Gate-based quantum computers available in 2021 are *noisy intermediate-scale quantum computers*; they are noisy because they cannot correct errors, and they contain anywhere from 50 to hundreds of physical qubits. Gate-based quantum computers are different from analog quantum computers because of their predicted ability to fully correct errors and break problems down into gate-based operations. Because noisy intermediate-scale quantum computers are limited in the number of qubits they contain

[27]It is unclear if quantum annealing machines will be equivalent to gate-based quantum computers—there are some problems that quantum annealing machines cannot solve.

and are not error-corrected, their computational resources are limited—users can only address certain problems on such systems and must be efficient in doing so.

Figure 3: Examples of qubits



Many different types of qubit technologies are being developed. The top image shows a quantum dot qubit. The bottom image is of a chip containing eight superconducting qubits.

Source: © Intel Corporation (top); Kasra Nowrouzi, Advanced Quantum Testbed, Lawrence Berkeley National Laboratory (bottom). | GAO-22-104422

Future quantum computers may use error correction methods, such as using logical qubits to allow for versatile and error-free quantum computers. Predictions indicate that the number of physical qubits needed for one logical qubit could range from a few hundred to more than 15,000, with the exact number dependent on many factors including the error rate, physical qubit performance, and choice of quantum error correction codes.

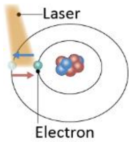
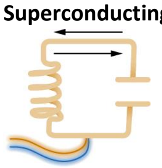
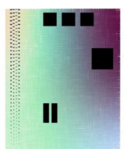
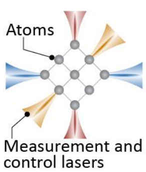
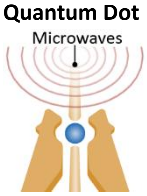
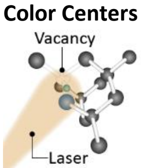
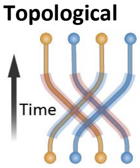
Physical qubits can be divided into two categories: (1) naturally-occurring particles, such as atoms, trapped ions, or photons; and (2) artificial structures, such as superconducting qubits or quantum dots.[28] See figure 3 for examples of qubit technologies.

Naturally-occurring qubits require improvements in engineering to better isolate them from the surrounding environment, and artificial qubits require scientific advances in order to increase the number of qubits in a quantum computer, according to an expert. It is not yet known what type of qubit will power a full-scale quantum computer, and it is too early to focus on the development of one type of qubit or quantum computer, according to the National Academies and others.[29] Table 1 provides information on qubit technologies used to build these computers and how they work.

[28] One expert said color centers and topological qubits were hard to characterize as either a naturally-occurring particle or an artificial structure.

[29] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*; Seth Lloyd and Dirk Englund, *Future Directions of Quantum Information Processing: A Workshop on the Emerging Science and Technology of Quantum Computation, Communication, and Measurement,* Virginia Tech Applied Research Corporation; and G. Popkin, "Scientists are close to building a quantum computer that can beat a conventional one," *Science,* (Dec. 1, 2016).

Table 1: Example qubit technologies used in quantum computers and how they work

Qubit Technology	How it works	Status
Trapped Ion 	Single ions (charged atoms) are trapped in electric fields, or electric and magnetic fields and laser-cooled to near absolute zero, the lowest possible temperature. Trapped ion qubits are manipulated with lasers or microwave pulses.	**Size of demonstration computers:** up to a few dozen noisy qubits. **Entities with platforms available:** IonQ, Honeywell, and Sandia National Laboratory's Quantum Scientific Computing Open User Testbed, among others.
Superconducting 	An artificial atom circuit loop made of superconductors cooled to almost absolute zero. These qubits are controlled with microwave electronics and can operate quickly.	**Size of demonstration computers:** up to dozens of noisy qubits. **Entities with platforms available:** IBM, Rigetti, D-Wave,[a] Google, and Lawrence Berkeley National Laboratory's Advanced Quantum Testbed, among others.
Photonic 	Encodes qubits in light that travels through optical chips or fiber. These qubit systems can operate at room temperature but some may require technologies at near absolute zero temperatures to detect qubits.	**Size of demonstration computers:** up to dozens of noisy qubits. **Entities with platforms available:** Xanadu.
Neutral Atoms 	Neutral, or uncharged, atoms are similar to trapped ions and are controlled by lasers or microwave pulses.	**Size of demonstration computers:** up to dozens of noisy qubits. **Platform availability:** late 2021 or early 2022, according to Cold Quanta.
Quantum Dot 	An artificial atom, similar to a transistor, consisting of a small semiconducting crystal controlled with microwaves or electrical signals. Quantum dot qubits require temperatures of approximately -272 degrees Celsius—one degree above absolute zero—to operate.	**Size of demonstration computers:** a few noisy qubits. **Platform availability:** no plans announced as of June 2021.
Color Centers 	An artificial atom in diamond or another crystal composed of a defect in the crystal often created by an added atom or a vacant space. Color center qubits are controlled with light and optically detected.	**Size of demonstration computers:** up to approximately two dozen qubits. **Platform availability:** no plans announced as of March 2020.
Topological 	Topological qubits may be created by, for example, channeling electrons along the boundary between two different materials. Topological qubits are composed of "quantum braids" in time.	Not yet demonstrated.

Sources: GAO analysis of a National Academies of Sciences, Engineering, and Medicine report, white papers, journal articles, and industry documents, Image Source: From 'Scientists are close to building a quantum computer that can beat a conventional one', G. Popkin, Science, December 1, 2016 (doi:10.1126/science.aal0442). Redrawn and modified with permission from AAAS (all other images). Image courtesy of Oak Ridge National Laboratory, Department of Energy. Carlos Jones, Oak Ridge National Laboratory Photographer (photonic), Dana Anderson, University of Colorado Boulder (neutral atoms) | GAO-22-104422

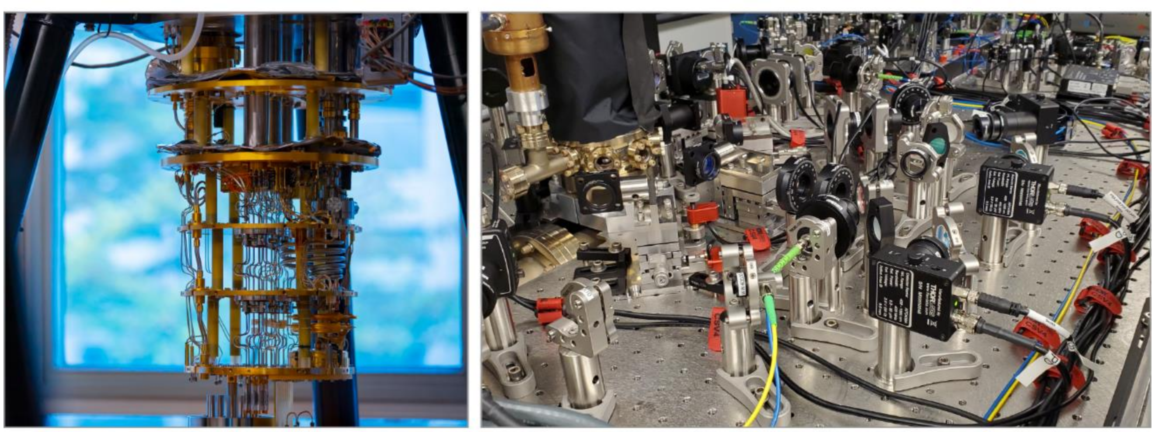
[a]According to D-Wave, their quantum annealing machines may contain more than 5,000 qubits. However, these qubits cannot be directly compared to those in noisy quantum computers.

Companies, national laboratories, and research groups have demonstrated early versions of quantum computers. These demonstrations used different qubit technologies in *quantum computing platforms* (see fig. 4). These platforms are hardware devices on which software can be installed or run. Noisy platforms using trapped ions, photons, or superconducting qubits are available for researchers and the general public to use over the internet, and are generally considered to be the most technologically mature gate-based quantum computing platforms.[30] Other qubit technologies—such as neutral atoms, quantum dot, and color centers in crystals—are not as mature.

Quantum computers contain multiple layers of hardware and rely on multiple classical computers to operate, as follows (see fig. 5):

- **User-interface classical computer.** The user-interface classical computer provides software development tools and services that a user expects from a computer. It runs on a conventional operating system. The user-interface classical computer may provide networking services and storage for applications run on the quantum computer.
- **Control processor.** The control processor classical computer executes the program provided by the user-interface classical computer, which implements the quantum algorithm and instructs the quantum computer on what measurements to perform. In doing so, the control processor identifies and triggers the quantum computer's gate operation sequence, or, for analog quantum computers, it sets up the initial qubit states and triggers the quantum computer's operation.

Figure 4: Examples of quantum computing hardware



Many different types of quantum computers are being developed. The left image shows superconducting quantum computer hardware. The right image shows trapped ion quantum computer hardware.

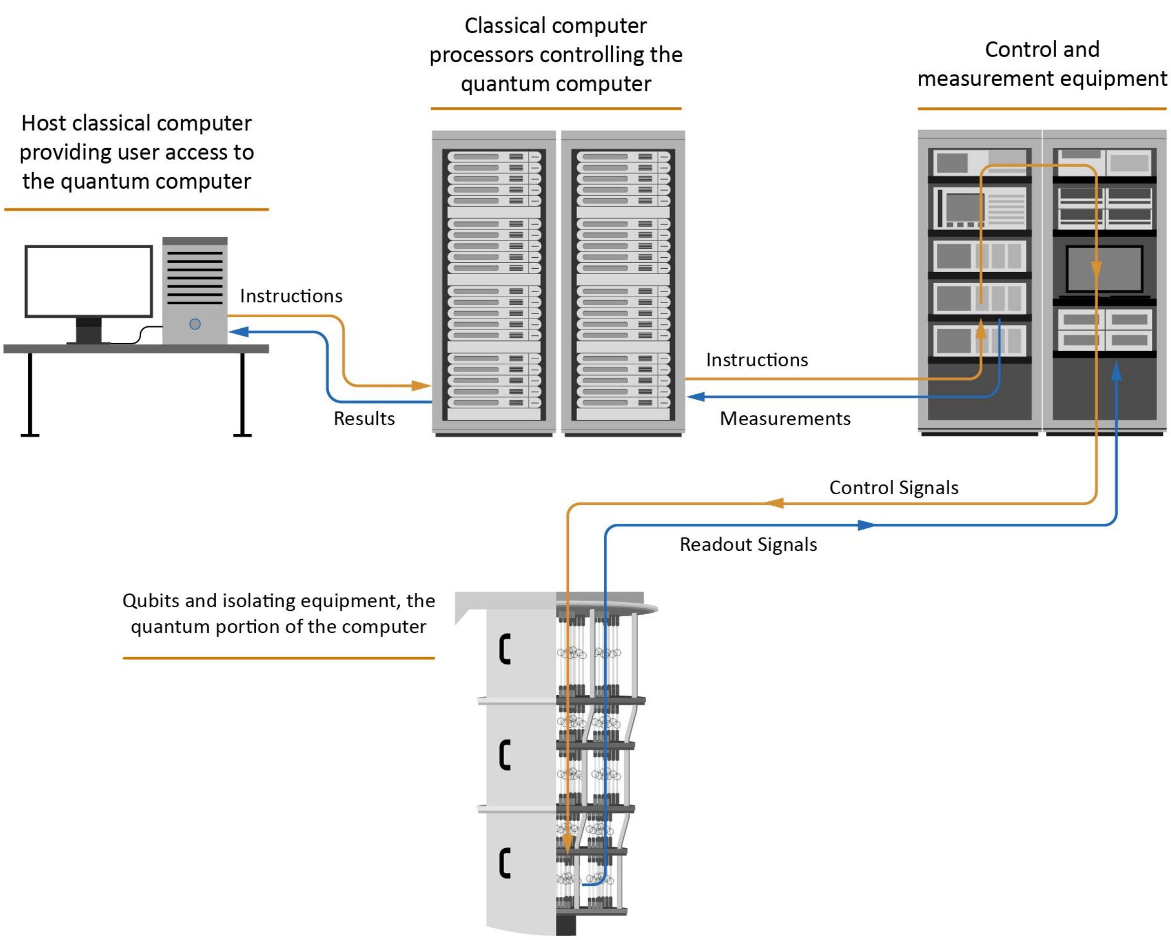
Source: ©Intel Corporation (left photo); Chris Seck, Oak Ridge National Laboratory (right photo). | GAO-22-104422

[30]One company has stated that it has granted access to its noisy demonstration quantum computers to over 140 companies, academic institutions, and national laboratories.

