White Paper

Demystifying the Capabilities of Quantum Technologies Available Today and in the Future

Chapter 3: Quantum Networking & Quantum Communications

ATARC Global Quantum Working Group

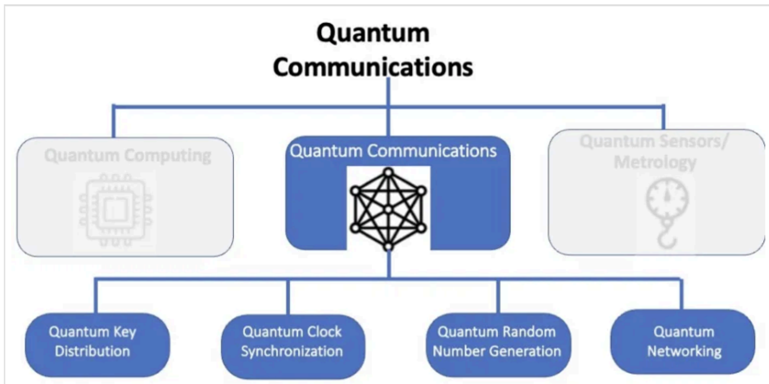
December 2024

ATARC
Advanced Technology Academic Research Center

Table of Contents

Disclaimer*: This white paper was prepared by the ATARC Quantum Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated. This white paper is intended to be a helpful guidance relating to current quantum technological capabilities.*

Chapter 3: Quantum Networking & Communications



Source: https://steveblank.com/2022/03/22/the-quantum-technology-ecosystem-explained/

With rapid advancements in quantum technologies, it's essential to understand the current and future capabilities of quantum networking and communications. At the forefront is Quantum Key Distribution (QKD), introduced by Charles Bennett and Gilles Brassard in 1984, which uses quantum mechanics to enable unbreakable encryption. QKD marks the shift of quantum theory from abstract science to practical, secure communication methods that differ fundamentally from classical encryption.

Here we explore the state and outlook of quantum networking and communications, demystifying their real-world applications, limitations, and transformative potential.

Quantum technologies exploit quantum physics and quantum mechanical effects which can lead to new capabilities with networking and communications. As highlighted by the US National Quantum Initiative Advisory Committee (NQIAC), "Quantum networking and communication … enable the transmission of quantum states and the distribution of entanglement across multiple quantum information systems. This capability could one day connect quantum devices to build larger-scale quantum computers or distributed quantum sensors with sensitivity that surpasses the standard quantum limit."[1]

Quantum communications utilize quantum states to encode information. The development of these secure communication protocols uses the principles of quantum mechanics (including superposition and entanglement) to ensure the confidentiality and integrity of transmitted information. Quantum networking refers to a type of network that uses quantum bits (qubits)

[1] https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Report-Quantum-Networking.pdf

to process and store information. Given the inherent interconnectivities of the two technologies, we will discuss both within this chapter.

Quantum communications and networking can be pure quantum technologies or hybrid quantum-classical networks. Pure quantum communication and networking technologies are farther away from maturing as the quantum technologies themselves have advancements which need to occur, and therefore most of today's technology are hybrid. These integrate quantum and classical communication channels, leveraging the strengths of both to enhance overall network performance. This approach is practical for gradually transitioning from classical to fully quantum networks.

Key Concepts in
Quantum Networking & Communications

Qubits and Superposition: In classical computing, bits are binary and can be either 0 or 1. Qubits, however, can be in a state of 0, 1, or both simultaneously, thanks to superposition. This property allows quantum computers to process vast amounts of data simultaneously.

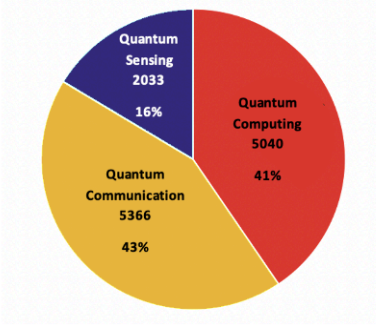
Entanglement: Quantum entanglement is a phenomenon where two or more qubits become interconnected such that the state of one qubit directly influences the state of another, regardless of distance. This property is crucial for quantum networking, enabling instantaneous communication across long distances.

Mature quantum networking and communications technologies are expected to provide safe and secure communications with a significant impact to national security as these have the potential to 1) improve security through the use of physics-based security that's unhackable; 2) increase computational power through distributed quantum computing networks; and 3) improve precision through distributed quantum sensors.

