Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated November 15, 2022

# Defense Primer: Quantum Technology

Quantum technology translates the principles of quantum physics into technological applications. In general, quantum technology has not yet reached maturity; however, it could hold significant implications for the future of military sensing, encryption, and communications, as well as for congressional oversight, authorizations, and appropriations.

## Key Concepts in Quantum Technology

Quantum applications rely on a number of key concepts, including superposition, quantum bits (qubits), and entanglement. *Superposition* refers to the ability of quantum systems to exist in two or more states simultaneously. A *qubit* is a computing unit that leverages the principle of superposition to encode information. (A classical computer encodes information in bits that can represent binary states of either 0 or 1, whereas a quantum computer encodes information in qubits, each of which can represent 0, 1, or a combination of 0 and 1 at the same time. Thus, the power of a quantum computer increases exponentially with the addition of each qubit.)

*Entanglement* is defined by the National Academy of Sciences (NAS) as a property in which "two or more quantum objects in a system can be intrinsically linked such that measurement of one dictates the possible measurement outcomes for another, regardless of how far apart the two objects are." Entanglement underpins a number of potential military applications of quantum technology. Both superposition and entanglement are, however, difficult to sustain due to the fragility of quantum states, which can be disrupted by minute movements, changes in temperature, or other environmental factors.

## Military Applications of Quantum Technology

The Defense Science Board (DSB), an independent Department of Defense (DOD) board of scientific advisors, has concluded that three applications of quantum technology hold the most promise for DOD: quantum sensing, quantum computers, and quantum communications. The DSB concluded that quantum radar, hypothesized to be capable of identifying the performance characteristics (e.g., radar cross-section, speed) of objects—including low observable, or stealth, aircraft—"will not provide upgraded capability to DOD."

### Quantum Sensing

Quantum sensing uses the principles of quantum physics within a sensor. According to the DSB, this is the most mature military application of quantum technologies and is currently "poised for mission use." Quantum sensing could provide a number of enhanced military capabilities. For example, it could provide alternative positioning, navigation, and timing options that could in theory allow militaries to continue to operate at full performance in GPS-degraded or GPS-denied environments.

In addition, quantum sensors could potentially be used in an intelligence, surveillance, and reconnaissance (ISR) role. Successful development and deployment of such sensors could lead to significant improvements in submarine detection and, in turn, compromise the survivability of sea-based nuclear deterrents. Quantum sensors could also enable military personnel to detect underground structures or nuclear materials due to their expected "extreme sensitivity to environmental disturbances." The sensitivity of quantum sensors could similarly potentially enable militaries to detect electromagnetic emissions, thus enhancing electronic warfare capabilities and potentially assisting in locating concealed adversary forces.

### Quantum Computers

According to NAS, "quantum computers are the only known model for computing that could offer exponential speedup over today's computers." While quantum computers are in a relatively early stage of development, advances—many of which are driven by the commercial sector—could hold implications for the future of artificial intelligence (AI), encryption, and other disciplines.

For example, some analysts have suggested that quantum computers could enable advances in machine learning, a subfield of AI. Such advances could spur improved pattern recognition and machine-based target identification. This could in turn enable the development of more accurate lethal autonomous weapon systems, or weapons capable of selecting and engaging targets without the need for manual human control or remote operation. AI-enabled quantum computers potentially could be paired with quantum sensors to further enhance military ISR applications.

In addition, quantum computers could potentially decrypt classified or controlled unclassified information stored on encrypted media, allowing adversaries to gain access to sensitive information about U.S. military or intelligence operations. Some analysts note that significant advances in quantum computing would likely be required to break current encryption methods. Their estimates suggest that a quantum computer with around 20 million qubits would be required to break current encryption methods; however, the most advanced quantum computers today generally have no more than 433 qubits.

The practical applications of quantum computers will likely be realized only after improvement in error rates and development of new quantum algorithms, software tools, and hardware. While, as NAS notes, "there is no guarantee that [these technical challenges] will be overcome," some analysts believe that an initial quantum computer prototype capable of breaking current encryption methods could be

developed in the 2030 to 2040 timeframe. For this reason, NAS concludes that "the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster." (Information intercepted prior to the deployment of post-quantum cryptography would not be protected.)

