GAO | Science, Technology Assessment, and Analytics

SCIENCE & TECH SPOTLIGHT:

QUANTUM TECHNOLOGIES

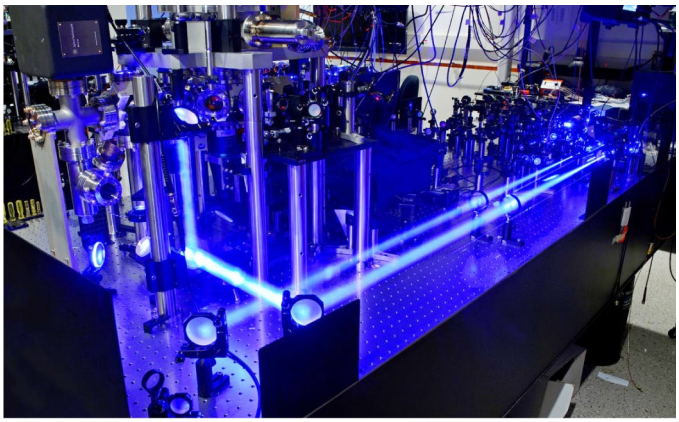
MAY 2020

WHY THIS MATTERS

Quantum technologies could revolutionize sensors, computation, and communication. As a result, they could strengthen the country's national security position and better protect sensitive and classified information, although many years of development may be needed to do so.

/// THE TECHNOLOGY

What is it? Quantum technologies build on the study of the smallest particles of energy and matter to collect, generate, and process information in ways not achievable with existing technologies. *Quantum sensors* could be used in science, industry, and navigation to make more precise and accurate measurements and offer potential benefits for critical defense and civilian applications, including maintaining timing and position accuracy in GPS-challenged or denied environments. *Quantum communications* could allow businesses and governments to securely transmit information. *Quantum computers* could dramatically accelerate computation for some applications, such as machine learning and decrypting information.



Source: Courtesy of Massachusetts Institute of Technology's Lincoln Laboratory. | GAO-20-527SP

Figure 1. Trapped Ion Qubit Test Bed in the Quantum Information and Integrated Nanosystems Group at Lincoln Laboratory. Qubit is a term for a quantum bit.

How does it work? Quantum technologies take advantage of counterintuitive properties that apply at the smallest scale. One property is a connection between two or more particles called "entanglement," in which characteristics are linked between particles, and measuring one particle reveals information about the others. Another property is "superposition," which allows a particle, while unobserved, to be in all possible observable states simultaneously. A third property is the "no cloning theorem," which prohibits the copying of unknown quantum states.

Quantum technologies use a combination of these properties to sense, communicate, and compute. For example, quantum sensors could use entangled particles of light to overcome stealth technologies and be resistant to advanced radar jamming. Quantum communication uses these properties to securely exchange encryption keys and determine if a message has been intercepted. And the "quantum bits" or "qubits" in a quantum computer use superposition and entanglement to process data in unique and potentially more effective ways.

How mature is it? Quantum technologies are not yet fully functional, although some are more mature than others.

- *Quantum sensors* are the most established, with some applications already in use. These technologies, which include atomic clocks and gyroscopes, need further development to reach their potential, likely requiring at least 5 more years.
- *Quantum communications* have progressed in the last decade, with advances in the use of fiber optics or satellites for quantum key distribution, to ensure that quantum cryptographic keys cannot be intercepted without the eavesdropper being detected. However, such technologies may have limited range. Fiber optic links become ineffective for quantum key distribution at distances over 60 miles. Satellite links have been demonstrated for ground distances of up to 4,700 miles, but such demonstrations are not entirely based on quantum physics and therefore are not fully secure. Fiber optic technologies will likely require at least 10 years of development before they can be used for long-distance secure networks. Satellite communications may be available sooner, but will require more development before they are fully secure and useful for practical quantum communications.
- *Quantum computers* are available with dozens of the fundamental components known as physical qubits, although a general use quantum computer may need more than 100,000 physical qubits. To develop quantum computers that can solve problems of practical significance—such as factoring the large numbers used in encryption schemes—it will be necessary to improve their hardware; such efforts could take 20 years. For example, chips would need to hold more physical qubits while maintaining accuracy and precision.

