MAY 2026

The Entanglement Edge

U.S. Strategic Priorities in Quantum Networking

Constanza M. Vidal Bustamante, PhD, and Morgan Peirce

CNAS | New Rules

About the Authors

Constanza M. Vidal Bustamante, PhD, is a fellow with the Technology and National Security Program at the Center for a New American Security (CNAS), where she leads the Center's quantum policy research. Her work examines the intersection of quantum technologies with U.S. national and economic security and currently focuses on the supply chains, manufacturing capacity, and deployment infrastructure needed to scale and sustain the United States' quantum competitiveness.

Vidal Bustamante is also an adjunct professor at Georgetown University's Walsh School of Foreign Service. Prior to CNAS, she was a science and technology policy researcher at the National Academies of Sciences, Engineering, and Medicine and at the Belfer Center for Science and International Affairs, where she led research on the domestic and international dynamics shaping the United States' strategy for technology leadership, digital technology governance, and semiconductor workforce development.

Vidal Bustamante's analysis has been published and featured in Just Security, *The Washington Examiner, Politico, Nature, ChinaTalk,* and Inside Defense. She holds doctoral, master's, and bachelor's degrees from Harvard University.

Morgan Peirce is a former research assistant for the Technology and National Security Program at CNAS, supporting the Center's research on quantum technology and cybersecurity. Before CNAS, Peirce was a fellow at the U.S. Indo-Pacific Command's Strategic Planning and Policy Directorate, where she focused on Northeast Asia. Peirce researched policy and technology at the Congressional-Executive Commission on China, the Center for Strategic and International Studies, and the National Committee on U.S.–China Relations. Previously, Peirce was a senior program associate on the China, Hong Kong, and Taiwan portfolios at the International Republican Institute. Peirce has published work in The Diplomat, *The National Interest*, and New Perspectives on Asia. She holds a master's degree in Asian Studies from Georgetown University's Walsh School of Foreign Service and a BA in government and East Asian languages from Smith College. Peirce lived and studied in China and has advanced Chinese language skills.

About the Technology and National Security Program

The CNAS Technology and National Security Program produces cutting-edge policy research to secure America's edge in emerging technologies while managing potential risks to security and democratic values. The program produces bold, actionable recommendations to drive U.S. and allied leadership in responsible technology innovation, adoption, and governance.

The Technology and National Security Program focuses on three high-impact technology areas: artificial intelligence, biotechnology, and quantum technology. It also conducts cross-cutting research to strengthen U.S. technology partnerships to promote secure, resilient, and rights-respecting digital infrastructure and ecosystems abroad. A focus of the program is convening the technology and policy communities to bridge gaps and develop solutions.

Acknowledgments

The authors thank Brandon Rodenburg, Julián Martínez-Rincón, Vivek Chilukuri, and Maura McCarthy for their valuable feedback and suggestions on earlier drafts of this report. They are also grateful to the dozens of experts in government, industry, and academia who participated in quantum technology roundtables at CNAS or who agreed to be interviewed as part of this research project. The authors also thank their CNAS colleagues Melody Cook and Caroline Steel for design and editing support. This report was made possible with the generous support of the Carnegie Corporation of New York.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues, and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

Table of Contents

01 Executive Summary

03 Introduction

04 Core Concepts in Quantum Networking

06 Quantum Networking Applications: Promise, Limitations, and Status

12 Technical Requirements and Challenges

15 A Comparative Assessment of U.S. and Chinese Ecosystems

21 Recommendations

24 Conclusion

25 Appendix

Executive Summary

QUANTUM NETWORKING—technologies that transmit quantum states between nodes—is an underappreciated but potentially consequential dimension of U.S.-China quantum competition. If harnessed at scale, quantum networking could accelerate the path to useful quantum computers by linking processors into more powerful systems; enhance the precision of sensors critical to navigation, surveillance, and scientific discovery; and potentially secure sensitive communications against eavesdropping. In practice, however, quantum networking remains nascent and far from delivering on this potential. Some first-generation versions are commercially available but substantially limited in capability, while the more advanced applications are still confined to research and early prototypes. Distinguishing between diverse quantum networking technologies—in both their maturity and strategic value—is critical for evaluating and strengthening the United States' position in this field.

DISTINGUISHING BETWEEN DIVERSE QUANTUM NETWORKING TECHNOLOGIES—IN BOTH THEIR MATURITY AND STRATEGIC VALUE—IS CRITICAL FOR EVALUATING AND STRENGTHENING THE UNITED STATES' POSITION IN THIS FIELD.

This report assesses the national security and economic implications of quantum networking, compares U.S. and Chinese strategies and progress, and offers recommendations to sustain U.S. leadership in high-impact applications. It analyzes application areas in secure communications (specifically quantum key distribution, or QKD), distributed quantum computing, and distributed quantum sensing, along with their technical requirements. Its findings underscore that quantum networking is not a single technology but a set of distinct use cases with different value propositions, timelines, and infrastructure needs, demanding a discerning policy approach.

Key Findings

Linking quantum computing modules within data centers is the most pressing and consequential application of quantum networking. Quantum computing companies across hardware modalities identify modular interconnections—links enabling separate processors to function as a single, more powerful system—as essential for scaling to the performance levels needed for high-impact applications from materials discovery to cryptanalysis. Unlike other quantum networking applications, whose value remains more speculative or niche, modular quantum interconnects are critical to realizing the economic and national security potential of quantum computing itself.

Longer-distance quantum networking applications present narrower use cases and harder technical requirements. Scaling quantum computing is more efficiently achieved within a local facility. Entangling sensors may not justify the overhead relative to enhancing individual quantum sensors or their classical networks. Next-generation communications protocols, while improving on early QKD, remain incomplete cybersecurity solutions whose cost relative to classical alternatives likely confines adoption to very narrow scenarios. All three domains also demand high-performing infrastructure—including quantum repeater architectures, exacting timing and synchronization, and extensive fiber or space-based deployments—beyond what data center–scale interconnections require.

QKD is at best a potential niche complement to post-quantum cryptography (PQC), not a replacement for it. The National Security Agency and several allied cybersecurity agencies have concluded that QKD's practical limitations—including implementation vulnerabilities, distance constraints, costly specialized infrastructure, and its inability to provide authentication—make PQC the primary solution for mitigating the threat of

quantum computers capable of breaking current encryption tools. Even China, the world's strongest QKD proponent, began developing its own PQC standards in 2025, and a prominent government advisory body separately acknowledged that PQC can meet security requirements in most scenarios. No country is pursuing QKD as its sole or even primary approach to secure communications.