Global Engagement on Quantum Networking & Communications

Efforts to advance quantum information science, including that of quantum networking and communications, are incorporated into quantum programs around the globe. Quantum communication patents are the largest segment of patents for quantum technologies (see Figure 1)[2]. Included within the quantum communications patents are technologies such as quantum internet, QKD and others. As noted in *Chapter 2, Demystifying the Capabilities of Quantum Technologies Available Today and in the Future*

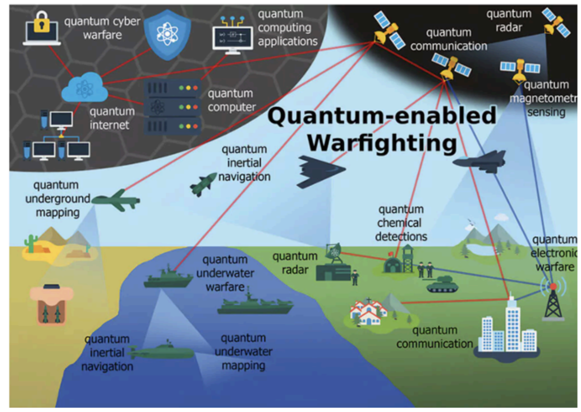
Figure 1: Quantum patents



[2] https://www.euroquic.org/wp-content/uploads/2024/03/QuIC-White-Paper-IPT-January-2024.pdf

Chapter 2: Quantum Sensing[3], China is leading the efforts for quantum communications patents with over 3600 patents, and the US is a distant second in patents with approximately 550 patents in quantum communications.

Figure 2: Quantum Enabled Warfighting



Quantum computing, communications, networking and sensing technologies, while developed individually will not be deployed in silos. Quantum technologies will ultimately interact with each other, and with classical technologies, creating a quantum ecosystem. One illustration of this interconnectivity is with defense implementation. One can see the interconnectivity of quantum computing, sensing, communications and networking as discussed by the Joint Air Power Conference Centre[4]. (see Figure 2)

Global leadership in the fields of quantum communications and networking development and deployment is being led by the People's Republic of China (PRC), which has made quantum communications technology a major focus of their quantum programs with a significant patent portfolio dedicated to quantum communication and networking technologies. According to the Information Technology & Innovation Foundation (ITIF) "China has secured global leadership, notably demonstrated through the development of the world's longest quantum key distribution (QKD) network—the 1,200-mile Beijing-Shanghai backbone. Coupled with the groundbreaking Micius satellite, which extends quantum communication over even greater distances, this network has put China at the forefront of secure, long-distance quantum communication."[5] (see Figure 3)

Figure 3: 1,200-mile China Quantum Communications Corridor

[3] https://atarc.org/wp-content/uploads/2024/07/demystifying-the-capabilities-of-quantum-technologies-available-today-and-in-the-future.docx-3.pdf

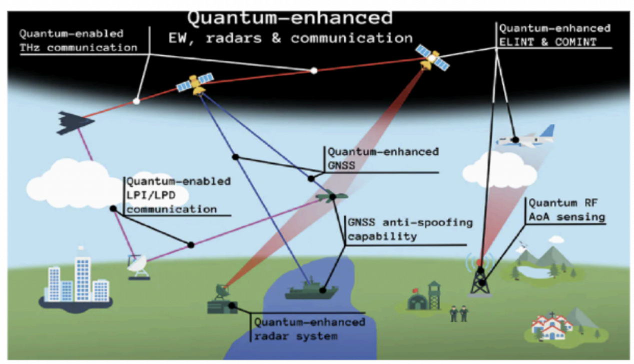
[4] https://www.japcc.org/articles/quantum-technology-for-defence/

[5] https://itif.org/publications/2024/09/09/china-is-challenging-us-leadership-in-quantum-technologies-new-report-finds/

PRC is not alone in its efforts. In Singapore, SPTel and Singtel, communication service providers, are working with Nokia and other companies on strengthening enterprise cybersecurity. In South Korea, a partnership known as the Quantum Alliance, provides an opportunity for companies like SK Telecom and Nokia to work together to develop South Korea's quantum ecosystem. In Japan, an operation centre in Otemachi is connected with three other places that are situated 12, 13 and 45 km away. In Japan a secure TV conference was demonstrated between Kogenei and Otemachi by performing trusted quantum key distribution[6] in 2010.