- **Control and measurement equipment.** The control and measurement equipment converts signals from the classical control processor into the signals needed to operate the quantum computer—it sends qubit control signals. Additionally, it converts qubit measurements from the quantum computer into data sent to the classical control processor layer.
- **Qubit and support systems.** The qubit layer contains the qubits and support systems needed to measure qubit output to determine if the qubits are in a 0 or 1 state upon measurement. This is the quantum portion of the computer and includes infrastructure to interpret and apply control signals to selected qubits. On a gate-based quantum computer, this layer performs operations referred to as gate operations on qubits, changing their surrounding environment to achieve a desired transformation. In order to prevent qubit decoherence, this layer must be isolated from its surrounding environment for the duration of a computation.

Similar to classical computers, a functional quantum computer will require extensive software. As with hardware, quantum computers would need several layers of

Figure 5: How a quantum computer works



Source: GAO analysis of a National Academies report and a journal article. | GAO-22-104422 software, programming languages, and algorithms. Early quantum computing software has been developed to support available noisy intermediate-scale quantum computers. Such computers may be especially sensitive to their software's quality and effectiveness because of their limited computational resources; therefore, even small gains in efficiency are important for these computers. While quantum computer programming may require different concepts and operations than classical computer programming, one NASA official and stakeholders pointed out that classical computer programming languages have been used to program some quantum computers by using such programs to prompt specific quantum computer operations. Furthermore, for efficiency, and because of the resource constraints on noisy quantum computers, code tends to be written and optimized for individual platforms and compiled—transformed from code a person can read into code that can be run on a computer—for every task. For example, to perform a chemistry calculation on a quantum computer, a user may need to specifically compile the program for that calculation. In contrast, classical computer programs can run many calculations using the same compiled code.

According to a report by the National Academies, in order to create a useful quantum computer, it will be important to concurrently develop hardware, software, and algorithms through a process called co-design.[31] Co-design could lead to improvements across all aspects of these systems, but could require researchers with a range of expertise, including computer scientists, engineers, and physicists. The National Academies report further states that insight gained from concurrently developing hardware, software, and algorithms helps to drive research forward and increases the chances of successful technology development.

2.1.2 Quantum communications

Quantum communications devices use the properties of quantum physics to transmit and receive information. Three categories are being developed: pre-quantum networks, quantum networks, and the quantum internet.

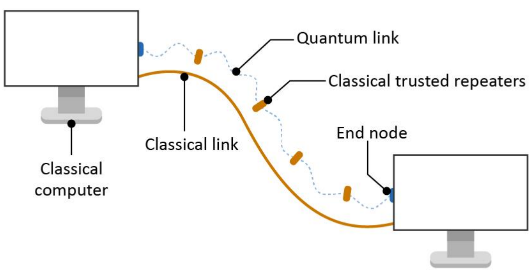
Pre-quantum networks

Pre-quantum networks let users send, receive, and measure quantum states (see fig. 6). One pre-quantum network application is quantum key distribution, in which two parties create an encryption key using the properties of quantum physics.[32]

[31] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*. In classical computing, co-design is the design cycle in which application performance is improved with respect to some metric, such as performance, by using software design to inform hardware design, and hardware design to inform software design.

[32] Once the key is established, users can send encrypted information over the classical internet.

Figure 6: Illustration of a pre-quantum network



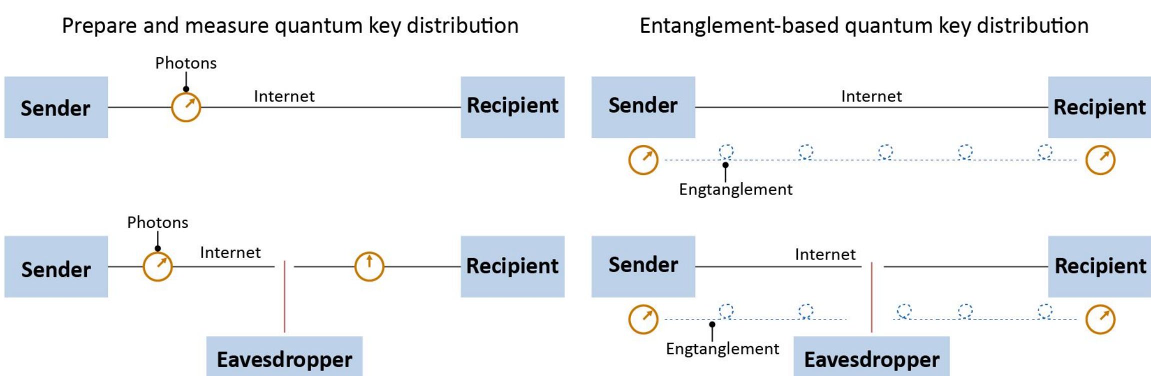
Source: Júlia Fort Muñoz for TU Delft. | GAO-22-104422

Quantum key distribution can securely deploy cryptographic keys without direct physical contact between two parties. It can be performed using two methods: (1) *prepare and measure*, which does not use entanglement; and (2) *entanglement-based quantum key distribution* (see fig. 7).[33] In "prepare and measure" quantum key distribution, the sender prepares and sends photons as a secret key. In doing so, a secret key is exchanged, because if an eavesdropper measures the photons being prepared and sent, the prepared photons are changed in a manner that the sender or receiver can detect, alerting them that the key has been compromised. In entanglement-based quantum key distribution, the sender and receiver establish an entangled photon pair that holds the quantum information necessary to generate a secret key.

Optical fiber may become ineffective for quantum key distribution at distances over approximately 60 miles, so a longer fiber optic quantum key distribution system would need specialized hardware to decode the quantum signal and re-encode a new quantum signal for the next leg of the system. Such systems are not fully secure because this hardware could be compromised and undetectably reveal the keys it receives and transmits during the decoding and re-encoding process. Alternatively, satellites might transmit quantum keys over distances greater than approximately 60 miles without the use of trusted repeater technologies.

Pre-quantum networks, such as those involving quantum key distribution systems, have been demonstrated and, according to experts, may be the first step in creating true quantum networks (see below). Some

Figure 7: Prepare and measure and entanglement-based quantum key distribution systems



Source: Júlia Fort Muñoz for TU Delft. | GAO-22-104422

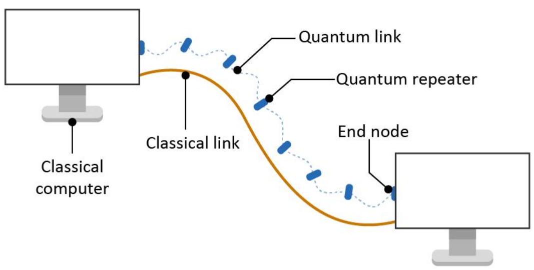
[33]Bennett and Brassard, "Quantum Cryptography," pp. 175-179, and Eckert, "Quantum Cryptography Based on Bell's Theorem," pp. 661-663.

quantum key distribution systems are available for purchase, but they are limited in range based on fiber optic constraints. Countries such as Japan and China have pre-quantum networks that perform quantum key distribution.

Quantum networks

The second category of quantum communications technologies is quantum networks (see fig. 8).

Figure 8: Illustration of a quantum network



Source: Júlia Fort Muñoz for TU Delft. | GAO-22-104422

Future quantum networks would allow for direct communication between two parties by creating entangled quantum states that are shared between the parties, a feature that is not possible in a pre-quantum network.[34] Future quantum networks would distribute entanglement between users as an essential network function and entanglement would likely be produced in multiple quantum network protocols.[35] Quantum networks are in the early stages of development (see fig. 9), and a three-node quantum network has been demonstrated.[36] Quantum networks may require *quantum repeaters*, which would re-transmit quantum information to overcome signal degradation, allowing networks to extend over large distances. However, NASA officials said satellites may be required to send quantum information over distances larger than a few hundred miles. Further, according to a National Science and Technology Council report, satellite-based systems for space-based quantum links may be critical components for the development of more sophisticated quantum networks.[37] They may also require: transducers to change the type of signal used from telecommunications frequencies to those used by quantum computers, memory to store a previously generated quantum link while establishing a second link, and developed network architectures to structure the flow of information. All of these technologies have either been conceptualized or are in the early stages of development.

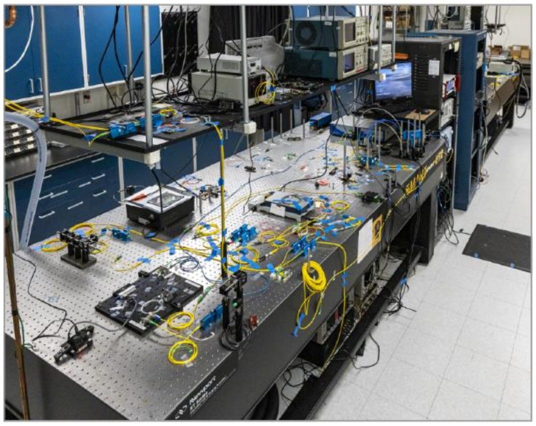
[34]DOD officials noted that the creation of entangled states may also be used to extend the communications range.

[35]In networking, a protocol is a set of rules for formatting and processing data among network users. Network protocols enable communications between different computers on network that may use vastly different software and hardware.

[36]A node is a connection point inside a network that can receive, send, create, or store data. In classical networking, a node requires some form of identification in order to access the network. Classical technology examples of nodes include computers, printers, and modems.

[37]National Science and Technology Council, Subcommittee on Quantum Information Science, *A Coordinated Approach to Quantum Networking Research* (January 2021).

Figure 9: A quantum network development laboratory



Source: Image courtesy of Oak Ridge National Laboratory (ORNL), Department of Energy. Carlos Jones, ORNL Photographer. | GAO-22-104422

Quantum networks will not exist in isolation from classical networks, but will rely on them for tasks such as exchanging control information, which coordinates network operations. In order to support quantum technology development, the existing classical communications infrastructure may need to be upgraded or new infrastructure built. Future quantum networks will require a new quantum-updated network stack with multiple hardware layers, including one layer for creating entanglement between quantum nodes and one for transporting qubits in coexistence with classical networks. Quantum networks will likely supplement, rather than supplant, classical networks.