China leads in first-generation quantum networking deployment, but that infrastructure does not automatically translate into readiness for higher-impact quantum networks. China operates over 10,000 km of QKD fiber across 80 cities, complemented by satellite-based demonstrations, providing a foundation of infrastructure and technical expertise it can build on as next-generation technology matures. However, next-generation quantum networks for distributed computing and sensing impose far greater technical requirements across enabling hardware, performance, and synchronization, which first-generation QKD infrastructure cannot meet.

The United States holds substantial assets, but its position is not self-sustaining. A growing ecosystem of leading researchers and companies—backed by substantial federal research and development (R&D) support as well as private capital—is making strides toward high-value quantum networking applications in computing, sensing, and communications. The U.S. government has avoided overcommitting to first-generation applications of limited strategic value, instead prioritizing next-generation technologies with high economic and security returns. However, additional steps could help the United States reap greater benefits from these investments.

Key Recommendations

1. Develop standard definitions, performance benchmarks, and assessments of quantum networking applications to enable rigorous evaluation of utility, progress, and capability gaps across applications and to sharpen the objectives and reduce redundancy across federally funded programs.

2. Accelerate quantum interconnects for scalable quantum computing within data centers as the most pressing quantum networking priority, expanding programs like the Defense Advanced Research Projects Agency's Heterogeneous Architectures for Quantum and complementary efforts at the national labs, the National Science Foundation, the National Institute of Standards and Technology (NIST), and other federal entities to advance critical components including quantum interfaces, memories, and single-photon sources and detectors.

3. Maintain a calibrated R&D portfolio for longer-distance quantum networking, sustaining an effective testbed ecosystem that generates decision-relevant evidence on entanglement-distribution performance, component integration, and comparison against classical alternatives without overcommitting to applications that may not materialize.

4. Secure enabling technologies' supply chains and infrastructure with spillovers beyond quantum networking, including photonic integrated circuits, precision timing systems, ultralow-loss fiber, and specialized materials where foreign dependencies or other gaps pose cross-cutting risks to quantum, communications, and defense sectors.

5. Accelerate post-quantum cryptography migration at home and coordinate with allies abroad, ensuring timely adoption of NIST PQC standards across government, critical infrastructure, and the private sector while working to prevent divergent allied approaches from creating interoperability risks for shared military and civilian systems.

Introduction

QUANTUM TECHNOLOGIES ARE A CRITICAL and intensifying arena of U.S.-China competition, with significant implications for national and economic security. Quantum computers could eventually transform drug discovery, materials science, and cryptanalysis, while quantum sensors are already advancing into early military deployments for high-precision navigation and timing. Across these domains, the United States retains important scientific and industrial advantages, but dominance is not guaranteed and the competitive landscape is evolving rapidly.

Quantum networking—technologies transmit quantum states between nodes—are a less known but potentially consequential dimension of this competition. Unlike classical networks, which move ordinary digital data, quantum networks carry signals that cannot be copied or intercepted without detection and can establish a strong correlation between distant particles—known as entanglement—that has no equivalent in classical physics. If harnessed at scale, quantum networking could accelerate the path to useful quantum computers by linking processors into more powerful systems; enhance the precision of sensor networks critical to navigation, monitoring, and scientific discovery; and potentially secure government and military communications.

In practice, quantum networking remains far from delivering on this potential. Early versions of the technology—referred to in this report as first-generation or "quantum networking 1.0," most notably quantum key distribution (QKD)—are commercially available but limited in capability. Next-generation or "quantum networking 2.0" architectures would distribute entanglement as a shared resource to support a broader range of applications, including linking quantum computing processors or sensors into more powerful systems and enhancing communications protocols with stronger security guarantees. However, these applications still require major technical advances, and whether they will deliver real-world utility given the difficulty and cost of implementation remains an open question. Distinguishing between these generations of technology, both in their maturity and their potential strategic value, is critical for evaluating the United States' quantum networking strategy.

China and the United States have taken divergent approaches. China has pursued large-scale QKD deployment and is also investing in entanglement-distribution technologies, positioning itself to compete across both generations of quantum networking. The United States has taken a restrained posture, deprioritizing QKD in favor of next-generation entanglement-distribution research, though with less federal spending than in quantum computing and sensing. U.S. policymakers must decide whether their restraint in pursuing quantum networking is strategically prudent or risks ceding capabilities that could prove critical as quantum technologies mature.

U.S. POLICYMAKERS MUST DECIDE WHETHER THEIR RESTRAINT IN PURSUING QUANTUM NETWORKING IS STRATEGICALLY PRUDENT OR RISKS CEDING CAPABILITIES THAT COULD PROVE CRITICAL AS QUANTUM TECHNOLOGIES MATURE.

This report seeks to inform that decision. Following an introduction to core quantum networking concepts, it assesses the promise, limitations, and technical foundations of applications in secure communications, distributed quantum computing, and distributed quantum sensing, and examines the enabling components and infrastructure each requires. It then compares U.S. and Chinese strategies, programs, and industrial bases, and concludes with targeted policy recommendations to sustain U.S. leadership in the quantum networking applications most likely to deliver strategic value.

Core Concepts in Quantum Networking

UNDERSTANDING THE STRATEGIC VALUE and outlook of quantum networking technologies requires first establishing two foundational distinctions: how quantum networks differ from classical ones, and what separates early generations of quantum networking from the more advanced emerging architectures. These distinctions shape the capabilities, infrastructure requirements, and maturity of the applications assessed in subsequent chapters and are essential for evaluating where to prioritize U.S. attention and investment.

Quantum networks differ fundamentally from classical networks in both capability and technical complexity. Classical communications networks move information—typically as binary bits via optical fiber—in a form that can be copied, amplified, and retransmitted without fundamental limits, allowing signals to travel long distances without significant degradation. In contrast, quantum networks distribute quantum states or entanglement. Because these states are fragile and are disturbed or destroyed when measured, they enable unique capabilities but are also far harder to build and operate.

Quantum networking generations differ substantially in their strategic value, maturity, and implementation requirements—distinctions that are central to evaluating where to prioritize U.S. investment and attention.

Quantum networking 1.0 encompasses direct quantum communication links between two endpoints. The most mature example is QKD, in which one party sends quantum-encoded signals to another to securely agree on a shared secret key that can then be used to encrypt communications. Because eavesdropping disturbs the signals in detectable ways, the two parties can verify whether their channel was compromised. QKD systems are commercially available today but face significant practical constraints, including limited range and hardware-related security vulnerabilities.