Early global collaboration was also demonstrated between ID-Quantique, a Swiss company, Senetas, an Australian company, and the University of KwaZulu-Natal in South Africa where they laid the foundation for commercial exploration of QKD. This collaboration began in 2008 and included projects such as QuantumCity and QuantumStadium in Durban, South Africa that showcased early adoption of quantum-secured communication[7]. These initiatives, implemented at demonstrable scale during the 2010 FIFA World Cup and in municipal fiber optic networks, offered valuable insights into the robustness of QKD systems in real-world, commercial environments. This momentum has contributed to the broader scope of international partnerships under the BRICS International Quantum Communications Research initiative, a multilateral collaboration between Brazil, Russia, India, China, and South Africa.[8]

Figure 4: Joint Air Power Conference Centre



The European Quantum Communication Infrastructure (EuroQCI) Initiative, led by the EU and the European Space Agency, is focused on designing, developing and deploying a secure quantum communications infrastructure composed of a terrestrial segment relying on fiber communications networks linking strategic sites at national and cross-border level, and a space segment based on satellites.[9] The EU program aims to safeguard sensitive data and critical infrastructures by integrating quantum-based systems into existing communication infrastructures for QKD, providing an additional security layer based on quantum physics. A European consortium, dubbed Nostradamus, is led by Deutsche Telekom (DT), a digitalization partner for the EU, and includes other partners including the French tech company Thales, and the Austrian Institute

[6] 3https://tu-delft.foleon.com/tu-delft/quantum-internet/the-six-stages-of-quantum-networks/
[7] Realizing long-term quantum cryptography
[8] BRICS International Quantum Communications Research Underway
[9] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

of Technology. The consortium is developing EU's quantum communications testing infrastructure.[10] Through the EuroQCI program, Nokia is working with the national research and education network of Greece, GRNET, the HellasQCI consortium to advance a nationwide quantum-safe network infrastructure.[11] There are other activities as well including a partnership with Nokia and Belgium communications service provider Proximus that completed a live trial of QKD by successfully encrypting and transmitting data between data centers in Brussels and Mechelen. In Portugal, IP Telecom is establishing quantum-safe connectivity for Portugal's three major data centers. In the report by the Joint Air Power Conference Centre, Dr. Michal Krelina has highlighted the importance of precision of quantum clocks within a quantum-enhanced communications infrastructure for defense purposes, and validates the interconnectivity of the different quantum technologies. (see Figure 4)[12]

In the United Kingdom, the government is asking industry for key commercial opportunities, technology requirements and milestones for quantum including quantum networking. The quantum networking call is asking for technology and research milestones to materialize quantum networks, analysis of competing quantum networking components, underpinning classical infrastructure requirements to inform ongoing policy developments, government, and infrastructure developments programs.[13]

In Canada, TELUS Corporation is partnering with quantum computing company Photonic to boost next-generation quantum communications. By providing Photonic with access to its fiber-optic network, TELUS will support the testing of innovative quantum technologies to improve the country's digital infrastructure.[14]

US engagement on quantum networking and communications remains concentrated within the research domain, with a few exceptions. From 2019-2024, the US Department of Energy (DOE) created five different quantum centers, and Q-NEXT is focusing on communications and networking. Q-NEXT research is focused on control and distribution of quantum information enabling secure communication over long distances using quantum repeaters and quantum sensors to achieve unprecedented sensitivities.[15] Q-NEXT has launched two national foundries for quantum materials. Another effort has begun in Tennessee with EPB of Chattanooga, an electric power distribution and telecommunication company, who has partnered with Qubitekk[16] and Oak Ridge National Lab to create the first US commercially available quantum network. This network is designed for private companies and government to run quantum

---

[10] https://www.sdxcentral.com/articles/news/eu-invests-200m-in-quantum-technology-to-secure-communications-networks/2024/01/
[11] https://www.forbes.com/sites/nokia-industry-40/2024/08/12/quantum-computing-is-coming-heres-what-needs-to-happen-first/
[12] https://www.japcc.org/articles/quantum-technologies-for-air-and-space/#:~:text=The%20average%20Technology%20Readiness%20Level,and%20are%_20demonstrating%20impressive%20results
[13] https://www.contractsfinder.service.gov.uk/notice/b1a5b405-9df5-4c0e-a4da-293969433080?origin=SearchResults&p=36
[14] https://finance.yahoo.com/news/telus-photonic-collaborate-boost-quantum-145300385.html
[15] https://nqisrc.org/
[16] https://qubitekk.com/epbquantumnetwork/

equipment and applications in an established fiber optic environment. This project is aimed at accelerating the process for bringing quantum communications technologies to market. The DOE announced[17] a private-public partnership dedicated to quantum and space with one of the objectives being to integrate and orchestrate a quantum secure communication demonstration in orbit. Also in the US, Cisco Quantum Lab has been established to work with universities and start-ups to develop the quantum frontier of networking and security. (see Figure 5)

Figure 5: Quantum Networking focus from CISCO

NASA announced sending quantum communications to the international space station. As part of the SpaceX 31st commercial resupply mission, NASA sent the Space Entanglement and Annealing Quantum Experiment, or SEAQUE, from the Jet Propulsion Laboratory in southern California to the international space station. SEAQUE is a technology demonstration that will explore how quantum technologies can improve communications across vast distances. If successful, the experiment may pave the way for quantum communication systems globally and in space.[18]