The quantum internet

The third category of quantum communications technologies is the *quantum internet.* The future quantum internet is a concept describing an advanced quantum network where quantum communications platforms connect many quantum devices—such as quantum computers—globally. The quantum internet could fully integrate classical and quantum networking technologies; employ quantum error correction; and require quantum repeaters, transducers, and memories—devices or systems that could store a quantum state for long periods of time. It has not yet been developed and will require significant hardware improvements. For example, a fully functional quantum internet will require advancing enabling technologies such as quantum entanglement sources (i.e., physical processes that create quantum-entangled states between two or more qubits), detectors, and quantum memories. While the quantum internet would connect quantum devices, it would not replace the classical internet.

2.2 Quantum technology costs and time to maturity

2.2.1 Quantum computing

A full-scale quantum computer is many years away. As of 2021, quantum computers are noisy intermediate-scale and, according to some potential end users, are not suitable for solving real-world problems. The next step would likely be fault-tolerant quantum computers, which are resilient against errors that occur when a quantum computer performs a calculation and are designed to directly implement algorithms developed for ideal quantum computers. The final step would likely be full-scale quantum computers, which would mitigate any system noise, including unintended qubit or environmental interactions, and could scale to hold thousands of logical qubits.

Companies and academics have demonstrated experimental, noisy-intermediate scale quantum computers that are designed to answer specific demonstration questions faster than a classical computer. Quantum computers developed in the next 3 to 5 years will likely be larger, noisy intermediate-scale platforms (see fig. 10). According to NASA officials, as such platforms develop, noise would decrease and error correction would increase.

Figure 10: A noisy intermediate-scale quantum computing facility

Source: Connie Zhou for IBM. | GAO-22-104422

However, there is some uncertainty as to how long it may take to develop fault-tolerant quantum computers. Some experts indicated noisy intermediate-scale quantum computers would be built for the next 5 to 10 years and others indicated that the first fault-tolerant quantum computers would be developed in the next few years.

Estimates of the time and costs to develop and build a prototype full-scale quantum computer are very uncertain and range widely. The following summarizes these estimates in three categories:

- **At least a decade.** Some agency officials, DOE laboratory officials, and stakeholders said developing and building a prototype full-scale quantum computer could take a decade and cost at least $1 billion. One stakeholder said developing a full-scale quantum computer in 10 years would require a Manhattan Project-type effort, while development through a more incremental, market-driven approach would take at least 15 years. This stakeholder estimated research and development would cost over $1 billion and that building the full-scale quantum computer would cost an additional $1 billion.[38] Existing computer and microelectronics technologies could facilitate quantum computer development, but this would take at least 10 years, according to one expert.
- **Decades.** Some agency officials, DOE laboratory officials, and stakeholders said it could take decades and cost billions to develop a full-scale quantum computer. One stakeholder said a government investment of approximately $10 billion could be required.
- **Could not be determined or development uncertain.** Some agency officials, DOE laboratory officials, and a stakeholder said they could not determine the cost and time frames necessary. Further, some DOE officials were uncertain that a useable, full-scale, error corrected quantum computer could ever be developed.

2.2.2 Quantum communications

As with quantum computing, estimates provided by agency officials, stakeholders,

[38] This estimate, according to this stakeholder, does not include quantum computer operating costs.

and experts for the time and costs to develop quantum communications technologies are very uncertain. The following summarizes the range of their estimates:

- **Prototype technology development in the next decade.** City-sized prototype networks could be developed in the next 5 to 10 years at a cost of $50 to $100 million, according to an expert and DOE laboratory officials, and systems extending beyond a 100-mile radius could be possible in a decade. Quantum communications technologies that are demonstrated in the next 5 years may be foundational technologies that enable quantum networks, such as quantum transducers, repeaters, and memories, and space-based entanglement distribution systems could start development. However, such time frames are uncertain and additional time would be required to mature these technologies for commercial use.
- **Developing a quantum internet could take decades.** Developing a quantum internet could take decades. According to DOD officials, DOE laboratory officials, and a stakeholder, quantum internet technology development could take decades and cost at least $1 billion. However, such estimates are uncertain. For example, DOD officials said demonstrations of very immature quantum communications technologies leading to a quantum internet could be 10 to 15 years away.
- **Could not be determined.** Some DOD officials, stakeholders, and one expert said further research would be needed before determining development costs and time frames.

2.2.3 Further technology development is needed

Technology development roadmaps

Companies, agencies, and stakeholders have published quantum technology development roadmaps, which describe how development may proceed. Companies envision gradually scaling up quantum computer size, with one company reporting plans to build a prototype 1 million physical qubit quantum computer by 2030 that, according to one stakeholder, would require a $2 billion to $3 billion investment and 1,000 doctoral-level scientists and engineers. Another company has announced plans to build a 1,000-plus physical qubit device by the end of 2023. In the areas of quantum communications, roadmaps indicate it will take at least a decade to develop a preliminary long-distance entanglement-based network, and longer to mature the technology. According to one expert, one of the biggest quantum communications technology development cost drivers is the cost of fabricating quantum components—there is no dedicated foundry that supports scalable quantum component development.[39]

[39]Another expert noted that a quantum fabrication facility could cost over $10 billion, similar to the cost of a leading edge transistor fabrication facility. However, according to a third expert, photonic qubits may not require a dedicated foundry—such systems may be manufactured at existing facilities.

Research and development efforts

Several kinds of research and development efforts are needed to mature quantum computing and communications technologies. Fully developing quantum technologies will require significant improvements to existing technologies along with research to develop new technologies. For example, the ability to package hardware that fits on large laboratory tables into a smaller form that can be manufactured and built into deployable devices must be developed. Research could lead to progress in next generation materials development with increased noise resilience, which could support efforts to build stable, compact, and low-cost quantum devices with practical deployment potential. Research could lead to more uniform qubits, increased qubit coherence time, and better-isolated qubits from the surrounding environment. Developing a quantum computer for more computationally intensive uses will also require significant improvements to existing technologies. Quantum technologies depend on classical technologies to operate and research is ongoing to integrate quantum and classical technologies.

Full-scale quantum computers will likely require a million, or more, physical qubits, requiring an increase in the physical system size and complexity to accommodate the necessary qubits. For example, NIST officials said that supporting technologies—such as dilution refrigerators that could support a large system containing 1 million physical qubits, lasers, and cryogenic systems—would be needed to meet the goal of a full-scale quantum computer.[40] One stakeholder said foundries do not yet produce qubits at a level expected for an industrial research and development system—qubit fabrication investments will be needed in order to advance the technologies. Another stakeholder said constructing a qubit costs about $10,000, and will continue to cost this much unless there is a significant breakthrough in qubit fabrication. Qubits are fragile and error prone; successfully using qubits for applications will require a high level of sophistication and control, and error free quantum computing requires quantum error correction.

Deriving full benefits from a quantum computer also requires continued work on algorithms, programming languages, and software. Research is ongoing to develop quantum algorithms that could better enable noisy-intermediate scale quantum computers to provide an advantage over classical computers.

Quantum communications technologies also require technology development. In order to fully function, such technologies will require the development of transducers and repeaters as well as network algorithms and protocols. Challenges connecting different parts of a quantum network while maintaining entanglement across the network will increase as the system size increases. Long-range communications networks will rely on establishing, distributing, and maintaining entanglement across thousands of kilometers. Both quantum computing and

[40]Dilution refrigerators and cryogenic equipment are part of the equipment that is used to cool some qubit technologies to near absolute zero temperatures. Dilution refrigerators available in 2019 could support a quantum computer containing approximately 1,000 physical qubits. Lasers can be used to "cool" atoms and ions and hold them in place.

communications technologies need research in quantum memory and supporting technologies.

2.3 Quantum computing and communications technologies may develop together

Quantum computing and communications technology developments are interconnected because they are based on the same quantum physics properties and share common hardware and laboratory techniques. Because of this, it is not always easy to distinguish boundaries between the technologies. Developments in one quantum technology are mutually dependent on developments in another and qubits being developed will be useful for quantum computing and communications applications such as performing calculations, memory storage, or information transmission. For example, in future quantum computers, trapped-ion qubits could be used to perform calculations, with the results converted to photonic qubits for transmission to another qubit technology that would be used as a qubit memory. Each different qubit technology has its own advantages and challenges that may make it suitable for specific quantum computing or communications applications.

3 Quantum Technologies Could Enable a Range of Applications

While quantum computing and quantum communications have the potential to be transformative, they are in the early stages of development. Some of the possible applications are known, and there may be additional applications yet to be discovered. Quantum computers could solve some problems that are intractable on a classical computer in areas such as chemistry simulations, optimization solutions, artificial intelligence and machine learning, large number factoring, and fundamental science. Quantum communications technologies could enhance secure communications and connect quantum devices, including quantum computers. However, there are potential drawbacks to quantum technology implementation and use, including complexity, cost, and energy consumption.

3.1 Quantum computers may eventually solve some intractable problems

Quantum computers are theorized to outperform classical computers for some critical problems such as simulating certain chemical interactions and factoring large numbers into their prime components, a task that underpins certain security protocols. Quantum computers could find applications in agriculture, energy, finance, pharmaceuticals, supply chains, and security, but it is unclear where they will have the largest effect. Quantum computing could introduce calculation techniques that enhance drug design research, aerospace engineering, and financial portfolio management. Further, some quantum computing applications have underlying computational similarities—they may use the same underlying algorithms, many of which operate by using the same key steps and protocols.

While a quantum computer can perform all the same computations as a classical computer, classical computers are a better option when a quantum advantage does not exist. In order for a quantum computer to show an overall advantage, it needs to offer a significant improvement over a classical computer and be economically feasible. Further, quantum computers will need to provide a significant improvement over classical computers before they are adopted, according to potential end users. The amount of improvement a quantum computer may need to provide to prove economically significant, varies by the potential end user's application and business needs. For example, one potential end user said it would be worth investing tens of millions of dollars for a two percent increase of accuracy in chemistry simulations at the early stages of drug development, while another potential end user said a 10 to 15 percent increase in chemical simulation efficiency would be useful.

The number of physical qubits needed for a quantum computer to provide a significant improvement over a classical computer is expected to vary by the application. For example, platforms with 100 physical qubits can solve small chemical calculations and may provide an advantage for some optimization problems. Quantum computers with 1,000 physical qubits could enhance machine learning and optimization problems. Factoring large numbers or simulating fertilizer or pharmaceutical molecules may require more than 1 million physical qubits (see fig. 11).