Quantum networks distribute quantum states or entanglement. Because these states are fragile and are disturbed or destroyed when measured, they enable unique capabilities but are also far harder to build and operate.

Quantum networking 2.0 architectures go further by distributing entanglement as a shared resource that multiple devices can draw upon and replenish on demand, unlocking a much broader range of strategic applications. When two nodes share entanglement, they can perform coordinated quantum operations that would not be possible with classical communication alone. Entanglement can serve as a security guarantee that bypasses any assumptions about hardware security, a key

Essential Quantum Networking Concepts

Qubits, superposition, and measurement: A qubit is the essential unit of quantum information. Where a classical bit takes a definite value of either 0 or 1, a qubit exists in a superposition of both states, meaning it has some probability of being in either state when measured. In quantum networking, qubits are often encoded into photons, or light particles, so they can be transmitted across nodes over optical channels such as fiber. Quantum states are fragile, and measurement inevitably disturbs them—a property that quantum communications protocols exploit to detect eavesdropping.

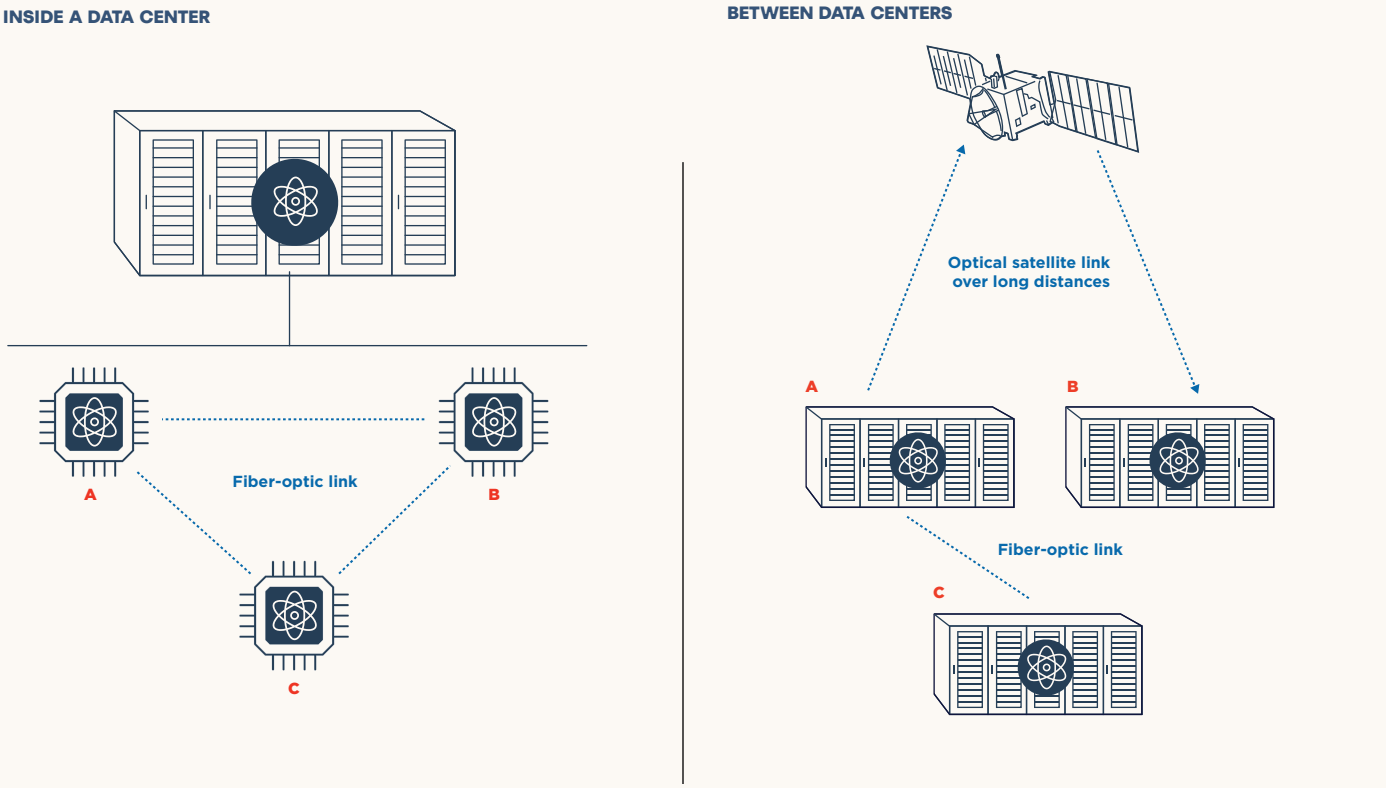
Entanglement: A quantum correlation between two or more qubits, such that measuring one instantly determines the properties of the others, regardless of distance. Entanglement is not a communication channel itself, but a resource that can be distributed across network nodes to enable joint measurements, coordinated quantum operations, and detection of eavesdroppers.

Entanglement distribution or "swapping": A protocol that extends entanglement across longer distances without physically transmitting quantum states end to end. The protocol first establishes shorter entangled links between neighboring nodes. At each intermediate node, a special joint measurement over two photons—one from each adjacent entangled link—transfers the entanglement to the endpoints of those links. Repeating this process across a chain of nodes extends entanglement to distant endpoints that never directly exchanged quantum signals. This is the core mechanism enabling quantum repeaters and scalable long-distance quantum networks.

Quantum repeaters: These are not devices themselves, but proposed protocols that, once implemented, would use successive rounds of entanglement swapping to distribute entanglement over long distances while suppressing the exponential signal losses in optical fiber. Quantum repeater systems rely on multiple specialized devices, including entanglement sources, quantum memories to store states while adjacent links succeed, single-photon detectors, and tight classical synchronization.

Figure 1 | Quantum Networking Connects Diverse Nodes Across Varying Scales and Link Types to Enable Strategic Applications

Quantum networks 2.0 distribute entanglement between nodes, establishing a shared resource that enables joint computation, coordinated measurement, or secure communications across distant devices. Nodes can be quantum computing chips or processing units, quantum sensors, or photon detectors, and links between them can traverse optical fiber or free-space channels, including terrestrial and satellite paths. The scale and infrastructure demands vary significantly by application. For example, data center–scale modular quantum computing (left) connects chips or processors within a single facility over short fiber links to form a more powerful computer and represents the most pressing and nearest-term quantum networking use case. Geographically distributed quantum computing (right) would connect devices via long-distance fiber or satellite links for niche purposes such as privacy-preserving access to remote quantum computers, but faces severe compounding signal loss over distance and requires quantum repeater architectures that have not yet been demonstrated.