Engineering quantum systems are advancing at a rapid pace, and researchers are looking to unleash the power of quantum technologies for secure communications and networking. Future fault-tolerant quantum computers, which aren't expected for many years, are expected to break the legacy public-key encryption systems, but today's advances in Post-Quantum Cryptography (PQC) algorithms, which are classic and not quantum technologies, can provide an answer to this cybersecurity threats. But many are looking at quantum solutions along with PQC efforts. The need for safe communications has expanded with the rapid growth of the Internet of Things. This amplified demand calls for new sources of randomness for security, and that is where quantum random number generators can provide a solution. In addition to direct applications, the underlying optical and photonics hardware technologies could find dual use for next-generation classical optical products, something Cisco is planning to leverage. Both a near-term market horizon and the value of the corresponding optics/photonics technologies make networking and security a sweet spot for investment in quantum technologies.

[17] https://www.energy.gov/technologytransitions/articles/us-department-energy-announces-first-its-kind-collaboration-quantum
[18] https://science.nasa.gov/biological-physical/investigations/seaque-space-entanglement-and-annealing-quantum-experiment/

Quantum Networking and Communications Technologies

As with quantum computing and quantum sensing, there is no one monolithic technology that covers networking and communications. Key distribution and random number generators are both used in cryptography and data security, but they have different purposes and methods and are different than the post quantum cryptography (PQC) algorithms which use classical computing and not quantum mechanical effects. Below is a high-level discussion of the different networking and communication technologies, the use cases, and their readiness levels.

Quantum Key Distribution (QKD): Authentication protocols in quantum networks ensure that communicating parties are genuine and not adversaries. Quantum authentication schemes often combine classical cryptographic techniques with quantum mechanics to provide robust security guarantees. This security is a key focus for QKD technologies. QKD is a secure communication method that uses quantum mechanics to encrypt and decrypt messages. Unlike classical encryption, which can theoretically be broken once a large enough fault-tolerant quantum computer is developed, QKD's security is based on the fundamental laws of physics and deemed to be unhackable. Any attempt to eavesdrop on a QKD process will inevitably alter the state of the qubits, alerting the communicating parties. There are a variety of different industries and use cases for QKD. According to the Boston Consulting Group (see Figure 6)[19] these span many difference areas including finance, defense, health care, telecommunications, etc. China and Europe make up more than half of the key geographies engaging with QKD. QKD's inability to be implemented in software or as a service on a network makes it difficult to integrate into existing network equipment. The US National Security Agency's position is that post quantum cryptography algorithms supported by NIST are more affordable at this time.[20] Both the benefits and detractions of QKD are discussed by the Quantum Economic Development Consortium in their report, QKD: Part of a Defense-In-Depth Security Strategy.[21]

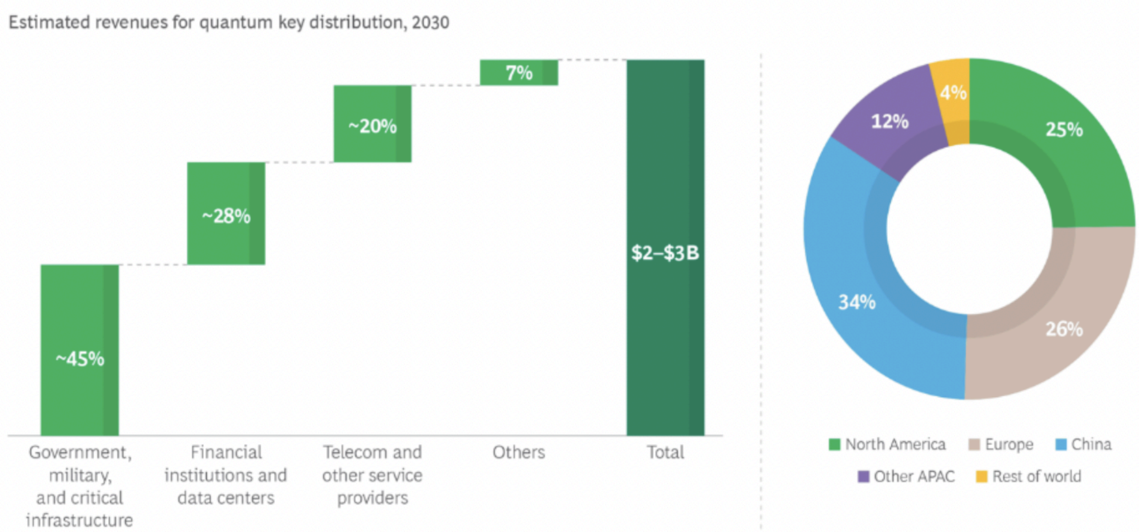
---

[19] hhttps://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications#:~:text=BCG%20helps%20global%20and%20regional,Public%20Sector