/// OPPORTUNITIES

Quantum technologies may enable the following advances, assuming extensive technological progress:

- **Improve measurement.** Quantum sensors may be able to locate previously invisible or stealth targets, or determine an object's location and speed, even if GPS is jammed or spoofed, or if a satellite link is lost.

- **Enable secure communication.** Quantum communications may eventually allow for completely secure quantum digital signatures, secure sharing of sensitive and classified information, or other applications.
- **Solve complex computational problems.** Quantum computers may one day be able to quickly complete tasks that classical computers cannot carry out efficiently—such as factoring large numbers, a task central to cracking current cryptographic systems.
- **Create a quantum internet.** Future communication technologies may be able to securely transmit information between quantum computers. The resulting quantum internet would be inaccessible to outside computers, because any attempts to access the network would reveal a hacker's presence.

/// CHALLENGES

Quantum technologies face many challenges to reaching full potential and, once developed, will pose serious challenges to information security.

- **Institutional boundaries.** Quantum technology development will depend on collaboration across institutions and skill sets, and on a multidisciplinary workforce with training in quantum physics, engineering, mathematics, and computer science.
- **Technology development.** Quantum technologies depend heavily on developing new capabilities. For example, quantum computers use extremely fragile qubits that require refrigeration technologies that maintain temperatures close to absolute zero, requiring qubits that compute at warmer temperatures, along with technologies to better insulate them from the environment. Further, limited infrastructure may be available to test and evaluate these technologies.
- **Determining limits.** Quantum sensors will need to surpass current operating limits in order to achieve the ultimate quantum physics limits to precision measurement. For example, it may be necessary to develop new materials in order to increase precision.
- **Application and algorithm development.** Quantum computers will speed up some applications, such as machine learning, chemistry modeling, and cryptography, and each application needs work in developing the quantum algorithms the computer would use. But quantum computers will not speed up the solving of some problems, such as those requiring large amounts of data.
- **Transitioning cybersecurity.** A full-scale quantum computer has the potential to break standard encryption technologies, creating a major information security risk. The cybersecurity infrastructure will need to evolve to create quantum-proof encryption and protect existing information.

/// POLICY CONTEXT AND QUESTIONS

Quantum technologies will require additional years of development and could revolutionize how people measure, communicate, and compute. The development of such technologies raises many policy questions:

- How can the United States build a workforce with the diverse, cross-cutting skills needed to develop quantum technologies?
- What are the national security implications of other nations developing quantum technologies? How might the United States prepare and respond? What are the implications of quantum sensor technologies that could track stealth targets?
- What are the implications of a quantum computer being able to break present-day encryption schemes?

/// SELECTED GAO WORK

- National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies, GAO-19-204SP.
- Science and Technology: Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas, GAO-18-656.
- GAO Strategic Plan 2018-2023: Trends Affecting Government and Society, GAO-18-396SP.

/// SELECTED REFERENCES

Library of Congress. Congressional Research Service. *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations.* R45409. Washington, D.C.: Updated Nov. 1, 2019.

Lloyd, Seth, 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.

National Science and Technology Council. *Advancing Quantum Information Science: National Challenges and Opportunities.* Washington, DC: July 22, 2016.

GAO SUPPORT:

GAO meets congressional information needs in several ways, including by providing oversight, insight, and foresight on science and technology issues. GAO staff are available to brief on completed bodies of work or specific reports and answer follow-up questions. GAO also provides targeted assistance on specific science and technology topics to support congressional oversight activities and provide advice on legislative proposals.

Timothy M. Persons, PhD, Chief Scientist, personst@gao.gov

Staff Acknowledgments: Karen Howard, PhD, (Director), R. Scott Fletcher, PhD, (Assistant Director), Charlotte E. Hinkle, PhD, (Analyst-in-Charge), Anika McMillon, and Ben Shouse.