It is not clear when quantum computers will outperform classical computers for such applications, according to potential end users. One expert said that quantum computers could have commercial value once they are fault-tolerant and can perform chemistry simulations.[41]

Figure 11: Size of quantum computer needed for different quantum computing applications

Increasing cost and complexity

Physical qubits[a]	Potential applications	Sectors with potential interest	Limitations
<1,000 qubits	• Calculations for small chemicals (H_2, LiH, BeH_2) require less than 100 qubits • Test quality of quantum hardware requires less than 100 qubits • Test theories about black holes • Quantum assisted optimization	Quantum computing companies Academia Research institutions	• May not be useful for end users • Unclear how much advantage is obtained for optimization
1,000 – 100,000	• Enhance machine learning • Enhance optimization problems • Test quality of quantum hardware • Finance simulations	Finance	• Unclear advantage for machine learning • Unclear how much advantage is obtained for optimization
100,000+	• Simulate critical fertilizer components • Chemistry for energy applications • Chemistry for pharmaceutical applications • Break some forms of encryption • Simulate crystals and metals • Simulate superconductivity • Grover's search algorithm	Pharmaceutical Energy Agriculture Security	• Limits to calculations • Unclear advantage for search algorithms • Post quantum cryptography prevents quantum attacks

Source: GAO analysis of government documents, journal articles, National Academies of Sciences, Engineering, and Medicine report, and interviews with agency officials and potential end users. | GAO-22-104422

[a]Some documents reported the number of logical qubits, a group of physical qubits that mimics a robust single stable qubit. If the number of physical qubits was not provided, we multiplied the number by 1,000 to obtain an estimated number of physical qubits. Estimates of the ratio of logical qubits to physical qubits include 1 to 300, 1,000, 10,000, and higher. As qubits improve, the number of physical qubits needed for some applications may decrease.

[41]Qubits are sensitive to their environment and can accumulate errors. A fault-tolerant quantum computer is resilient to errors accumulated by individual qubits. Using error correction techniques it may be possible to have a quantum computer that mitigates errors on individual qubits.

According to a report by the National Academies, chemistry simulations may be the application where quantum computers have the most effect.[42]

Potential end users explained that quantum computers will augment, rather than replace, classical computing. Experts and agency officials said that unknown quantum computing applications may be developed; as quantum computers advance, users will develop new ways to use them.

The following describes five areas where quantum computing applications may prove useful.

3.1.1 Optimization

Optimization problems involve finding the best decision or action with respect to minimizing or maximizing a goal or objective. Algorithms have been proposed that would run on a quantum computer to improve investment strategies for financial portfolios; minimize supply chain costs and resources; and find the best locations for solar, wind, or hydroelectric power plants in order to meet energy needs. However, the advantage quantum computers would have over a classical computer is unclear for optimization. An expert and a potential end user said, for certain tasks, like finance, a small improvement in a quantum computer's solution over a classical solution could be beneficial to users. Quantum computers with as few as 50 to 100 high-quality qubits may begin to provide an advantage over a classical computer for optimization problems.

3.1.2 Artificial intelligence and machine learning

Quantum computers may shorten the time needed to run a machine learning algorithm and solve machine learning problems that are intractable on a classical computer.[43] The resulting improvements could include better disease detection through enhanced searching of genetic data, and more accurate credit scores through enhanced pattern recognition. Potential noisy-intermediate scale quantum computing applications are being studied. However, experts, agency officials, and stakeholders disagree on the extent of the effect. While some said that quantum computers provide an advantage for artificial intelligence and machine learning, others said an advantage is unclear. Other stakeholders said that it is challenging for quantum computers to process large amounts of data, which is often needed for machine learning. In order to circumvent some of these challenges, quantum computers may solve part of a calculation while a classical computer solves the rest; however, this may require

[42] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.

[43] Artificial intelligence technologies seek to allow computers to mimic human thinking and problem solving. Early attempts used computers programmed with expert-provided rules or criteria to address a problem. A sub-field of artificial intelligence, machine learning, enables computers to use large quantities of data to develop rules and criteria themselves in order to address a problem. GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care,* GAO-21-7SP (Washington, D.C.: Nov. 30, 2020).

developing software and protocols to efficiently distribute a problem between quantum and classical computers.

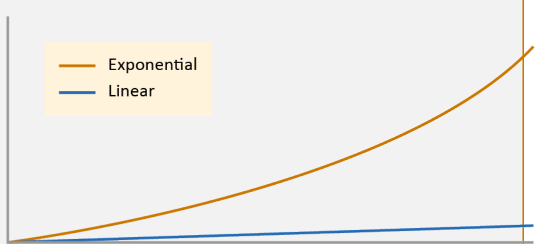
3.1.3 Factoring large numbers

Quantum computers are theorized to factor numbers in exponentially fewer steps than a classical computer (see text box).

Exponential

An exponential change is expressed by a variable in an exponent of a mathematical equation. Exponential growth is rapid (see figure below). When discussing computational complexity, exponential can also be used to mean a problem that grows faster than a polynomial, even if the growth is not a true exponential.

Comparison of linear and exponential growth



Source: GAO. | GAO-22-104422

Source: GAO analysis of textbooks and agency document | GAO-22-104422

Factoring a number involves finding the unique set of prime numbers that can be multiplied together to produce that number. For very large numbers, this problem is intractable on a classical computer. Some forms of encryption, such as the Rivest-Shamir-Adleman algorithm, commonly called RSA, rely on this fact. These encryption methods would be vulnerable if a quantum computer could, as theorized, efficiently factor large numbers.[44] For RSA encryption, this feat may require more than a million physical qubits, in order to implement error correction techniques to make the quantum computer fault-tolerant. However, some forms of encryption are predicted to be resistant to an attack by a quantum computer.[45] Post quantum cryptography is an area of research developing such encryption (see text box).

3.1.4 Chemistry

Quantum computers may be able to simulate critical chemical processes that are infeasible on a classical computer. The resulting knowledge of how various materials and compounds behave could lead to improvements in batteries, fertilizers, and pharmaceuticals. According to potential end users, better chemical simulations may also reduce the time needed to create a drug or other valuable

Post quantum cryptography

Post quantum cryptography—also called quantum-resistant cryptography—is a classical cryptographic system that is secure against decryption attempts using either quantum or classical computers. Such systems can work in conjunction with existing communications protocols and networks. The National Institute of Standards and Technology (NIST) is developing post quantum cryptography standards and has a program to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms.

Source: GAO analysis of NIST documents | GAO-22-104422

[44]Because internet encryption uses a combination of techniques, some of which rely on the difficulty in factoring large numbers, internet security may be compromised by quantum computers. One expert explained that bulk data are encrypted differently such that they are not vulnerable to quantum computers in the same way.

[45]NIST is developing post quantum cryptography encryption standards. As of June 7, 2021, NIST aims to release draft standards in 2022-2023 and finalized standards by 2024.

compound. Small chemistry simulations—such as simulations of a hydrogen molecule—have been demonstrated on quantum computers, but these simulations are already done on a classical computer. According to DOD officials, quantum computers have not yet performed chemistry simulations of commercial interest.

Chemistry simulations allow scientists to understand experimental results and system properties. If a simulation is accurate enough, it may be able to predict the results of an experiment without having to perform the experiment. A specific type of chemistry calculation critical to understanding reactions is calculating the energy of molecular orbitals—areas around a molecule where an electron could be located. It is challenging for classical computers to calculate orbitals because, while accuracy improves as more orbitals are added to the simulation, the problem size also grows exponentially. For example, according to a peer-reviewed journal article, the largest classical computer calculation studied a molecule of four chromium atoms that had 24 orbitals.[46] The article predicts the full calculation for the chromium molecule would take 116 days using 8,196 classical processors. Molecules of interest to industry are often larger and more complex. In comparison, a single quantum computer with over a million qubits and sufficiently low error rates may be able to simulate a more complicated molecule in 5 to 130 days.[47] Classical computers can simulate larger molecules using approximation methods, which can result in significant error.

Quantum computers may supplement, rather than replace, classical computer chemistry simulations. While a quantum computer may be able to solve more complicated chemistry problems, it still has limitations on the size of problems it can solve. Many drugs would need simulations of more than 200 orbitals for an accurate calculation of the entire molecule. A hybrid approach would allow a highly accurate simulation of the critical part of a large molecule on a quantum computer and a less accurate simulation for the rest of the molecule on a classical computer.

Quantum computers will not be able to solve all chemistry problems. A quantum computer's potential effect on the chemical and pharmaceutical industries is unclear because the necessary steps of creating and testing chemicals, such as a vaccine or drug, are often more time consuming than simulating the chemical, according to a stakeholder.

3.1.5 Fundamental science

Quantum computing may provide new or more efficient ways to test physics theories, potentially leading to a better

[46] K. D. Vogiatzis, D. Ma, J. Olsen, L. Gagliardi, and W. A. De Jong, "Pushing configuration-interaction to the limit: Towards massively parallel MCSCF calculations," *The Journal of Chemical Physics* vol. 147, (2017): p. 184111.

[47] In this example, it could be possible to simulate 54 orbitals of the iron molybdenum cofactor, a critical molecule for fertilizer production. M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, "Elucidating reaction mechanisms on quantum computers," *Proceedings of the National Academy of Sciences* vol. 114, no. 29 (2017): pp. 7555-7560.

understanding of the universe. For example, using a quantum computer to conduct fundamental science research may help further the understanding of quantum gravity or black holes, because quantum physics underpins these topics. Further, quantum computers may have applications analyzing data from high energy physics experiments.

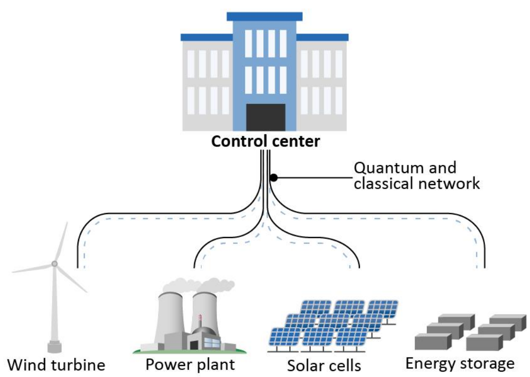
3.2 Quantum communications could enhance security, sensing, and computing

Quantum communications technologies—which exchange quantum information—could support other quantum technologies, such as quantum computers and sensors, and provide new information security protocols. Quantum communications applications could include enhanced techniques for astronomy, connecting quantum computers, and blind quantum computing. Quantum communications could introduce new protocols to improve applications including GPS and more accurate clocks.

As discussed in section 2.1.2, quantum communications includes the following three technologies:

- **Pre-quantum networks.** Pre-quantum networks may enable quantum secure communications protocols, such as quantum key distribution. Such security could affect businesses and government operations in a range of sectors, including national security, elections, finance, energy delivery, and health services. For example, quantum communications security protocols could secure the power grid by protecting data sent between a control center, energy sources, and energy users to control power generation, storage, and energy dispatch (see fig. 12).[48] It is unclear how much of an advantage a quantum secure communications line provides over classical cryptography because classical encryption schemes are often sufficient and uncertainties remain about the security of a quantum communications system.[49]

Figure 12: Secured communications over a power grid



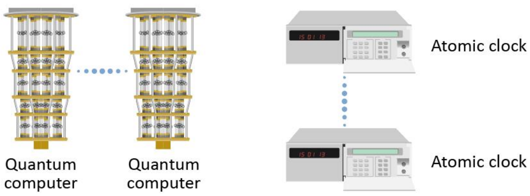
Source: GAO analysis of expert comments and peer-reviewed articles. | GAO-22-104422

[48] Z. Tang, P. Zhang, W. O. Krawec, and Z. Jiang, "Programmable Quantum Networked Microgrids," *IEEE Transactions on Quantum Engineering* 1 (September 16, 2020), and P. Y. Kong. "A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security," *IEEE Systems Journal* (September 9, 2020).

[49] The National Security Agency has released a frequently asked question document on quantum computing and post-quantum cryptography which includes information on quantum key distribution and quantum cryptography. National Security Agency, *Frequently Asked Questions: Quantum Computing and Post-Quantum Cryptography*, PP-21-1120 (Aug. 2021).