Individual quantum computing chips or processors networked with each other via entanglement for joint computation inside a data center, forming a more powerful quantum computer.

Quantum computers networked with each other via entanglement for joint computation across facilities.

vulnerability of existing QKD systems. Connected quantum computing chips or processing units can act as a coordinated machine, potentially enabling the kind of fault-tolerant quantum computing that could enhance the discovery of new materials or break encryption. And entangled networks of quantum sensors could achieve measurement precision that no individual sensor could reach alone, further boosting navigation and scientific discovery. However, the theoretical capabilities of quantum networking 2.0 applications come with substantially harder technical requirements, as discussed in subsequent chapters.

Differences between classical and quantum networks and across quantum networking generations reveal a landscape of technologies that vary widely in their theoretical value and technical readiness. The next chapter provides a deeper examination of applications across communications, distributed quantum computing, and distributed quantum sensing to assess their potential utility, inherent limitations and challenges, and current maturity.

Quantum Networking and the Limits of the Internet Analogy

A note on terminology: The "quantum internet" is a catchy concept that has attracted significant attention to quantum networking, but whose inconsistent use risks misallocating scarce policy attention and resources. This term is often used interchangeably with any form of quantum networking, and in other cases, it is used more narrowly to describe an aspirational network of networks distributing quantum states across local, national, and global scales.[1]

The term quantum internet invites a direct but misleading comparison to the classical internet. The classical internet is a global, general-purpose network that distributes readable information, stores and replicates it across servers worldwide, and grows more useful as more people join it. Quantum networks differ fundamentally, as quantum information cannot be broadcasted or copied. What quantum networks distribute instead is entanglement, which is not information per se, but a shared physical *resource*: a fragile correlation between the endpoints that can be spent to generate shared encryption keys, perform joint computations, or synchronize distant sensors. Entanglement can only be used once, must be actively replenished, and yields value only when combined with local quantum operations and classical communication.

Quantum networks are therefore unlikely to be global and open like the classical internet. They require specialized hardware, high-precision timing and synchronization, and tightly controlled environments. Most near- and medium-term value arises in carefully scoped applications where users, infrastructure, and performance requirements are well defined, such as linking quantum processors within a data center or enabling precision sensing over a specific geographic area.

This report therefore avoids the term "quantum internet" and instead treats quantum networking as a set of enabling technologies whose most plausible value lies in narrow, high-consequence applications within carefully engineered networks.

Quantum Networking Applications: Promise, Limitations, and Status

QUANTUM NETWORKING APPLICATIONS VARY WIDELY in their value propositions and maturity, with implications for their relative prioritization and support. This chapter examines three primary applications—quantum key distribution, distributed quantum computing, and distributed quantum sensing—assessing each for their potential, current and inherent limitations, and development status.

- **Post-quantum cryptography (PQC) remains the primary solution for mitigating the encryption-breaking potential of future quantum computers.** PQC refers to a new set of classical cryptographic standards whose underlying math is not vulnerable to quantum computers. PQC is the only scalable, near-term approach to securing systems against quantum computers and is the recommended path across U.S. and allied cybersecurity agencies.
- **Quantum key distribution (QKD) is a potential niche complement, not an operational solution or a replacement for PQC.** Both legacy and emerging QKD systems remain incomplete security solutions with persistent hardware, integration, and scaling challenges.
- **Selective investment in device-independent (DI)-QKD research can yield strategic spillovers.** DI-QKD is significant not as a near-term security solution but because it can drive progress in the technical capabilities needed for next-generation quantum networks, including for scalable quantum computing and enhanced quantum sensing. It can also serve as a proxy for tracking international quantum networking capabilities.

Quantum Key Distribution

Quantum communications encompass technologies that use quantum properties to transmit information with security guarantees rooted in physics rather than computational assumptions. Although foundational work in this area predates concerns about quantum computing, the discovery that sufficiently powerful quantum computers could break widely used public-key cryptography, and therefore expose sensitive government and commercial data, has renewed interest in quantum-based approaches to securing communications.[2]

Today's public-key cryptography relies on mathematical problems that are intractable for classical computers but which could be solved efficiently by a powerful quantum computer.[3] To mitigate this threat, the U.S. government has prioritized the development of and transition to PQC, a software-based approach deployable through existing infrastructure that relies on alternative mathematical problems believed to be resistant to both classical and quantum attacks.[4]

Quantum communications offer a fundamentally different approach. Instead of relying on computational difficulty, quantum cryptographic protocols use quantum effects—such as measurement disturbing quantum information—to detect intrusions and achieve information-theoretical security; this means that under the protocol's assumptions, security does not depend on an adversary's computational capabilities.[5] However, these protocols still require classical authentication between endpoints, a limitation that qualifies the claim of unconditional security.

The most mature and widely deployed quantum communications application is QKD, which enables two parties to generate a shared secret key. Researchers and companies are also exploring other quantum-enabled security applications, such as position verification and digital signatures, but these remain at an early research stage.[6] Existing commercial QKD systems fall under what this report calls quantum networking 1.0, in which a sender prepares quantum states in photons and a receiver measures them over a direct optical link, usually fiber. Any third-party attempt to intercept the transmitted quantum signals introduces detectable errors. If the error rate falls below a defined threshold, the parties can distill a shared secret key with provable security guarantees that can then be used in conventional encryption schemes.

QKD's Current and Inherent Limitations

Despite strong theoretical security claims, QKD presents several constraints, limiting its practical deployment. The National Security Agency (NSA), in guidance first issued in 2020 and reaffirmed in 2024, stated that it "does not generally consider QKD a practical security solution" for national security systems.[7] Several allied governments—including the United Kingdom, Australia, Canada, France, Germany, and Singapore—have issued similar statements, recommending PQC as the primary cryptographic solution to mitigate the threats of quantum computers (see Table A1 in the appendix).[8]

These expert assessments reflect QKD's current and inherent limitations:

- **QKD is an incomplete cybersecurity solution.** It generates encryption keys but does not provide authentication, endpoint security, or protection against application-layer threats, all of which must still be addressed through classical systems.
- **Distance and scaling remain constrained.** Quantum signals attenuate rapidly in optical fiber, and extending the range typically requires trusted relay nodes that reintroduce classical security vulnerabilities.
- **Implementation vulnerabilities undermine theoretical guarantees.** Demonstrations of side-channel attacks on commercial QKD systems—in which an adversary extracts key information by exploiting hardware imperfections like detector timing or photon-emission patterns, rather than breaking the underlying protocol—undermine claims of QKD's "absolute" or "unconditional" security.[9]
- **Links are susceptible to disruption.** The sensitivity of quantum signals makes QKD systems vulnerable to denial-of-service attacks that can interrupt key generation.
- **Deployment requires specialized infrastructure.** QKD requires dedicated hardware and integration, adding operational complexity and cost relative to software-based classical alternatives that can be deployed on existing digital networks.