[20] https://steveblank.com/2022/03/22/the-quantum-technology-ecosystem-explained/

[21] https://quantumconsortium.org/qkd-part-of-a-defense-in-depth-security-strategy/

Figure 6: Key Sectors and Geographies for QKD



Within QKD, there are different technologies include:

- Device-Independent QKD (DI-QKD): DI-QKD protocols do not rely on the trustworthiness of the devices used in the communication process. This enhances security by eliminating potential vulnerabilities introduced by compromised hardware or software.
- Continuous-Variable QKD (CV-QKD): Unlike discrete-variable QKD, which uses individual photons, CV-QKD employs continuous variables such as the quadrature components of a light field. CV-QKD systems can be more compatible with existing telecommunication infrastructure, leveraging homodyne detection techniques.

Quantum Random Number Generators (QRNGs): Quantum random number generators are a hardware component that generates unpredictable random numbers using quantum mechanical effects. QRNGs are used in a variety of applications, including cryptography, data security, statistical analysis, and gaming. QRNGs are considered a root of trust in cybersecurity because they produce unpredictable outcomes in a controlled way. QRNGs are believed to have built in checks for tampering to provide high attack resistance. According to Boston Consulting Group (see Figure 7)[22] there are several industries who can benefit from and have a need for QRNGs including industries that use the Internet of Things, data centers, and financial institutions.

[22] https://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications#:~:text=BCG%20helps%20global%20and%20regional,Public%20Sector

Figure 7: Industries and Drivers for Quantum Random Number Generators

	% of revenues (projected)	
Financial institutions	33%	• Better random numbers for encryption to facilitate higher cybersecurity resistance • Quantum vault to store digital keys for blockchain (in combination with QKD) • Monte Carlo simulations
Cloud, data center, and network	30%	• Improved data encryption in data centers with high-quality random numbers • Randomness generation as a cloud offering for end customers (QRNG as a service) • Improved encryption in 5G/6G telecom infrastructure
IoT devices	26%	• Improved security for IoT devices, mainly in applications where security is important and in cases where higher-end devices with enough memory are used (such as connected cars, industrial IoT, smart cities, and smart logistics)
Smartphones	7%	• QRNG low-cost chips in smartphones contribute to more secure communications, ecommerce, and mobile payments • Marketing differentiator for smartphone manufacturers
Noncryptographic applications	5%	• Internal and external (as a service) sources of high-quality random numbers that can be used in encryption across industries (including QRNG as a part of HSM, combination of QRNG with PQC) • True source of randomness for R&D, gambling (online gaming, lotteries) • Protection of information from sensors in smart grids and other energy infrastructures

Quantum Repeaters: Quantum repeaters are essential for extending the range of quantum communication. They amplify the quantum signals without disturbing their quantum state, overcoming the limitations imposed by signal loss and decoherence over long distances. It is widely believed that a necessary and highly demanding requirement for quantum repeaters is the existence of matter quantum memories.[23] These technologies are in development currently.

Quantum Memory: Quantum memory devices are an enabling technology that stores quantum information reliably. These will be crucial for synchronizing qubits in a network, allowing for complex quantum communication protocols. Quantum memories are key components of quantum communications as they will enable the storing of quantum information and can be used with quantum repeaters to extend the range of secure communication networks. This is important for quantum repeaters, networks and cryptography, and currently in development.

Quantum Internet: According to the University of Chicago, “The quantum internet is a network of quantum computers that will someday send, compute, and receive information encoded in quantum states. The quantum internet will not replace the modern or “classical” internet; instead, it will provide new functionalities such as quantum cryptography and quantum cloud computing.”[24] Researchers estimate that it will take 10-15 years to create an

[23] https://www.nature.com/articles/ncomms7787
[24] https://news.uchicago.edu/explainer/quantum-internet-explained

entangled network of quantum computers. Unlike traditional computers, it's not believed that individuals will own their own personal quantum computers, instead, quantum computers will be cloud accessible (as they are now), but the future quantum internet would link multiple quantum computers together. While the full use for a quantum internet is still theoretical, The quantum internet represents a paradigm shift in how we think about secure global communication.[25] Beyond quantum computing, the quantum internet is thought to be able to keep technology in perfect sync across long distances using quantum clocks. The vision of a fully realized quantum internet involves connecting quantum computers and sensors across a network, enabling advanced applications such as distributed quantum computing, quantum cloud computing, and more efficient and secure global communication. The quantum internet is nascent as it will need mature quantum technology to be fully developed prior to networking them together.