- **Quantum network**. Quantum communications could create a network of quantum devices such as computers, sensors, and others, in order to improve device performance. Quantum networks could connect atomic clocks, resulting in more precise timing (see fig. 13).

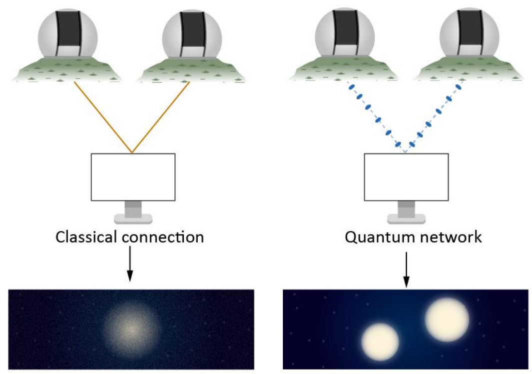
Figure 13: Potential implementations of local quantum networks



Source: GAO analysis of government documents, peer-reviewed journals, and interview with agency officials. | GAO-22-104422

Furthermore, a quantum network could connect quantum sensors, which would theoretically have better sensitivity than classical sensors. The resulting sensor network could lead to improvements in telescopes, environmental sensors, and sensors used in health care. In astronomy, such networks could enable more precise imaging of stars and planets (see fig. 14) and support future experiments in particle and gravitational physics. Quantum networking experiments conducted in 2020 relied on devices with limited functionality and performance.

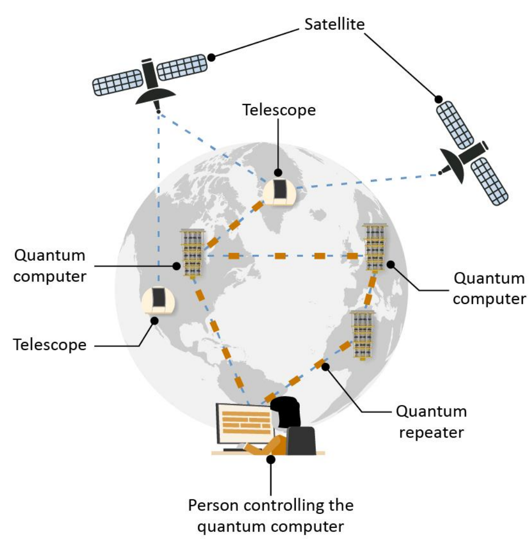
Figure 14: Quantum communications could lead to improved telescopes



Source: GAO analysis of professional society publications. | GAO-22-104422

- **Quantum internet.** The quantum internet is envisioned as an advanced global quantum network (see fig. 15). An expert explained that the quantum internet could provide some additional capabilities such as enhanced network security, but it will not, for example, increase data rates. Quantum communications technologies will not create instantaneous communications.

Figure 15: Potential implementations of the quantum internet

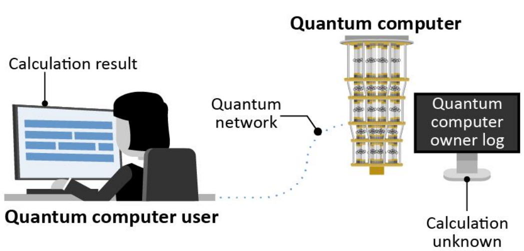


Source: GAO analysis of a government document and peer-reviewed journals. | GAO-22-104422

3.3 Some applications will require both computing and communications technologies

Blind quantum computing is one application that requires both advanced quantum computing and communications technologies (see fig. 16). It allows users to perform calculations on a quantum computer owned by someone else, yet keeps their data inputs, quantum computations, and outputs private.[50] To use blind quantum computing, a remote user would connect to a quantum computer using quantum communications. This would require a non-trivial interface between the quantum computer's qubits and the qubits used for quantum communications.

Figure 16: Blind quantum computing



Source: GAO analysis of textbook and peer reviewed article. | GAO-22-104422

Some laboratories have demonstrated blind quantum computing on a small scale. However, blind quantum computing that is accessible from long distances and able to perform any quantum algorithm will require both an advanced quantum computer and an advanced quantum network.

A second application that requires both quantum computing and communications technologies is distributed quantum computing. This application could allow users to run larger and more complex calculations by networking quantum computers together, effectively increasing the quantum computer's size. A quantum network would connect quantum computers by entangling qubits in those computers with one another. To accomplish this, distributed quantum computing may require devices known as interconnects, which might transfer quantum information between different types qubits.[51] Early quantum computers may be specialized for specific applications, according to NASA officials, so distributed quantum computing could help solve complex problems by connecting quantum computers with different specialties.

In addition to the applications listed, quantum computing and communications technologies could be a source of random number generation (see text box).

Quantum random number generation

Quantum technologies may offer a source of truly random numbers. Random number generation is used in many technologies, including cryptography, scientific computing, gaming, and lotteries. Having a true random number generator is important with simulations that are sensitive to subtle patterns, such as certain biological simulations, or with security applications that depend on numbers being unpredictable.

Source: GAO analysis of peer-reviewed articles and a Science and Technology Policy Institute report. | GAO-22-104422

[50]Some information cannot be hidden from the quantum computer's owner, such as how many resources a quantum computer commits to a calculation.

[51]Interconnects are devices which allow for the transfer of information between two types of technologies such as such as fiber optic cable and semiconductors.

3.4 Quantum technology drawbacks

Quantum technologies may have drawbacks, including the following:

- **High cost and complexity.** A potential end user and DOD officials noted quantum technologies may have prohibitively high costs and complexity, and from an industry perspective, there is no clear return on investment. Because quantum computers may be specialized for specific problems, according to a potential end user, the cost savings from the increased speed and accuracy provided by a quantum computer may be diminished by the need to switch between quantum computer types. It is important to determine the benefit a user will receive, since users may not adopt a technology that provides a small, but expensive, benefit, according to DOD officials and a potential end user.
- **Understanding results.** End users described difficulties with understanding the results from a quantum computer, because a quantum computer processes information differently than a classical computer. It may be possible to incorrectly interpret the results of a quantum computer, according to one potential end user, and another potential end user explained it is unclear how to certify quantum computer calculations.
- **Energy consumption.** An expert and potential end user expressed concern about quantum technology's energy consumption. Some quantum devices require specialized cooling equipment and temperatures near absolute zero. However, because some calculations are classically intractable, meaning the energy resources needed grow exponentially compared to the problem input size, a quantum computer could still solve some of these calculations with significantly fewer resources.
- **Information transmission rates.** Stakeholders explained that the slow information transmission rate limits the amount of information a quantum computer can process.
- **Malicious use of quantum computers.** Bad actors could use quantum computers maliciously to, for example, decrypt protected information or misuse sensitive data.
- **Jamming.** Quantum communications technologies may be more susceptible to jamming than classical communications technologies.

Some of these drawbacks also exist in classical computing, and potential end users said there were no inherent drawbacks to using a quantum computer, as long as it is economically feasible for the intended applications. A potential end user explained there are no inherent drawbacks because quantum computers are a tool to provide new computational capabilities. According to another potential end user, if a quantum computer works, choosing to use a quantum computer is a simple cost-benefit decision.

4 Factors Affecting Quantum Technologies and Policy Options to Address Them

4.1 Several factors affect the development and use of quantum technologies

Drawing on information from experts, stakeholders, and literature, we identified several factors that affect the development and use of quantum technologies, including collaboration, workforce size and skill, investment, and the supply chain. These factors affect government, academia, and industry involved in quantum technology development.

4.1.1 Collaboration

The amount of collaboration among multiple scientific disciplines, sectors, and with international partners can affect quantum technology development. While there are ongoing efforts to sustain collaboration—such as the 2018 National Quantum Initiative Act which intends to promote collaboration among the government, laboratories, industry, and universities—stakeholders commented on the need for more collaboration across different scientific disciplines such as materials science, physics, and engineering; without such collaboration, it may be difficult to make quantum computing breakthroughs. According to a National Science and Technology Council report, quantum technology research has mostly occurred within existing institutional boundaries, such as within individual university departments, and continued efforts to collaborate across institutions are needed to accelerate progress.[52] Further, one expert noted that quantum technology development efforts between academia, industry, and government can be isolated. Without collaboration, it may be challenging to identify key applications.

Experts also noted the need to support quantum technology development through international collaboration. For example, agency officials told us international collaboration is needed because no country has the resources to develop quantum technologies alone. A lack of international collaboration could cause the United States to lose its quantum computing advantage if U.S. developers do not leverage the skills of leading talent in other countries, according to one stakeholder. While experts noted the need for international collaboration, they also described how such collaboration may be challenging because of export controls, such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR).[53] Experts

[52]National Science and Technology Council, Interagency Working Group on Quantum Information Science, *Advancing Quantum Information Science: National Challenges and Opportunities*, (Washington, D.C.: July 2016).

[53]The Department of State is responsible for the export and import of defense articles and services pursuant to Section 38 of the Arms Export Control Act, as amended, 22 U.S.C. §2778, and Executive Order 13637. The ITAR, found at 22 C.F.R. parts 120-130, implement the Arms Export Control Act. The EAR, found at 15 C.F.R. part 730 et. seq., are issued by the United States Department of Commerce, Bureau of Industry and Security. The Export Control Reform Act of 2018 was enacted as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, and is the principal legal authority for the Export Administration

told us these controls could make it challenging for quantum technology developers to discuss their work across national lines.

4.1.2 Workforce

According to experts, agency officials, and other stakeholders, the United States needs to develop a strong quantum workforce in order to maintain its leadership position in quantum technology hardware and software development. They added that the U.S. educational system does not equip enough graduates with the right skills to undertake complex tasks required for quantum technology development. As a result, there are more quantum technology jobs than people to fill them. Further, one stakeholder said training in the production of superconducting circuits is much less supported in the United States than in other countries. Quantum technology workers will need varied levels of higher education, although stakeholders said there are also opportunities to train programmers and technicians who did not attend college.

One particular challenge employers may face when expanding their quantum workforce is hiring foreign quantum technology talent. For example, stakeholders told us visa requirements can hamper hiring efforts. However, these requirements exist for foreign policy and national security reasons. Additionally, for reasons of national security, export controls may require an entity to obtain an export license in order to release certain information to foreign nationals, including foreign national employees.[54] For example, under the EAR, deemed exports—any release in the United States of a controlled technology or source code to a foreign person—may require an export license which may complicate employing talent from other countries. While experts said there may be missed opportunities to hire leading talent in quantum technologies if employers restrict their talent pool to the United States, these controls also address a legitimate national security risk. For example, we previously reported that there is a risk foreign students and scholars will "export" sensitive knowledge they gain to their home countries.[55] Export controls implemented by the U.S. government mitigate this risk.

4.1.3 Investment

Because of quantum technology's long development time frames, sustained investment is particularly important to advance the technologies. We previously reported that long-term investment is important to better support technology development across multiple stages of

Regulations. See Pub. L. No. 115-232, Title XVII, Subtitle B, August 13, 2018, codified at 50 U.S.C. § 4801 et seq.