Recent progress in PQC development, combined with the growing urgency to complete migration before quantum computers can break current encryption, exacerbates QKD's comparative limitations. Following an eight-year international process led by the National Institute of Standards and Technology (NIST), the United States finalized its first PQC standards in 2024.[10] The transition is expected to take several years and cost billions of dollars in the United States alone, reinforcing the need for scalable, deployable solutions.[11] U.S. and allied cybersecurity agencies have issued guidance prioritizing the migration of high-value systems by 2030 and most other systems by 2035, especially as the capabilities of quantum computers accelerate.[12]

> Allied governments that actively support QKD R&D still recognize that this technology requires substantial technical advances before it can provide reliable security.

Yet countries have diverged in their subsequent treatments of QKD. U.S. agencies have generally deprioritized QKD research and deployments, instead prioritizing PQC for quantum-safe cryptography and quantum networking 2.0 applications that seek to connect quantum computers or quantum sensors. By contrast, China and several other countries continue to invest heavily in QKD, including countries whose cybersecurity authorities have pointed out its technical limitations (see Table A1 in the appendix).

Increasingly, vendors frame QKD not as an alternative to PQC but as a complement for high-value connections—such as those linking financial institutions, government agencies, or critical infrastructure—that may warrant an additional layer of security should PQC algorithms prove vulnerable. However, since QKD itself relies on classical encryption to authenticate the communicating parties, a development that breaks PQC would also undermine the authentication on which QKD depends.

Moreover, allied governments that actively support QKD R&D still recognize that this technology requires substantial technical advances before it can provide reliable security. Beyond its direct applications, continued investment in QKD may also reflect its perceived value as a near-term pathway for building quantum networking infrastructure, technical expertise, and operational experience that could support more advanced quantum technologies in the future, even if QKD itself is not useful to secure communications.[13]

Emerging QKD Protocols and Their Significance Beyond Communications

Emerging QKD protocols aim to reduce reliance on trusted hardware while preserving the goal of secure key establishment. In this context, a "trusted" device is one that must be physically secured and assumed to behave as intended, as a compromise could expose the key. First-generation systems depend heavily on this assumption, particularly for signal detectors. Newer approaches modify the underlying trust model so that certain components no longer need to be trusted, meaning a compromise at those points cannot leak key material.

Measurement-device-independent (MDI)-QKD—and a variant called twin-field QKD—enables both parties to send quantum states to a central relay that performs a joint measurement and publicly announces limited information about how the signals relate to each other, not their actual values.[14] Using this information and their own records, the parties can establish matching key bits. Because the relay never learns the key itself, it does not need to be trusted, eliminating a major class of detector-based attacks. Several university and federal laboratories in the United States, Europe, and China are pursuing MDI-QKD research.[15]

Device-independent (DI)-QKD pushes security furthest by removing the need to trust the internal functioning of quantum devices altogether. Instead, its security is based solely on observed quantum correlations between measurement outcomes. Unlike the protocols covered above, DI-QKD relies on establishing entanglement between the communicating nodes and performing statistical tests to verify that no eavesdropper could have prior knowledge of the key.

Recent experimental progress reveals both promise and remaining challenges. In February 2026, a team at the University of Science and Technology of China (USTC) led by prominent scientist Pan Jianwei demonstrated DI-QKD over 100 km of fiber, achieving key rates at distances relevant to real-world metropolitan networks for the first time.[16] These results reflect significant progress with no comparable demonstrations in the United States, though key-generation rates remain far below operational requirements, and extending performance to longer distances will require further advances in entanglement quality and generation rates.

Despite these advances, emerging QKD protocols leave unresolved many of the core limitations identified by the NSA and others. They remain mechanisms for the distribution of keys rather than complete security solutions, still depend on classical encryption for authentication, require highly specialized devices and infrastructure, and face significant technical barriers before they can deliver reliable, large-scale deployments.

Critically, however, the significance of DI-QKD extends beyond cryptography. Its technical requirements—including high-quality entanglement distribution, quantum memories, and entanglement swapping—are also foundational for long-distance networks of quantum computers or sensors. Progress in DI-QKD could therefore serve as a stepping stone toward quantum networking 2.0, making it a strategic near-term benchmark for the field.

Distributed Quantum Computing

- **Modular quantum computing within single facilities is the highest-priority application of quantum networking.** Linking processors within data centers is increasingly viewed as a necessary path to scaling useful quantum computers and currently is far more mature and strategically compelling than longer-distance distributed computing.
- **The main bottlenecks for modular quantum computing vary by hardware modality, but all approaches require significant further development.** Trapped-ion and neutral-atom systems need faster and more efficient optical connections between processors; superconducting systems face engineering constraints in scaling cryogenic microwave links and, potentially, unresolved microwave-to-optical conversion; and photonic systems must reduce optical loss across the entire system. Across modalities, component integration, real-time classical control systems, and supporting infrastructure also require advances.
- **Geographically distributed quantum computing is a narrower, longer-term application.** Its most credible uses include secure remote access and federation of scarce resources at distant facilities, but it depends on technically challenging repeater-grade capabilities that remain immature.

Quantum computing holds promise for applications in chemistry, materials science, optimization, and cryptanalysis, with important economic and security implications. However, building quantum processors large enough to deliver real-world utility remains a central challenge across hardware modalities. Every approach faces physical and engineering limits on how many qubits can be reliably controlled within a single processor before error rates, fabrication yields, or control complexity degrade performance. Quantum networking offers a path to fault-tolerant computation by connecting multiple smaller, high-quality quantum processors via entanglement to operate as

a single, more powerful system. This is similar to how classical supercomputers derive their power from networking many processors rather than scaling up a single chip.

Distributed quantum computing is envisioned at two levels: data center–scale modular quantum computing and geographically distributed quantum computing. These differ significantly in their current strategic importance as well as in their technical requirements and maturity. Data center–scale quantum interconnects represent a practical pathway to unlocking useful quantum computing and its associated economic and security advantages, while longer-distance distributed quantum computing remains a more specialized and longer-term prospect.