Industries That Could Benefit from Quantum Networking & Communication Technologies

As with computing and sensing technologies, quantum networking and communications technologies can provide needed security which could benefit a variety of different industries. From enhanced security and secure data transfers to fully realized quantum internet, here are a few use cases and industries which have been identified, but future benefits may become more apparent as technologies mature.

- **Energy:** Networking can secure communication between power grid components, such as generators, substations, and control centers. It can also help protect against insider threats and facilitate secure data sharing.
- **Lotteries and Gaming:** Quantum communications can provide random number generation for lotteries and online gaming to ensure a uniform winning probability.
- **Finance:** Quantum computing can aid in finance, especially with its advanced simulation capabilities and optimization calculations, and secure communications networks can provide resilience and security. It can also help credit card companies with security customer data.
- **National Security & Cybersecurity:** Secure communications with QKD and ultimately the quantum internet will provide enhanced cybersecurity for companies and governments. For example, QKD ensures that communication channels are virtually immune to eavesdropping and hacking attempts. This is particularly beneficial for federal agencies handling sensitive data.
- **Materials discovery:** A quantum network can provide enhanced computational power needed for breakthroughs in materials discovery, currently outside the reach of classical computation alone.

[25] https://news.uchicago.edu/explainer/quantum-internet-explained

- **Quantum AI:** A quantum network can provide enhanced computational power to drive breakthroughs in next-gen quantum AI.

In the next few years, several sectors like IT, space, research, healthcare and retail can attain fast communication and high-performance computing with quantum networking. The near-term uses of QKD and QRNGs have created a focus, mainly in Europe and Asia, for developing and deploying commercial use of QKD. There is also a growing penetration of QRNG chips in smartphones, tablets, PCs, and data centers. Future adoption is believed to happen with increased integration of QRNG chips in Internet of Things infrastructure and devices. As quantum computing and quantum sensing mature, then additional integration into communications and networking will occur.

Quantum Networking & Communications Key Players

As with all quantum technologies, there are a growing number of organizations, governments and academia developing and testing quantum networking and communications technologies. This list is not meant to be exhaustive, but instead a selected list of players of different organizational sizes and from different regions.

Mid-Large Players

Toshiba Corporation, a Japanese company has created QKD products as well as a Quantum Key Management System for the storage, transmission and routing of quantum keys between the nodes of a quantum-secured network.

QuantumCTek, a Chinese mid-size company specializing in quantum communication products and services. plays a crucial role in China's quantum communication infrastructure. QuantumCTek was founded by a group of prominent scientists, including China's "father of quantum" Pan Jianwei and leading quantum pioneer Guo Guangcan. The company has focused on developing QKD technologies.

Nokia, a Finnish Company is working on a secure quantum internet through several public-private partnerships in Europe and Asia.

Boeing, has announced plans to launch a quantum networking satellite demo in 2026.[26] Boeing plans to deploy a small satellite in 2026 to test technology needed for a quantum internet capable of connecting more advanced sensors and computers worldwide

[26] https://spacenews.com/boeing-plots-2026-quantum-networking-satellite-demo/

Small Players/Start-Ups

Qubitekk, a US company, is working to build a quantum network with the partnership of EPB and Oak Ridge National Lab in Tennessee. Their view is that a commercial quantum network, the common-use equipment, software, and network management must be achieved through the integration of commercially released products offered and supported by industry vendors. Only recently has this been possible due to the growth of the quantum component industry. Reliable commercial qubit sources, single photon detectors, quantum-compatible fiber optic switches, and a variety of other devices and software are now available for procurement and inclusion in a commercial quantum network.[27]

Quantum Xchange, a US start-up provides the Phio Trusted Xchange (TX), a quantum-safe, out-of-band key delivery system. Their technology can support QKD deployments, they are not a quantum communications provider or reseller. Their quantum-safe key exchange supports quantum keys generated from any source (QRNG or QKD) protected by any method.

ID Quantique, a Swiss based company, provides high-performance quantum-safe security with QKD and commercial QRNGs. They are also building quantum sensing technologies. ID Quantique (IDQ) has successfully demonstrated the use of quantum communications in the banking industry to secure data through the use of their QRNG to generate keys for security applications and cryptologic operations, such as authentication, digital signatures, and secure access control

Quantum Bridge, a Canadian, quantum networking start-up that is delivering symmetric key distribution technology that achieves future-proofed security at scale, without asymmetric encryption. They are working on key distribution and have shown long-distance quantum cryptography over 200km will remain secure even with seriously flawed detectors.[28]

Quintessence Labs, an Australian company, is providing QKD, QRNGs and Quantum Key management systems. to provide strong data protection and help organizations build a quantum-safe future.