[54]For example, under the EAR, any release in the United States of covered technology or source code to a foreign person is deemed an export to the foreign person's most recent country of citizenship or permanent residency. Similarly, under ITAR, any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

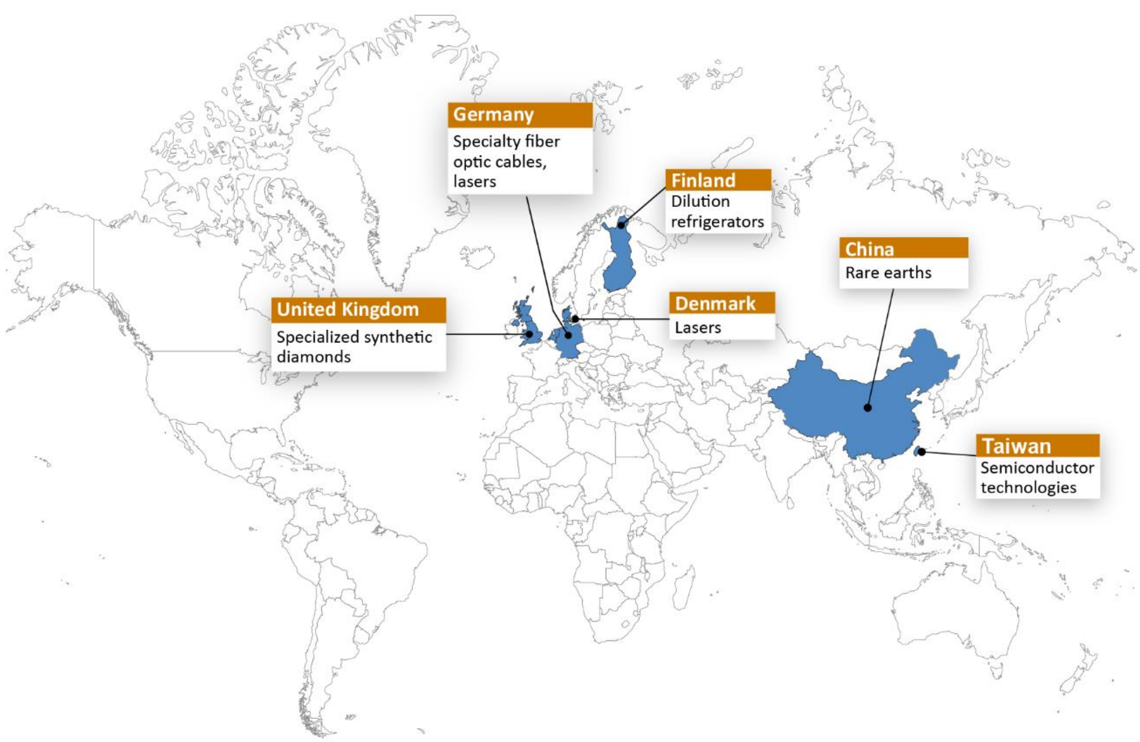
[55]GAO, *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues,* GAO-20-394 (Washington, D.C.: May 12, 2020*).* We also previously found that U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest. GAO, *Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence,* GAO-21-130 (Washington, D.C.: Dec. 17, 2020).

innovation, such as design, building, and testing.[56] However, quantum technology investors may be more likely to be focused on profit from short-term technology and application development. Talent may leave industry and academia because of insufficient funding, and little progress may be made.[57] One stakeholder said funding fluctuations may make it difficult to maintain institutional knowledge, and NSF officials said waning interest in the field or declining funding could negatively affect technological progress. Several other nations have made large investments in quantum technologies, so continued U.S. support is critical if the United States wants to maintain its leadership, according to a National Academies report.[58] DOE laboratory officials said funding for basic research and early development activities is particularly important because the ultimate path forward for quantum technologies is uncertain.

4.1.4 Supply chain

The quantum technology supply chain is global and specialized. For select examples of some component parts supplied from outside of the United States, see fig. 17. As

Figure 17: Select examples of certain quantum technology component parts supplied from outside the United States



Source: GAO analysis of public information. | GAO-22-104422

[56] GAO-18-656.

[57] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.

[58] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.

noted below, the quantum supply chain includes potential *single points of failure* and may be located in other countries, which could interrupt or disrupt development if certain supporting technologies are unavailable.[59] For example, one type of dilution refrigerator is only available from Finland, which represents a potential single point of failure. According to experts, dilution refrigerators are part of a small industry, and necessary to maintain the low temperatures quantum technologies require. Additionally, specialized synthetic diamonds needed for certain quantum technologies are only made by one company in the United Kingdom. Further, one expert noted the potential for such companies to be purchased by companies from countries such as China.

We previously reported that the continued availability of rare earth elements may be at risk and subject to supply and pricing changes by China.[60] China accounted for 80 percent of U.S. imports of rare earth elements between 2016 and 2019. China previously adopted domestic production quotas and restricted exports of rare earth elements, which caused a spike in prices.

One expert said developers need access to certain supporting technologies such as microwave and radio frequency electronics that are required to control and measure superconducting qubits at cryogenic temperatures, but such components are not commercially available and the quantum market is not large enough to develop specialized components. Experts said it would be helpful for some supporting technologies that are a part of the quantum supply chain to be more scalable, deployable, and affordable for developers.

According to a 2018 White House report, one of the biggest hurdles to quantum technology development is a lack of suitable and reliable components and equipment.[61] Examples include specialized lasers, high-quality optical fibers, cryogenic components, and rare and critical materials such as helium-3. Such components can be expensive, according to stakeholders. For example, dilution refrigerators require helium-3, an expensive gas in limited supply, to maintain low temperatures.[62]

Additionally, quantum communications technologies may require large-scale infrastructure projects, such as new or updated satellites, and updated optical communications infrastructure. For example, one stakeholder said the quantum internet cannot be operated on existing fiber networks and hardware, and will

[59]A single point of failure represents part of a system that, if it fails, causes the entire system to fail.

[60]GAO, *Rare Earth Materials in the Defense Supply Chain*, GAO-10-617R (Washington, D.C.: Apr. 14, 2010).

[61]National Science and Technology Council, *National Strategic Overview for Quantum Information Science.*

[62]According to two users of helium-3 we spoke to, helium-3 can cost approximately $3,000 to $4,000 per liter on the open market, although researchers with a government contract can buy it for $600 per liter. We reported on a domestic shortage of helium-3 in 2011 when the United States government was developing its response. See GAO, *Managing Critical Isotopes: Weaknesses in DOE's Management of Helium-3 Delayed the Federal Response to a Critical Supply Shortage,* GAO-11-472 (Washington, D.C.: May 12, 2011).

require new infrastructure projects to transmit quantum information over long distances. Specifically, end-to-end hardware and quantum repeaters will need an entirely new and massive national infrastructure project if the quantum internet is to be widely adopted. According to NSF officials, building quantum repeaters is a complex engineering challenge and remains an open area of research. A full quantum network would require tens of thousands of quantum repeaters, according to DOE laboratory officials—approximately 100 quantum repeaters would be needed to transmit information from Chicago to New York City.

The qubit manufacturing process is another area in need of supply chain advances. More advanced quantum technologies, such as full-scale quantum computers, may contain more than a million physical qubits; several experts described the need for qubit foundries to manufacture qubits at the scale required for quantum technology development and use. According to one stakeholder, such foundries are not yet at the point where materials can be made reliably and consistently, and yields are not yet at a level expected from an industrial research and development platform. However, one expert said there has been little effort by many quantum technology researchers to interact with leading semiconductor foundries. Foundries make money by producing a large quantity of an item and a small number of wafers are needed to support quantum technology research; therefore, there is little incentive to prioritize research over larger-scale projects, according to this expert.

4.2 Several policy options may help address factors affecting the development and use of quantum technologies

We developed policy options that policymakers—legislative bodies, government agencies, standards-setting organizations, industry, and other groups—could consider taking to help address the four key factors above, and to enhance benefits or mitigate drawbacks that affect quantum technology development and use. This is not an exhaustive list of policy options. We intend for these options to provide policymakers with a broader base of information for decision-making. The options are neither recommendations to federal agencies nor matters for congressional consideration.

4.2.1 Encourage collaboration

Policymakers could encourage further collaboration in developing quantum technologies.

Potential implementation approaches

- Encourage collaboration among researchers in different scientific disciplines, such as physics, materials science, and mechanical engineering.
- Consider strengthening collaboration among different sectors, such as government, academia, the private sector, hardware providers, and potential quantum technology end users.

- Consider increasing international collaboration between the U.S. and other countries leading in quantum technology development.

Opportunities

Collaboration among researchers from different disciplines could enable technology breakthroughs. For example, materials science, chemistry, and condensed matter physics researchers could collaborate, leveraging knowledge and tools to improve materials used in quantum devices.[63] Further, multidisciplinary teams can help translate technologies from the laboratory, such as turning a proof-of-principle entanglement demonstration into a robust, scalable platform useful in a real-world quantum network.[64]

Partnerships among different sectors can accelerate research and development and can facilitate technology transfer from a research setting to the private sector, federal agencies, and others. One expert said quantum technology development is often disconnected from real-world applications, and increased interactions between developers and potential end users could lead to the discovery of key applications where quantum technology has a major effect. Collaboration among hardware developers and experts in other fields could also enable potential end users to use quantum technologies to enhance their work, according to agency officials, DOE laboratory officials, and stakeholders. Further, agency officials described how such collaborations could provide hardware developers with feedback on how hardware performs when used for real-world applications.

International collaboration in developing quantum technologies could bring mutual benefits to the United States and other countries. There is a precedent of over 20 years of international cooperation in quantum information technologies; such efforts have helped accelerate scientific discovery while also promoting economic growth and national security.[65] International quantum technology collaborations could bring benefits including sharing resources and expertise, as well as growing the marketplace for quantum technologies.[66]

Considerations

Collaboration may be challenging because researchers and companies may be concerned with protecting their intellectual property. For example, companies may want to maintain leadership in quantum technology development and decide to not publish research results, which could reduce the flow of ideas to other researchers, according to a National

[63] National Quantum Coordination Office, *Quantum Frontiers, Report on Community Input to the Nation's Strategy for Quantum Information Science,* October 2020.

[64] National Science and Technology Council, *Advancing Quantum Information Science: National Challenges and Opportunities*.

[65] National Science and Technology Council, *National Strategic Overview for Quantum Information Science.*

[66] National Science and Technology Council, Subcommittee on Quantum Information Science, *National Quantum Initiative Supplement to the President's FY 2021 Budget*, 2020.

Academies report.[67] DOE laboratory officials told us that, when working on collaborative projects, quantum researchers may be concerned with protecting their intellectual property against those who sponsor the research because results could be communicated to potential competitors. As such, stakeholders underscored the need to balance intellectual property protection with the need to encourage successful collaboration.

Institutional differences could make collaboration difficult. Efforts such as defining and articulating a common outcome, developing common terminology, establishing compatible policies and procedures, and fostering open lines of communications may help different quantum technology groups collaborate.[68]

As we previously discussed, export controls applicable to quantum technologies may complicate disclosure of aspects of a technology's development across national lines. In particular, quantum cryptography, post quantum cryptography algorithms, helium-based refrigeration, synthetic diamond material, and certain materials growth and fabrication techniques, are listed on the Commerce Control List covered under the EAR.[69] However, export controls manage national security risks associated with exporting sensitive items while ensuring that legitimate trade can still occur.[70]

One additional consideration for international collaboration is foreign influence on U.S. research. We previously reported on such concerns.[71] A 2018 "Dear Colleague" letter sent from the National Institutes of Health to over 10,000 universities described concerns that foreign government talent recruitment programs can influence researchers receiving federal funding to divert intellectual property and federally funded research to other countries.

