White paper

Preparing for a secure quantum future

A quantum internet guide for federal agencies

verizon

The future of the internet is quantum.

The future of the internet is quantum, and it isn't far from actuality. Over the past few years, the U.S. federal government has made the creation of the quantum internet a national priority. In early 2020, the Department of Energy (DoE) held a workshop that resulted in a roadmap and guide for creating the first quantum internet, and in 2021 the government budgeted over $235 million to begin building this next generation communication network. Most recently, on May 4, 2022, the Biden Administration signed two directives aimed at advancing national initiatives in quantum information science (QIS).

Many federal agencies have begun expressing interest in the massive capabilities that quantum technology enables, and with some already beginning to develop ways to harness this power, this is only the beginning of the quantum era.

What is quantum internet?

Simply put, quantum internet is a term for the network that will support communication between quantum endpoints including quantum computers and quantum sensors using properties of quantum mechanics. Agencies and research institutions globally are collaborating in a full-scale effort to develop the technologies needed to make the quantum internet widely available, something that, if current predictions are correct, will happen this decade.

This revolutionary technology will connect quantum computers to the benefit of solving currently intractable problems, hastening the pace of scientific research and driving economic development. Furthermore, they can facilitate the transfer of larger amounts of data in a more secure manner than current capabilities allow. The benefits are evident for agencies already using quantum technologies, and eventually will work to fully integrate with the current Internet (thus, becoming a key part of the United States' infrastructure).

Advancements in quantum technology

The quantum internet can in the future allow secure transfers of massive amounts of data. While classical data technology uses digital bits to store and transmit information, quantum technology uses qubits. The difference between standard bits and qubits is that standard bits are deterministic, only holding one value at a time, represented by either a '0' or a '1'.

Qubits on the other hand are probabilistic, representing both at the same time. Another difference is how the data technologies are represented in communications; bits are represented by electrical voltages or optical power, but qubits are represented by certain properties of quantum particles like photons or electrons.

Using elements of quantum physics, this rapidly advancing technology can allow new paradigms for computing and communications. To make the quantum internet feasible on a wide scale, researchers and organizations are focusing on developing technologies related to specific quantum properties. These quantum properties are at the core of quantum communications.

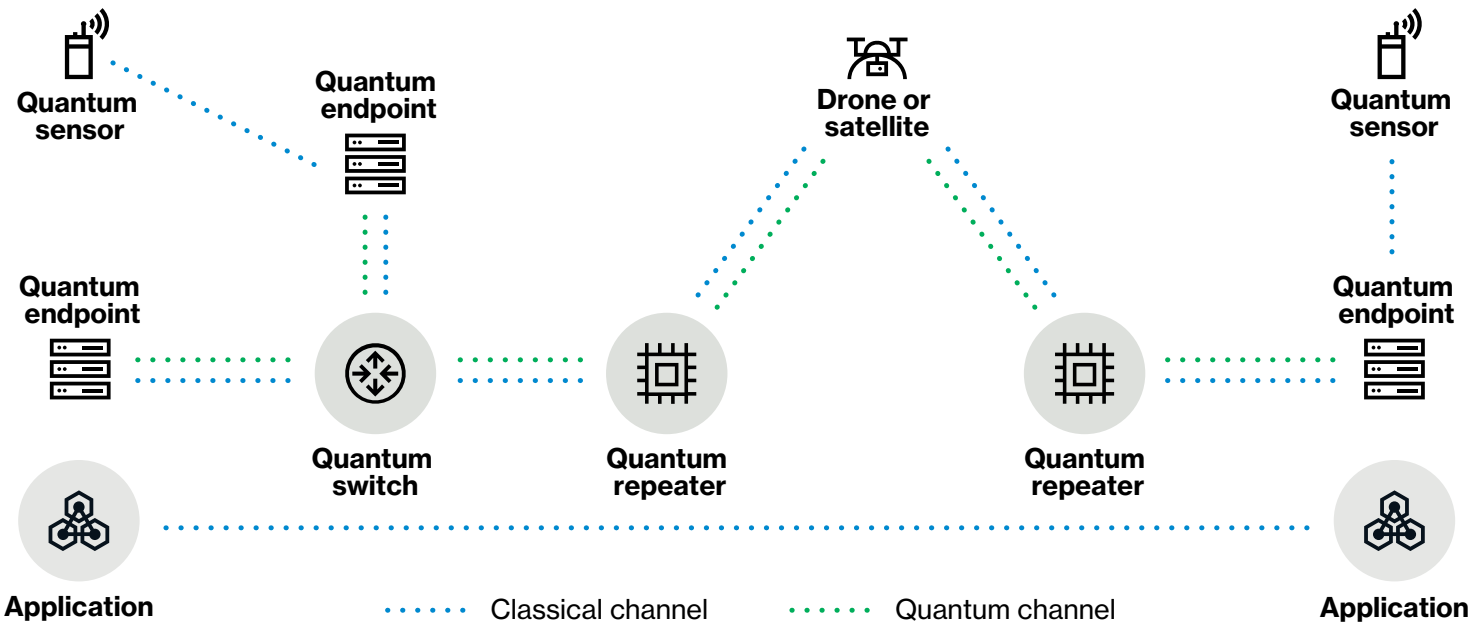
- **Quantum superposition**
  The qubit's ability to exist in two states at once as both '0' and '1' is known as superposition. Quantum superposition allows for parallelism, making it possible for agencies to analyze multiple outcomes in one operation, as well as making the data more secure. The superposition is broken down and reverted to a deterministic, classical bit value as soon as the qubit is read or measured, making it extremely difficult for hackers to infiltrate because they destroy the qubit as soon as they read it.