In May 2022, the Biden administration released *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10)*, which "directs specific actions for agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography." NSM-10 notes that the Director of the National Institute of Standards and Technology and the Director of the National Security Agency (NSA) are developing and expected to publicly release by 2024 technical standards for quantum resistant cryptography. In September 2022, NSA issued a cybersecurity advisory stating that it "expects the transition to [quantum-resistant] algorithms for [national security systems] to be complete by 2035 in line with NSM-10."

### Quantum Communications

Quantum communications—excluding quantum key distribution ([QKD], discussed below)—are in a nascent stage of development. Quantum communications could theoretically enable the secure networking of quantum military sensors, computers, and other systems, thus improving performance over that of a single quantum system or classical communications network. Networking could additionally strengthen the robustness of such systems at range, thus expanding the potential environments in which they could be deployed (i.e., outside of the laboratory settings generally required to sustain fragile quantum states). This could significantly expand the military utility of quantum communications.

Quantum key distribution is a subset of quantum communications that uses the principles of quantum physics to encrypt information that is then sent over classical networks. QKD enables secure communications that cannot be covertly intercepted during transmission. (QKD communications can, however, be intercepted at the relay stations currently required for long-distance transmissions.) China is reportedly investing heavily in QKD and completed construction of an approximately 1,250 mile Beijing-Shanghai quantum network in 2016. Nonetheless, the DSB concluded that "QKD has not been implemented with sufficient capability or security to be deployed for DOD mission use."

## Funding and Recent Legislative Activity

Congress has considered the management and implications of quantum technology. For example, Section 234 of the FY2019 National Defense Authorization Act (NDAA) (P.L. 115-232) directs the Secretary of Defense—acting through the Under Secretary of Defense for Research and Engineering—to execute a quantum technology research and development program in coordination with the private sector and other government agencies.

Furthermore, Section 220 of the FY2020 NDAA (P.L. 116-92) requires DOD to develop ethics guidelines for the use of quantum technologies, as well as plans for supporting the quantum workforce and reducing the cybersecurity risks associated with quantum technologies. It additionally authorizes the Secretary of each military department to establish Quantum Information Science (QIS) Research Centers that may "engage with appropriate public and private sector organizations" to advance quantum research. To date, the Navy has designated the Naval Research Laboratory as its QIS Research Center, while the Air Force has designated the Air Force Research Laboratory as a QIS Research Center for both the Air Force and Space Force. The Army says it does not plan to establish a QIS Research Center at this time.

Section 214 of the FY2021 NDAA (P.L. 116-283) directs the services to compile and annually update a list of technical challenges that quantum computers could potentially address within the next one to three years. The list currently includes quantum chemistry, optimization, and machine learning. Section 214 also directs the services to establish programs with small and medium businesses to provide quantum computing capabilities to government, industry, and academic researchers working on these challenges. Section 1722 directs DOD to conduct an assessment of the risks posed by quantum computers, as well as current standards for post-quantum cryptography.

Finally, Section 105 of the FY2022 NDAA (P.L. 117-81) directs the President to establish—through the National Science and Technology Council—the Subcommittee on the Economic and Security Implications of Quantum Information Science, while Section 229 directs the Secretary of Defense to "establish a set of activities to accelerate the development and deployment of dual-use quantum capabilities."

## Potential Questions for Congress

- What funding level does the current maturity of military applications of quantum technology warrant? To what extent, if at all, should the U.S. government invest in and research technologies that enable quantum military applications (e.g., materials science, fabrication techniques)?
- To what extent, if at all, can commercial advances in quantum technology be leveraged for military applications?
- How mature are U.S. competitor efforts to develop military applications of quantum technologies? To what extent, if at all, could such efforts threaten advanced U.S. military capabilities, such as submarines and stealth aircraft?
- What measures are being taken to develop quantum-resistant encryption and to protect data that have been encrypted using current methods?
- What measures, if any, should the United States take to ensure that the quantum workforce is sufficient to support U.S. competitiveness in quantum technology?

**Kelley M. Sayler**, Analyst in Advanced Technology and Global Security

**IF11836**

## Disclaimer