4.2.2 Expand the quantum technology workforce

Policymakers could consider ways to expand the quantum technology workforce.

Potential implementation approaches

- Leverage and enhance existing programs.
- Create new programs, such as special multidisciplinary research tracks or undergraduate programs.

[67] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*.

[68] GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

[69] The EAR contains a list called the Commerce Control List which is comprised of ten broad categories including telecommunications and information security, computers, and materials processing. Each category is then divided into five functional groups, including software, and technology. The Commerce Control List is not an exhaustive list of things that are within the scope of EAR.

[70] GAO-20-394.

[71] GAO, *Federal Research: NIH Should Take Further Action to Address Foreign Influence*, GAO-21-523T (Washington, D.C.: Apr. 22, 2021).

- Create pre-college programs for early exposure to quantum concepts.
- Promote job training, such as cross-training from other sectors and industry or public sector training programs.
- Consider policies to facilitate appropriate hiring of international students and researchers who are deemed not to pose a risk to national security.

Opportunities

Education could provide students and personnel with the qualifications and skills needed to work in quantum technologies across the private sector, government, or academia. Experts and DOE laboratory officials told us the quantum technology workforce would require a broad education base representing many disciplines and levels of training.

Some existing programs provide opportunities for students or postdoctoral scholars to learn skills that are necessary for the quantum workforce. For example, NSF has several programs aimed at supporting multidisciplinary workforce development, including a joint industry-academia graduate training program called the Quantum Information Science and Engineering Network, a Quantum Science Summer School to train graduate students and postdoctoral scholars in quantum science, and a Graduate Research Fellowship Program. Similarly, NIST joint research centers provide opportunities for students and postdoctoral scholars to learn from NIST researchers. DOE laboratories also offer internships aimed at providing hands-on quantum technology training to students, officials told us.

New programs could provide graduates with the appropriate skillsets for quantum technology jobs. Experts and DOE officials said universities are developing new quantum information science courses, but further work remains. DOD officials said that, in order to improve the quantum workforce, it is necessary to develop new quantum engineering and quantum information science curricula. Such curricula should include quantum engineering, circuit design, logic, and algorithm development, among other topics, DOD officials said.

Training personnel from different disciplines in quantum technologies could enhance quantum talent. DOE laboratory officials said an alternative to recruiting external talent would be for an organization to cross-train its employees and that a national laboratory setting provides an advantage when cross-training employees because researchers from different disciplines who could potentially learn quantum concepts are available.

Companies could use international hiring to grow the quantum workforce, stakeholders told us. One stakeholder said international hiring could allow U.S. quantum employers to attract and retain international top talent. Retaining international talent could also benefit the economy. According to the National Academies, international students who remain in the United States after earning their degrees contributed to an increase of more than $29 billion to the economy in 2016.[72]

Considerations

According to DOE laboratory officials, efforts to increase the quantum computing workforce may affect the number of personnel in other high-demand technology fields. According to a 2019 testimony to Congress by the President of the National Academy of Sciences, U.S. born students are not entering science, technology, engineering, and mathematics fields in sufficient numbers. One stakeholder commented that related technology fields, such as machine learning, also experience a shortage of skilled personnel.

It may be difficult to adequately develop workforce plans to accommodate quantum technology needs. We previously reported that, to successfully implement their missions, agencies need to identify current skills gaps, future workforce needs, and select the right human capital strategies to address them.[73] The quantum workforce's size and scope may not be well understood until the technologies are further developed.

International hiring may be challenging because of visa requirements and export controls. One expert said some members of their workforce who are not U.S. citizens have had difficulty extending their visas, while conducting breakthrough work. As previously discussed, visa requirements exist for foreign policy and national security reasons. Further, one expert expressed concern that ITAR and EAR have previously made hiring foreign talent challenging. Notably, several experts described deemed exports as a challenge to working with international employees, because of potential issues around discussing controlled information with non-U.S. persons on a project. However, as previously discussed, export controls address a legitimate national security risk. Additionally, there may be challenges hiring recently graduated international students in the United States. For example, we previously reported the U.S. may be at risk of missing out on global transformational technological advances because of limited efforts to attract and retain talent.[74] Further, foreign applications and enrollment in graduate education have shown recent declines.[75]

4.2.3 Incentivize or support investment

Policymakers could consider ways to incentivize or support continued investment in quantum technology development.

Potential implementation approaches

- Consider investments that are targeted toward specific results, such as quantum technology testbeds.

[72]Written statement issued by the witness Marcia K. McNutt, President, National Academy of Sciences, Engineering, and Medicine, *Maintaining U.S. Leadership in Science and Technology,* testimony before the House Committee on Science, Space, and Technology, 116th Cong., 1st sess, Mar. 6, 2019.

[73]GAO, *Science and Technology: Strengthening and Sustaining the Federal Science and Technology Workforce,* GAO-21-461T (Washington, D.C.: Mar. 17, 2021).

[74]GAO-18-656.

[75]McNutt, *Maintaining U.S. Leadership in Science and Technology*.

- Continue investment in quantum technology research centers.
- Support grand challenges, in which organizations ask the public to submit solutions to a specific goal or problem and reward the winners.

Opportunities

Investments targeted towards specific results could help advance quantum technologies, according to experts. They identified several areas of need, including improved access to quantum computers, a focus on real-world applications, and software development tools. One example is targeted investments in quantum technology testbed facilities, which could support technology development. Quantum testbeds are unique facilities that bridge the gap between academic research and physical resources like hardware. According to DOE laboratory officials, testbeds allow researchers to explore device functionality, a step that supports quantum technology development. Moreover, testbeds can help encourage transparency as precompetitive technologies are developed, establish a common quantum technology vocabulary, develop and refine interface and other relevant standards, define performance metrics and benchmarks to allow users to compare different devices, and provide hands-on courses to train users in quantum technologies.

Grand challenges have shown success in accelerating technology development and could be leveraged for quantum technologies. One example is a grand challenge related to autonomous vehicle development in 2004 and 2005 hosted by the Defense Advanced Research Projects Agency, in which five teams successfully navigated their autonomous vehicles through 132 miles of desert terrain. One expert commented that a series of challenges could be valuable, possibly targeting certain milestones in quantum technology development. Another said grand challenges de-risk investment in quantum technologies because the host agrees to purchase a solution for their intended use case.

Considerations

It may be difficult to fund projects with longer-term project time frames. Specifically, while experts cited a need for sustained investments because of long development time frames, they also discussed the inherent uncertainty that such investments will be able to sustain quantum technology development until commercial applications are developed and other funding sources established.[76] We previously reported that adopting best practices such as grouping technology development activities into two portfolios, incremental and disruptive, can improve innovation investments and management.[77] Such approaches may be considered to

[76]We previously reported that, because of long time frames associated with technology development, there can be a gap in funding and investment support that makes it challenging to translate research into commercialized products or services. GAO-18-656.

[77]Incremental development improves product lines, whereas disruptive development is for riskier innovative, and potentially transformational, technologies. GAO, *Defense Science and Technology: Adopting Best Practices Can Improve Innovation Investments and Management*, GAO-17-499 (Washington, D.C.: June 29, 2017).

mitigate financial risk associated with disruptive technology development.

One broad consideration for investments is a lack of standards, which could affect quantum technology investments. Standards help to benchmark the performance of quantum technologies, according to one expert. Standards also help define the properties and functions of products and signal when technologies work as expected.[78] In the absence of standards to benchmark the performance of quantum technologies, businesses and consumers may not be confident that products will work as expected. However, developing standards too early may deter the growth of alternative technology pathways or lock development into existing pathways. According to stakeholders, quantum technology standards remain an open area of discussion.

4.2.4 Encourage the development of a robust, secure supply chain

Policymakers could encourage the development of a robust, secure supply chain for quantum technologies.

Potential implementation approaches

- Enhance efforts to identify supply chain needs and gaps.
- Expand quantum technology fabrication capabilities.
- Create additional quantum foundries to develop quantum-based technologies.

Opportunities

A robust supply chain could help mitigate quantum technology development risks by expanding access to necessary components and materials or by providing improved economies of scale. It could also help quantum developers who require access to certain electronics that are not available commercially and are instead made in-house or assembled using parts intended for a different purpose, according to an expert. DOE laboratory officials said a reliable supply chain would be helpful because it is difficult for a single laboratory to scale up their fabrication to produce millions or billions of components that work reliably.

Improvements in the quantum material fabrication capabilities could ensure that a reliable supply of materials is available to support quantum technology development. According to one report, development and deployment of quantum technologies will be contingent on the ability to reliably produce novel quantum materials.[79] Fundamental improvements in fabrication tools and techniques will be required to produce these new materials and the quantum technologies that incorporate them at scale. One stakeholder underscored the importance of fabricating

[78]GAO, *National Institute of Standards and Technology: Additional Review and Coordination Could Help Meet Measurement Service Needs and Strengthen Standards Activities*, GAO-18-445 (Washington, D.C.: July 26, 2018).

[79]National Science and Technology Council, *Advancing Quantum Information Science: National Challenges and Opportunities*.

qubits reliably and in the quantities needed for full-scale quantum computers.

Quantum foundries could help support scalable manufacturing of the component parts needed for quantum technology development. According to NSF, quantum foundries can help develop materials needed to enable quantum technologies, train the quantum workforce, and accelerate quantum technology development.

Considerations

There are general risks posed by a global supply chain. It is difficult to obtain a complete understanding of a component's source and potential vulnerabilities. We previously reported that dependence on a global supply chain can significantly limit visibility into, understanding of, and control over how technologies are developed, distributed, and deployed.[80] For example, federal agencies that rely extensively on information and communications technology (e.g., computing systems, software, and networks), a field related to quantum technology, to carry out their operations face numerous supply chain risks. Such risks include threats posed by counterfeiters who may exploit vulnerabilities in the supply chain, compromising the confidentiality, integrity, or availability of an organization's systems and the information they contain. Similar risks and may need to be taken into consideration for the quantum technology supply chain.

Some critical components such as rare earths—the basis of some quantum devices—have supply chain risks that may be difficult to mitigate. Mining operations are primarily outside the United States, which may pose risks to continued mineral availability.[81] Further, although they are relatively abundant overall, rare earths occur in low concentrations in the ground and are difficult and costly to mine. Alternative options for obtaining rare earths, such as recovery from batteries, permanent magnets, and fluorescent lamps, are available in limited quantities.

According to one stakeholder, quantum foundries take a long time to develop and can be costly. They include special tooling and processing technology, which can cost millions of dollars because of low demand, according to the same stakeholder. Further, one expert explained that because of the variety of approaches for constructing qubits, including superconducting, quantum dot, trapped ion, and photonic qubits, a variety of fabrication capabilities are needed. According to this expert, this variety adds to cost and risk when investing in expensive equipment and facilities.

[80]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-21-171 (Washington, D.C.: Dec 15, 2020).

[81]GAO, *Rare Earth Materials: Developing a Comprehensive Approach Could Help DOD Better Manage National Security Risks in the Supply Chain*, GAO-16-161 (Washington, D.C.: Feb. 11, 2016).