- **Quantum entanglement**
  A significant part of quantum communications, quantum entanglement happens when two subatomic particles interact and influence each other. Using entangled qubits, it's possible for agencies to generate secure cryptographic keys on two separate devices. Quantum entanglement also allows for an exponential increase in computing power as well as data transfer rates.

- **Quantum teleportation**
  Quantum teleportation exploits entanglement to enable data transfer between quantum endpoints encoded in qubits. This secure transfer method allows a substantial amount of information to be transported with very few bits being used on a traditional network, transforming how agencies share massive internal and external data.

Quantum technology will benefit network security.

Building on the definition of quantum internet and its capabilities, the next section will examine the benefits it will bring to network security, along with the stages and milestones necessary to make it a reality. As experts work to create this future Internet within the next decade, there are plenty of next steps and considerations for federal agencies to make in preparation.



Cryptography and security for future networks

Ahead of the fulfillment of the quantum internet, quantum mechanics are already helping make information, data, and communication more secure. In 2020, one of the first private sector Quantum Key Distribution (QKD) network prototypes was created and successfully tested. QKD may be one of the initial applications available on the quantum internet distributing encryption keys to secure applications on the Internet.

Encoding random information on photons of light and transmitting that information to another endpoint allows the derivation of the same encryption key at two different locations. The properties of quantum mechanics and QKD protocols provide unconditional security against eavesdroppers. Encryption keys derived on the quantum internet could then be used to secure confidential applications on the Internet.

The development of these capabilities is well underway, but it will take some time for them to become ubiquitous. Quantum computers will likely be similar to the first classic computers, which were large mainframes that filled entire rooms and took decades to become widely available. In the meantime, the quantum internet will provide a way for organizations to securely take advantage of quantum computing.