[27] https://static.epb.com/sha-930d7f7/assets/quantum/documents/2211.14871.pdf
[28] https://arxiv.org/abs/1109.1473

Academia/National Labs

Quantum Collaborative includes Arizona State University supports research harnessing end-to-end entanglement for quantum networking. They work with industry partners including IBM, Dell and Quantinuum.

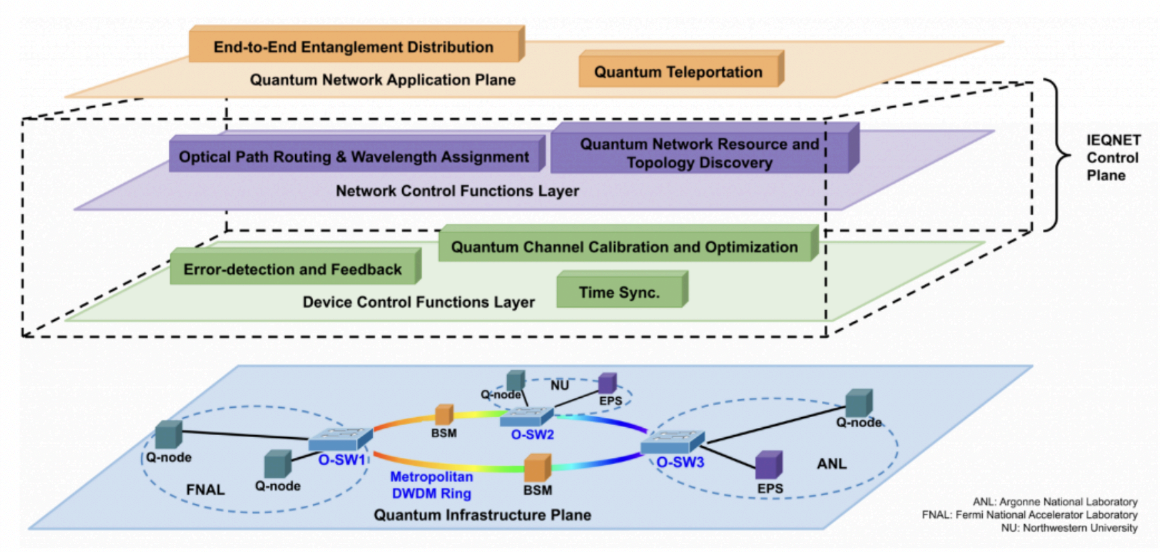
TNO, the Netherlands organization for applied scientific research has announced collaborating with Airbus Central Research and Technology to contribute to the Quantum Internet for advancing quantum communications and networking.

Oak Ridge National Lab, in the US, is creating quantum key distribution technologies as well as developing the fundamental building blocks for realizing quantum sensor networks, quantum repeaters and ultimately, a future quantum internet.

Fermi National Lab, in the US, is working on a control panel to enable a quantum internet. (see Figure 8)[29] Fermi also received funding from the Department of Energy for developing a nationwide quantum network through the Advanced Quantum Networks for Scientific Discovery (AQNET-SD) project[30]. AQNET-SD researchers are working to develop several technologies and protocols to establish and optimize a quantum network between Fermilab and Argonne National Laboratory using quantum-encoded photons, the particles that transmit quantum information. Also included in this project are University of Illinois at Urbana-Champaign and Northwestern University.

[29] https://news.fnal.gov/2023/02/nobel-winning-experiment-enables-fermilab-led-quantum-network/
[30] https://news.fnal.gov/2023/10/fermilab-receives-doe-funding-to-further-develop-nationwide-quantum-network/

Figure 8: Illinois-Express Quantum Network, or IEQNET, led by Fermilab



IEQNET's quantum networking architecture relies on three planes: an infrastructure plane (connectivity of physical devices), a control plane (control of individual devices and the network as a whole), and an application plane (end-to-end networking services). Image: IEQNET

Challenges Facing Quantum Networking and Communications

Despite its promise, quantum networking and communications technologies face several challenges. Many are similar to challenges facing quantum computing and sensing, but others are unique such as the need for long-range quantum entanglements required for advanced quantum networking and communications infrastructures to be operationally deployed.

Scalability: Developing scalable quantum networks requires overcoming significant technical hurdles, including the integration of quantum components and the development of robust quantum repeaters and memory.

Error Correction: Quantum systems (computing, sensing, communications and networking) are highly susceptible to errors due to decoherence and other quantum noise. Developing effective quantum error correction methods is essential for reliable quantum communication. Intentional introduction of noise is also a potential attack vector given the extreme sensitivity to noise. Ability to prevent noise and distinguish natural noise from artificial noise is important. Characterization of noise is critical for QKD /QRNG applications since the 'noise' is actually a desirable aspect. There are advancements in error correction being made by industry and researchers, but a full-error corrected system is still many years away.