Modular Quantum Computing Within Data Centers

The most pressing and widely supported application of quantum networking is for modular quantum computing within a single facility or data center, at distances ranging from meters to perhaps a few kilometers. In this approach, multiple smaller processors or modules are linked via specialized hardware, known as quantum interconnects, so they can function as one logical machine, enabling fault-tolerant, utility-scale quantum computing.

Making separate processors work together requires establishing entanglement between them. Each joint operation across processors consumes an entangled connection, so the system must generate these connections both quickly and at high quality. Two key metrics define interconnect performance: rate—how many successful connections are produced per second—and fidelity—how closely each connection matches the ideal. Experts estimate that fault-tolerant operation requires tens of thousands to millions of connections per second, depending on processor speed and error-correction scheme, at fidelities above 98 or 99 percent.[17] Meeting these thresholds depends on the quantum interconnects themselves as well as fast classical control systems to coordinate timing, confirm successful connections, and manage errors. The implementation pathway varies by hardware modality, and connecting processors across different modalities is a longer-horizon goal.

Data center–scale quantum interconnects represent a practical pathway to unlocking useful quantum computing and its associated economic and security advantages, while longer-distance distributed quantum computing remains a more specialized and longer-term prospect.

Trapped-ion systems are the most advanced experimentally in photonic modular interconnects. Recent work has demonstrated quantum computations across two optically linked processors with connection quality reaching 97 percent of the theoretical ideal, and leading companies are targeting interconnected modules by 2028.[18] A central remaining challenge is speed: Less than 1 percent of connection attempts succeed due to optical loss at various steps, and because each cross-processor operation consumes a successful connection, current rates can be several hundred times too slow for fault-tolerant computation.[19] Approaches to closing this gap include improved optics to capture more of each qubit's emitted light, adding intermediate memory nodes that allow each side of a connection to succeed independently, and running multiple connection attempts in parallel.[20] Additionally, ions and most neutral atom species emit visible-wavelength light that suffers high loss in optical fiber, requiring conversion to telecommunications wavelengths even over short distances. This conversion has been demonstrated but introduces additional signal loss.[21]

Like trapped ions, neutral-atom platforms use atom-based qubits and could in principle be linked through optical connections.[22] Their potential advantage is the ability to support large numbers of qubits in flexible arrangements within a single processor, which extends the in-processor scaling runway considerably further than for other modalities, though modular operation will likely remain important at utility scale.[23] However, they remain at an earlier developmental stage than trapped ions in demonstrating networked computing between separate processors. Neutral atoms interact weakly with light in open space, making it difficult to extract photons reliably. Overcoming this will likely require specialized optical hardware to concentrate and redirect the atom's light emission, and while some companies are developing such hardware, it has not yet been integrated with operational processors.[24]

Superconducting systems face interconnection challenges that vary with distance. Industry roadmaps envision scaling superconducting systems by first linking multiple chips within a shared cryogenic refrigerator, then connecting multiple processors across refrigerators using superconducting microwave cables.[25] This approach has been demonstrated at distances approaching one meter, but it requires maintaining the entire connection path at near absolute zero temperatures, constraining how the system can be physically arranged and scaled.[26] At longer distances, superconducting systems would need devices (transducers) that convert quantum signals from microwave to optical frequencies for transmission over fiber. This is a major unsolved engineering challenge that demands high conversion efficiency, extremely low noise, and cryogenic compatibility.[27]

Photonic quantum computing architectures are distinct because the quantum information is already carried by particles of light, making them naturally suited to sending quantum information over optical links.[28] Instead, their main scaling challenges

center on the fact that every lost photon means lost qubit information, disrupting not just a connection between modules but the computation itself. This places stringent demands on the efficiency of photon sources, detectors, and optical switching, as well as on the manufacturing these components at scale.[29]

Several enabling technologies for quantum interconnects are shared across hardware modalities that use optical links, including single-photon detectors, low-loss fiber-optic components, precision timing and synchronization systems, and classical software and control systems that can coordinate operations across processors in real time.

An emerging direction in modular quantum computing is connecting processors of different hardware modalities to combine their respective strengths, such as the fast gate operations of superconducting qubits with the longer coherence times of atom-based systems. A system that combines these strengths could potentially outperform any single modality and offer an alternative path to useful quantum computing. However, this poses substantial difficulties, including bridging fundamentally different physical signals at the hardware level and developing software that can compile and distribute computations across qubit types with very different operating characteristics. The Defense Advanced Research Projects Agency's (DARPA's) Heterogeneous Architectures for Quantum (HARQ) program, launched in 2026, is tackling these challenges.[30]

Geographically Distributed Quantum Computing

A more demanding and longer-term application is connecting quantum processors across data centers at metropolitan, regional, or longer distances. Unlike modular quantum computing within one facility, which aims to scale a single machine, geographically distributed quantum computing would link distant systems for more specialized purposes.

Long-distance networking of quantum computing is not the ideal pathway to scale computing capabilities, as scaling within a single facility is considerably less technically demanding and more efficient in terms of reducing signal loss.[31] Instead, longer-distance links could serve as a work-around to federate scarce or specialized existing quantum resources across institutions when proactive local buildup is not possible. Long-distance quantum networks could also enable niche use cases such as delegated (or "blind") quantum computing, in which users could theoretically run computations on remote quantum processors without revealing their data or computations to the operator.[32]