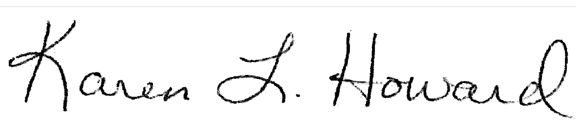
5 Agency and Expert Comments

We provided a draft of this product to Department of Defense, Department of Energy, Intelligence Advanced Research Projects Activity, National Aeronautics and Space Administration, National Institute of Standards and Technology, National Science Foundation, and Office of Science and Technology Policy with a request for technical comments. The Department of Defense, Department of Energy, Intelligence Advanced Research Projects Activity, National Aeronautics and Space Administration, National Institute of Standards and Technology, and Office of Science and Technology Policy provided us with technical comments, which we incorporated as appropriate.

We invited the participants from our meeting of experts to review our draft report. Of the experts, 10 agreed to receive the draft for review and technical comment, and we incorporated comments as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretaries of Defense, Energy, and Commerce; the National Aeronautics and Space Administration Administrator, and the Directors of National Intelligence, the National Science Foundation, the Office of Science and Technology Policy, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at 202-512-6888 or HowardK@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made contributions to this report are listed in Appendix IV.



Karen L. Howard, PhD
Director
Science, Technology Assessment, and Analytics

List of Addressees

The Honorable Jack Reed
Chairman
The Honorable James Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Eddie Bernice Johnson
Chairwoman
The Honorable Frank Lucas
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Maggie Hassan
United States Senate

The Honorable John Thune
United States Senate

The Honorable Anna G. Eshoo
House of Representatives

The Honorable Bill Foster
House of Representatives

Appendix I: Objectives, Scope, and Methodology

We prepared this report under the authority of the Comptroller General to assist Congress with its oversight responsibilities, in light of broad congressional interest and the crosscutting nature of quantum computing and communications technologies. We examined (1) the availability of quantum computing and communications technologies and how they work, (2) potential future applications of such technologies and the potential benefits and drawbacks from their development and use, and (3) factors that could affect technology development and the policy options available to help address those factors, enhance benefits, or mitigate drawbacks.

To conduct our work across all three objectives, we interviewed officials from the Department of Defense, Department of Energy, Intelligence Advanced Research Projects Activity, National Aeronautics and Space Administration, National Institute of Standards and Technology, National Science Foundation, and Office of Science and Technology Policy. We also interviewed a non-generalizable sample of stakeholders from academia, industry, and trade groups. Our interviews focused on quantum computing and communications activities, technology uses, potential future applications, and the potential benefits, drawbacks, and considerations related to developing such technologies. We selected stakeholders with expertise in quantum computing or communications technologies, understanding of potential applications, their effects, or expertise in factors relevant to quantum information technology development and adoption, a review of relevant documents, and through snowball sampling.

We also interviewed potential end users about plans to use a quantum computer and the technology's benefits and drawbacks. We selected a non-generalizable sample of six potential end users from multiple sectors including the pharmaceutical and finance sectors, based on continued company interest in quantum computing, press releases or published articles, collaborations with quantum computing companies, and being a potential end user not directly involved with a quantum computer's creation.

We reviewed documents identified by agencies, experts, and GAO. To gain insights into quantum computing and communications technology maturity, their applications, potential benefits and drawbacks of their usage, and policy options, we reviewed agency documents, peer-reviewed literature, and white papers, and reviewed literature from the years 2010 to 2020 identified by a GAO librarian. We selected the most relevant literature for further review based on our objectives.

We collaborated with the National Academies of Sciences, Engineering, and Medicine (National Academies) to convene a one-and-a-half day meeting of experts from academia, government, and industry. We invited experts with assistance from the National Academies—based on expertise in quantum computing, quantum communications, quantum applications, and expertise in the economic, social, or legal implications of quantum computing and communications technologies—to obtain a range of perspectives on the maturity of quantum computing and communications technologies, challenges, factors that could affect technology development and use, applications, and policy options. See Appendix II for a list of experts who participated in our meeting. We asked the experts who attended our meeting to identify any potential conflicts of interest, and we found the group of experts, as a whole, had no inappropriate biases. While this meeting was planned and convened with the assistance of the National Academies, all final decisions regarding meeting substance and expert participation were GAO's responsibility. At their request, experts received a draft of our report for review and technical comment, which we incorporated as appropriate.

For objective 3, in addition to the steps above, we conducted policy and legal literature searches to determine policy options that are available to help address factors that could affect the development and use of quantum computing and communications technologies. We conducted a two-person literature review from the years 2010 to 2020 and selected the most relevant articles for further review.

We intend policy options to provide policymakers with a broader base of information for decision-making.[82] The options are neither recommendations to federal agencies nor matters for congressional consideration and are not listed in any specific rank or order. We present four policy options in response to the factors identified during our work and discuss potential opportunities and considerations of each. While we present options to address the major factors we identified, the options are not inclusive of all potential policy options. The policy options and analyses were supported by the above evidence. Policy ideas, identified from the evidence above, were adapted into policy options by combining similar ideas that were duplicative, could be grouped into a higher-level policy option, were examples of how to implement a policy option, or did not fit into our scope. We grouped the remaining ideas based on themes (e.g., collaboration).

We conducted our work from July 2020 to October 2021 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

[82] Policymakers is a broad term including, for example, Congress, elected officials, federal agencies, state and local governments, academic and research institutions, and industry.

Appendix II: Expert Meeting Participation

We collaborated with the National Academies of Science, Engineering, and Medicine to convene a one-and-a-half-day meeting of experts to inform our work on quantum computing and communications technologies. The meeting was held virtually on January 11-14, 2021. Experts who participated in this meeting are listed below. Experts provided additional assistance throughout our work, including providing materials for our review, images for inclusion in the report, answering technical questions, reviewing our draft report for accuracy, and providing technical comments.

Andrew Childs
Professor and Co-Director
University of Maryland, and Joint Center for Quantum Information and Computer Science

Jim Clarke
Director of Quantum Hardware
Intel Corporation

Chip Elliott
Chief Technology Officer (Retired)
BBN Technologies

Eden Figueroa
Associate Professor
Stony Brook University

Jay Gambetta
IBM Fellow and Vice President of Quantum Computing
IBM T.J. Watson Research Center

Barbara Goldstein
Associate Director, Physical Measurement Laboratory
National Institute of Standards and Technology

Saikat Guha
Associate Professor
University of Arizona
Director
NSF Center for Quantum Networks

Brian LaMacchia
Distinguished Engineer
Microsoft

Matt Langione
Principal
Boston Consulting Group

Debbie Leung
Professor and University Research Chair
Institute for Quantum Computing, University of Waterloo

John Martinis
Professor
University of California, Santa Barbara and Silicon Quantum Computing

Celia Merzbacher
Executive Director
Quantum Economic Development Consortium

Christopher Monroe

Gilhuly Family Presidential Distinguished Professor, ECE and Physics Department, Duke University

Chief Scientist,

IonQ, Inc.

Alejandro Perdomo-Ortiz

Associate Director of Quantum AI

Zapata Computing

Josh Richman

Chief Revenue Officer

Psi Quantum

Simone Severini

Professor of Physics of Information

University College London

Director, Quantum Computing

Amazon Web Services

Krysta Svore

General Manager

Microsoft

Jake Taylor

Technology and Public Purpose Fellow

Harvard

Appendix III: Selected Definitions

Some common quantum information technology terms include:

- **Decoherence.** The exchange of energy and information from a qubit to the environment. Decoherence results in the irreversible loss of quantum information.
- **Entanglement**. Qubits can be connected such that acting upon one qubit, such as a measurement, can reveal information about the other qubits it is connected to.
- **Logical qubit**. A group of physical qubits that mimics a robust single stable qubit.
- **Observable state.** A state capable of being measured. The superposition in a qubit is between two observable states, and a measurement reveals the value of one of these states.
- **Quantum coherence time.** The amount of time that a qubit maintains a superposition state, which limits the time during which a qubit can do an operation for computing or communications applications.
- **Qubit (or quantum bit).** The fundamental hardware component of quantum technologies. Qubits maintain quantum properties for extended periods of time. They can be constructed from photons, trapped ions, neutral atoms, superconducting circuits, quantum dots, and color centers in crystals.
- **Superposition**. A state where a qubit exists simultaneously in any combination of all possible observable states. Measurement collapses the qubit to be in a single state.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO contact

Karen L. Howard, PhD, (202) 512-6888 or howardk@gao.gov

Staff acknowledgments

In addition to the contacts named above, R. Scott Fletcher (Assistant Director), Charlotte E. Hinkle (Analyst-in-Charge), Claire McLellan, and Britney Tsao made key contributions to this report. Jenny Chanley, Leia Dickerson, April Gillens, Anika McMillon, Amy Pereira, Ben Shouse, Andrew Stavisky, Hai Tran, Walter Vance, and Jack Wang also contributed to this report.

(104422)

Related GAO Products

GAO, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS*, GAO-21-320SP (Washington, D.C.: May 10, 2021).

GAO, *Defense Science and Technology: Opportunities to Better Integrate Industry Independent Research and Development into DOD Planning*, GAO-20-578 (Washington, D.C.: Sept. 3, 2020).

GAO, *Science & Tech Spotlight: Quantum Technologies,* GAO-20-527SP (Washington, D.C.: May 28, 2020).

GAO, *Defense Supplier Base: Challenges and Policy Considerations Regarding Offshoring and Foreign Investment Risks,* GAO-19-516 (Washington, D.C.: Sept. 5, 2019).

GAO, *National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies,* GAO-19-204SP (Washington, D.C.: Dec. 13, 2018).

GAO, *Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas,* GAO-18-656 (Washington, D.C.: Sept. 26, 2018).

GAO, *2018-2023 Strategic Plan: Trends Affecting Government and Society,* GAO-18-396SP (Washington, D.C.: Feb. 22, 2018).

GAO, *Defense Science and Technology: Adopting Best Practices Can Improve Innovation Investments and Management,* GAO-17-499 (Washington, D.C.: June 29, 2017).

GAO, *Electronic Waste: DOD Is Recovering Materials, but Several Factors May Hinder Near-Term Expansion of These Efforts,* GAO-16-576 (Washington, D.C.: June 20, 2016).

GAO, *Rare Earth Materials: Developing a Comprehensive Approach Could Help DOD Better Manage National Security Risks in the Supply Chain*, GAO-16-161 (Washington, D.C.: Feb. 11, 2016).

GAO, *Helium Program: BLM's Implementation of the Helium Stewardship Act of 2013,* GAO-14-751T (Washington, D.C.: July 15, 2014).

GAO, *Helium Program: Urgent Issues Facing BLM's Storage and Sale of Helium Reserves,* GAO-13-351T (Washington, D.C.: Feb. 14, 2013).

GAO, *Neutron Detectors: Alternatives to Using Helium-3,* GAO-11-753 (Washington, D.C.: Sept. 29, 2011).

GAO, *Managing Critical Isotopes: Weaknesses in DOE's Management of Helium-3 Delayed the Federal Response to a Critical Supply Shortage,* GAO-11-472 (Washington, D.C.: May 12, 2011).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact: Website: https://www.gao.gov/fraudnet/fraudnet.htm
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, YoungC1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

Stephen Sanford, Managing Director, spel@gao.gov, (202) 512-9715
U.S. Government Accountability Office, 441 G Street NW, Room 7B37N, Washington, DC 20548