Standardization: As the field is still in its infancy, there is a need for standardization in quantum networking protocols and hardware to ensure interoperability and widespread adoption.

Advancements are needed in the quantum networking architecture technologies as well, those include:

Quantum Teleportation: Quantum teleportation[31] is a process by which the state of a qubit can be transmitted from one location to another, without physically transferring the qubit itself. This is achieved using entanglement and classical communication. It's a fundamental protocol for quantum networking, enabling the transfer of quantum information over long distances. This is still nascent technology in the R&D phase. In 2023, researchers were able to teleport quantum information from a photon to a solid-state qubit over a distance of 1km,[32] but longer distances need more advancements in technology.

Photonics and Optical Fibers: Quantum networks often rely on photonics, utilizing light particles (photons) to transmit qubits through optical fibers. There have been some advances in photonic technology[33] but additional scientific breakthroughs are vital for developing practical and scalable quantum networks.

Entanglement Swapping: Entanglement swapping is a technique used to create entanglement between two qubits that have never directly interacted. This is crucial for extending the range of quantum networks, as it allows for the creation of long-distance entanglement by linking shorter entangled segments. Due to the fundamental laws of quantum physics, a classical optical repeater can't be used to regenerate a qubit as it travels through a network. Using a quantum repeater will provide an alternate way of solving the problem without violating the laws of quantum physics. Boeing along with partner HRL Laboratories have been working on developing such a device and plan to launch it in a sun-synchronous orbit in a satellite called Q4S, approximately 550 kilometers above Earth by 2026.[34]

Quantum Transducers: Quantum transducers convert quantum information between different physical forms, such as between optical and microwave photons. This is

[31] https://www.nature.com/articles/s42254-023-00588-x
[32] https://timestech.in/science-to-technology-of-quantum-teleportation/#:~:text=Long%2Ddistance%20quantum%20teleportation:%20In,1km%20using%_20multiplexed%20quantum%20memories
[33] https://www.nature.com/articles/s41377-023-01173-8
[34] https://quantumcomputingreport.com/boeing-announces-plans-to-demonstrate-entanglement-swapping-in-orbit/

essential for interfacing quantum processors (typically operating at microwave frequencies) with optical quantum communication channels. Recent progress has notably enhanced their efficiency and bandwidth. For example, efficiencies nearing 80% have been reported.[35]

Node and Link Configuration with Synchronization: Quantum networks consist of nodes (quantum processors or repeaters) and links (quantum channels). The configuration of these elements impacts the network's efficiency, robustness, and scalability. Topological considerations include mesh, star, and ring configurations. In a fully realized quantum network the end computers would be fault-tolerant quantum computers. QuTech is working on realizing an advanced quantum network in the Netherlands with quantum nodes placed at Delft, The Hague, Leiden and Amsterdam.[36] The goal is for these nodes to function as end nodes as well as quantum repeaters. Synchronization in quantum networks involves aligning the timing of quantum operations across nodes. Precise synchronization is crucial for operations like entanglement swapping and quantum teleportation, ensuring coherent interactions between qubits.

Chapter 3: Conclusion a Call to Action to Advance Quantum Networking and Communications

Quantum networking and communications, along with all quantum technologies, has tremendous implications for the future. It will fundamentally change how we secure data, and security in our technology-driven world means everything. Losing that security – and our privacy – can have devastating consequences.

Understanding these advanced technical aspects and supporting research advancements in the different quantum technologies through government programs and public-private partnerships should be a focus on international collaboration of like-minded governments. Enhanced maturity will be enabled through advanced research, involvements in testbed programs to accelerate technological advancements.

Quantum networking holds the potential to revolutionize secure communications and data transfer, with significant implications for national security, scientific research, and advanced technology development. It can provide needed security for critical infrastructure and our financial institutions as well as provide advancements for national security and commercial industries. While challenges remain, ongoing research and development are steadily paving the way for a future where quantum networks play a critical role in our communication infrastructure.

[35] https://www.nature.com/articles/s41566-022-00959-3
[36] https://tu-delft.foleon.com/tu-delft/quantum-internet/the-six-stages-of-quantum-networks/

We recommend that the US government continue to support the advancement of quantum technologies through the National Quantum Initiative Act, and other legislative initiatives. The global supply chain and engagement of quantum technologies also indicates the need for like-minded governments to work together to advance and enhance our security and communications. Lastly, advancing quantum technologies should be through public-private partnerships and should include businesses of all sizes, as many of the innovations within quantum technologies are coming from small, non-traditional government contractors, as well as from larger organizations.