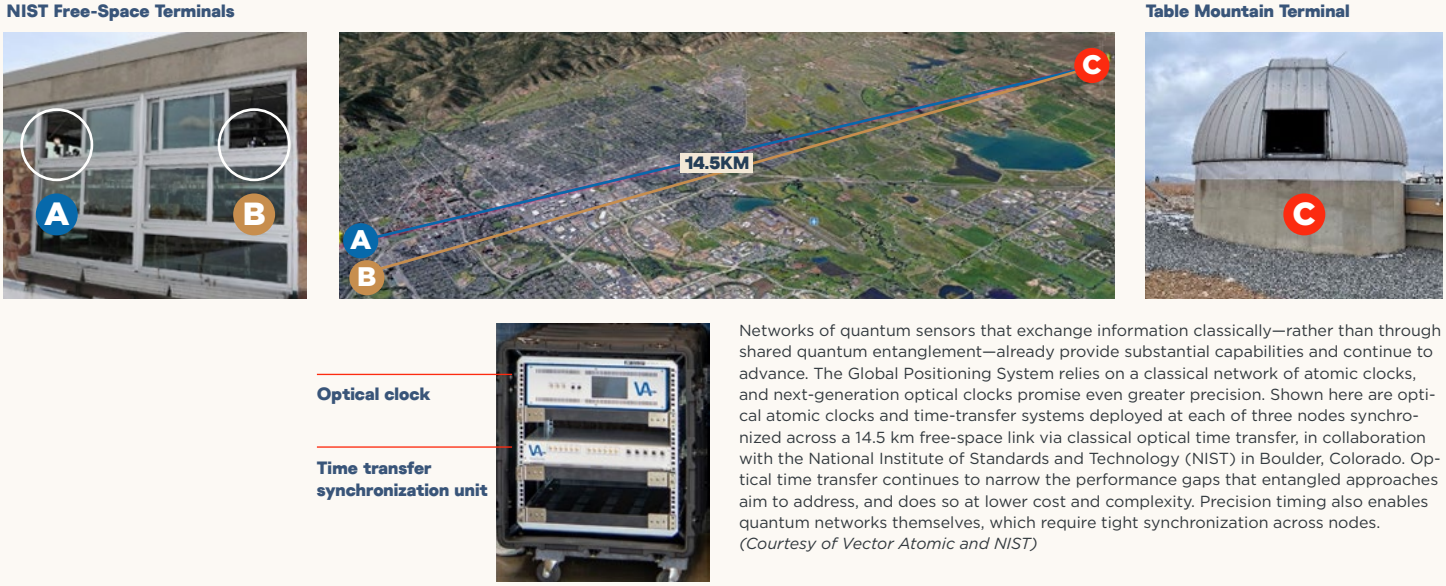
The technical difficulty for long-distance quantum networking is substantially larger than for modular interconnects within a data center. Over tens or hundreds of kilometers, photon loss is exponentially severe, and quantum states cannot be merely amplified like in classical networks. Long-distance distributed quantum computing therefore requires quantum repeater architectures, including quantum memories that can store quantum states long enough to coordinate network operations, processes that allow the sharing of entanglement across intermediate nodes, high-fidelity interfaces with existing optical fiber, and tightly integrated classical control and timing across the network. The U.S. government supports over a dozen quantum network testbeds across the country, making progress on these building blocks for quantum repeaters, but they remain far from operational deployment.

Distributed Quantum Sensing

- **Individual quantum sensors and classical networks of quantum sensors already deliver major strategic value.** Global Positioning System (GPS) and other global navigation satellite systems demonstrate that classical networks of atomic clocks already enable the global distribution of highly precise timing information, underpinning major civilian and defense domains.
- **Distributed quantum sensing has yet to demonstrate practical advantage over these alternatives.** Entangling sensor arrays can theoretically reduce fundamental quantum noise, but real-world sensing environments are typically dominated by environmental noise that entanglement cannot address. In most scenarios, the modest operational benefit is unlikely to justify the substantially greater technical complexity compared to improving the performance of individual quantum sensors, adding more sensors to a classical network, or advancing existing time transfer protocols.
- **The potential value of distributed quantum sensing justifies sustained research and development.** Even incremental improvements in timing and sensing precision could carry significant military and scientific value, making distributed quantum sensing an important area for continued R&D. Targeted experimentation can establish whether entanglement delivers operationally meaningful advantage before scaling resources.

Quantum sensing uses fragile quantum states to measure time, motion, fields, and other physical quantities with exceptional precision, with major applications in fields like navigation, timing, geophysics, and fundamental science.[33] Distributed quantum sensing seeks to extend these capabilities by linking sensors into a coordinated network. Assessing the value of distributed sensing requires distinguishing between classical and quantum networks.

Classical networks of quantum sensors already deliver major benefits. The most prominent examples are GPS and other global navigation satellite systems. These are networks of atomic (quantum) clocks whose outputs are synchronized and combined through classical time transfer and data processing. For decades, atomic clocks have been the gold standard for precision timekeeping, and their classical networking underpins major civilian and military functions, from navigation and logistics to telecommunications and financial trading.



Networks of quantum sensors that exchange information classically—rather than through shared quantum entanglement—already provide substantial capabilities and continue to advance. The Global Positioning System relies on a classical network of atomic clocks, and next-generation optical clocks promise even greater precision. Shown here are optical atomic clocks and time-transfer systems deployed at each of three nodes synchronized across a 14.5 km free-space link via classical optical time transfer, in collaboration with the National Institute of Standards and Technology (NIST) in Boulder, Colorado. Optical time transfer continues to narrow the performance gaps that entangled approaches aim to address, and does so at lower cost and complexity. Precision timing also enables quantum networks themselves, which require tight synchronization across nodes. *(Courtesy of Vector Atomic and NIST)*

Quantum networks of quantum sensors have a different mechanism and goal. They would connect sensors via entanglement, reducing collective noise below what independent sensors can achieve and substantially improving measurement precision.[34] Two applications have attracted the most interest. First, entanglement-based clock synchronization could theoretically improve timing accuracy and resilience against tampering over long distances and in contested environments. Second, entanglement could enhance very-long-baseline interferometry (VLBI), a technique that combines signals from widely separated sensors to create high-resolution images. VLBI is already used classically—for example, it produced the Event Horizon Telescope's first black hole photograph—but entanglement could extend it from radio to optical wavelengths, yielding far sharper resolution. Laboratory research has begun demonstrating the promise of both applications for distributed quantum sensing.[35]

Despite their theoretical promise, quantum networks of sensors remain nascent, and their practical value is unproven. A central limitation is that entanglement only addresses one source of measurement error: It correlates sensors so that fundamental quantum randomness partially cancels across the network. However, in real-world environments the dominant sources of noise hindering precision sensing are environmental, such as seismic vibration, atmospheric turbulence, temperature changes, and geomagnetic fluctuations. In such environments, entanglement-based sensitivity gains may translate into little operational benefit.

Moreover, the technical demands of generating and maintaining entanglement between sensors may outweigh its incremental benefits over near-term alternatives. Quantum networks require reliable entanglement-distribution hardware, stable photonic links, and timing synchronization across nodes to within a trillionth of a second or better (subpicosecond), exceeding what current commercial infrastructure can support.[36] The incremental benefit of entanglement must therefore be evaluated against deploying better individual quantum sensors, using more sensors, or improving classical synchronization and data-fusion techniques.[37] Recent advances in optical atomic clocks and optical time transfer illustrate how alternative techniques continue to close performance gaps that entanglement aims to address.[38] Research demonstrations have achieved subfemtosecond synchronization over hundreds of kilometers, and commercial hardware now delivers femtosecond-level precision in rack-mounted form factors, both at a more favorable cost-to-performance ratio than entanglement-distribution infrastructure.[39]

Nevertheless, distributed quantum sensing via quantum networking could still yield high-impact capabilities in specific domains where even incremental improvements could carry significant military or scientific value. Targeted experimentation in these fields can drive additional improvements and ongoing assessments on whether quantum networking delivers operationally meaningful advantages over alternatives before scaling resources.