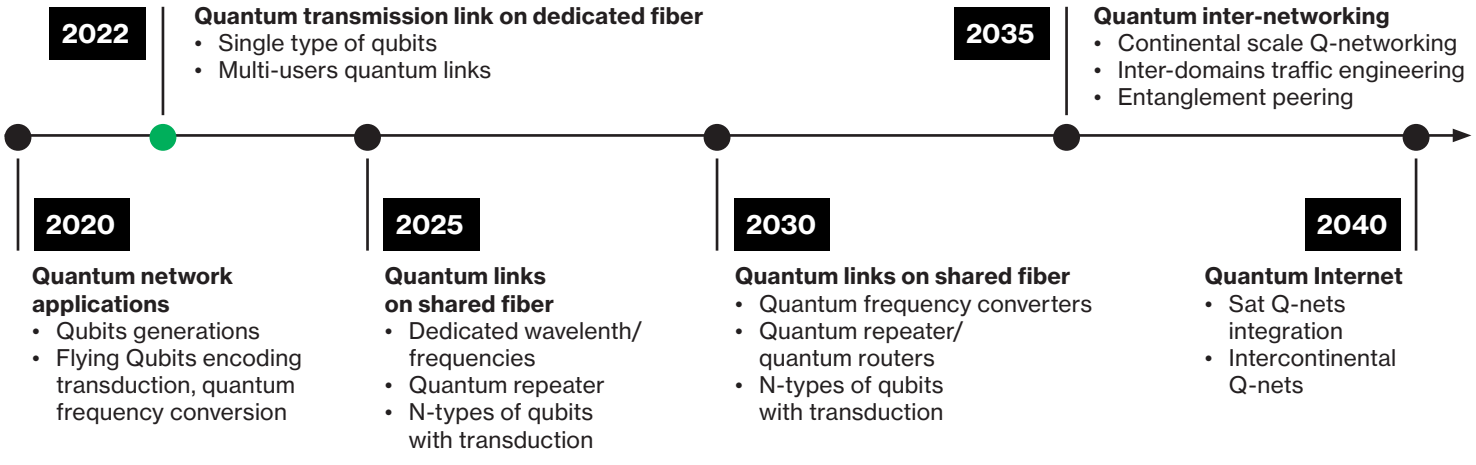
It will be possible to encrypt a data set and send it over the quantum internet to a quantum computer. A quantum computer could also receive the instructions for program execution, and after completing the instructions, then send the results back to the organization for decryption. During transit or computations, the actual data is never revealed since it is encrypted.

The DoE's roadmap to the quantum internet

The road to the quantum internet is being paved in several stages, which have been mapped out by the Department of Energy (DoE) and scientific researchers. One of these roadmaps, proposed by Professor Stephanie Wehner in 2018, is based on technology functions that become more advanced as the stages progress. Of the six milestones laid out by Wehner, the first two, trusted repeater and prepare and measure, have already been realized, and the next two, addressing the entanglement generation and quantum memory, are in progress with some success demonstrated already. Wehner's plan is like the DoE's blueprint, except for the final stage.

The DoE's blueprint, *From a Long Distance Entanglement to Building a Nationwide Quantum Internet,* begins and ends with synergy. It is the culmination of a February 2020 workshop that involved representatives from DoE national laboratories, academia, industry, U.S. government and others interested in quantum computing. This collaborative effort lays out five milestones that the U.S. will need to reach the quantum internet and explains the research opportunities that need to be further explored to advance the technology needed. The last milestone of the DoE's plan again notes that a large-scale collaborative effort between academia, government, and industry is needed to build and grow the quantum internet.

Recognizing the impact the quantum internet can have on addressing climate change and protecting the power grid, the DoE has allocated millions of dollars in the last few years to research and development. Protecting the power grid has been one of the DoE's main motivators in leading government agencies in developing a plan and working toward the creation of the quantum internet. While the plan has been mapped out for the quantum internet, it will take the united efforts of many to make it a reality.



Preparing for the future of internet

In the future, the quantum internet will offer a wealth of new communication capabilities, some of which have yet to be imagined. It was the DoE's 2020 symposium that formally launched the quantum internet initiative on a federal scale, but it will require a collective effort from agencies and research institutions to make it a reality. By combining these efforts, it is hoped that quantum internet will one day augment the current internet, making every day internet connections across the world more secure and efficient.

Although the drive for the quantum internet is a new endeavor, those spearheading the movement are quickly turning theory into reality to meet the mission. While the DoE is at the forefront of government investment in the quantum internet development, other agencies are vital to the on-going success. By committing funding and resources to developing quantum safe networks and identifying future use cases that will help solve our most pressing challenges.

For more information on the federal government's National Quantum Initiative, visit quantum.gov.

verizon