Connecting Quantum Sensors and Quantum Computers

An underdeveloped but potentially high-impact application of quantum networking lies in linking quantum sensors directly to quantum computers. Feeding sensor data to a quantum computer in its raw quantum form—rather than first converting it to classical data, which destroys most of the quantum information—would enable substantially more useful information to be extracted from each measurement.[40] Such a capability could be valuable for signals intelligence, where extracting faint signals from noisy environments is a persistent challenge, as well as for scientific domains like materials characterization and biomedical sensing, where extracting meaningful information from limited measurements could be particularly advantageous.

A 2022 proof-of-principle experiment demonstrated this advantage using 40 qubits, requiring roughly 10,000 times fewer experiments than the best classical approach, even on imperfect hardware.[41] However, passing data directly from a quantum sensing device to a computer without first converting it to classical information has not yet been achieved. Quantum sensors and quantum computers typically rely on different physical hardware and operate at incompatible energy scales. Bridging them would likely require codesigning the devices for this purpose, rather than simply attempting to add an interface to existing ones. DARPA's HARQ program, which explores combining distinct qubit modalities into interconnected systems, may yield relevant lessons and could be expanded to tackle sensor-to-computer connections directly.[42]

Technical Requirements and Challenges

THE PREVIOUS CHAPTER ASSESSED THE PROMISE and limitations of specific quantum networking applications. Realizing the highest-impact applications will require continued advances across multiple enabling technologies and techniques. This chapter reviews the components, infrastructure, and cross-cutting challenges involved in quantum networking, identifying where requirements overlap and where they diverge and demand more targeted attention.

- **High-impact quantum networking 2.0 applications share substantial technical overlap with each other but much less with first-generation QKD.** Modular and long-distance quantum computing, distributed sensing, and emerging device-independent QKD all depend on high-rate, high-fidelity entanglement distribution. First-generation QKD shares some physical infrastructure, such as fiber and photon detectors, but does not require entanglement, memories, or the same performance thresholds. Investment in QKD infrastructure does not automatically build readiness for higher-impact 2.0 applications.
- **Signal loss, noise, and errors compound across the technology chain and worsen considerably with distance.** Meeting entanglement requirements for quantum networking 2.0 applications is significantly harder for long-distance networks, which face severe compounding transmission loss and require quantum repeater architectures that have not yet been demonstrated operationally.
- **Both quantum and classical technology layers are critical to operation and require continued advances.** On the quantum side, interfaces, memories, and detectors all need further improvement to maximize connection rates and signal quality. On the classical side, infrastructure including fiber quality, timing systems, and real-time control software is often as decisive for performance as the quantum hardware itself.

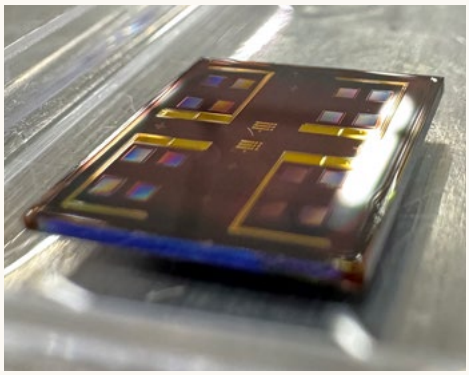
Technical and Infrastructure Requirements

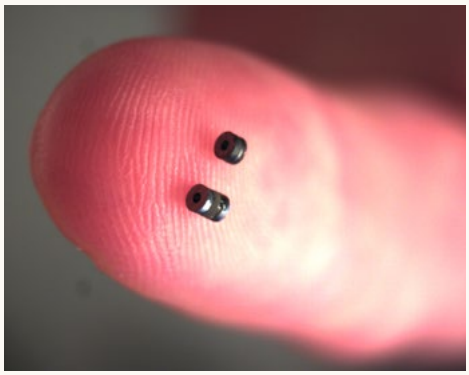
Across quantum networking 2.0 applications, a central objective is to distribute entanglement at high rates (how many usable quantum connections can be produced per second) and high fidelity (how closely each connection matches the ideal), over distances meaningful for the application. Achieving this depends on two connected layers of technology: a quantum layer that generates, processes, stores, and measures quantum states, and a classical infrastructure and control layer that transmits those states and coordinates operations through synchronization, monitoring, and orchestration.[43] Every component in both layers contributes to the end-to-end rate and fidelity of entanglement distribution, and limitations at any single stage can constrain overall performance. Each layer involves components and performance demands that are partly shared across applications and partly specific to each.

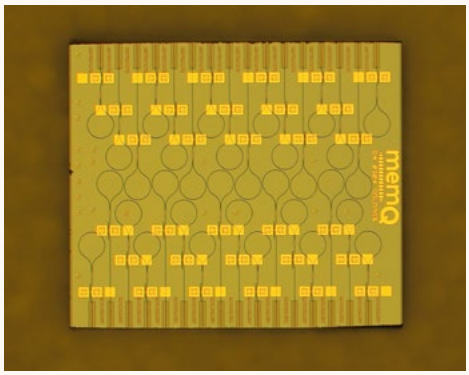
The Quantum Layer

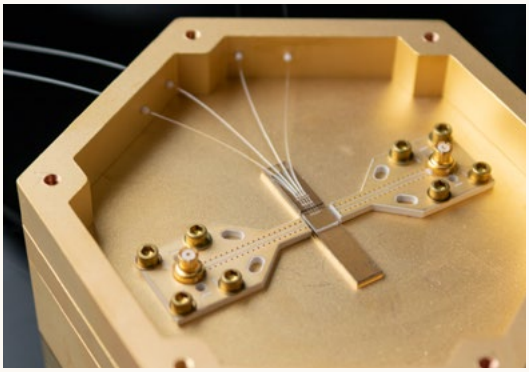
Generating and extracting quantum signals. All quantum networking applications begin with producing quantum states that can travel between nodes. In distributed quantum computing, the signal is typically generated by the computing qubit itself, such as an atom emitting a photon entangled with its internal state or a superconducting qubit emitting a microwave signal. Especially for atom-based systems, capturing that signal efficiently may require specialized devices known as photonic interfaces to enhance photon emission and collection and to couple it into the link that connects the processors. Other approaches, including some distributed computing architectures and quantum communications like QKD, rely on dedicated photon sources to generate quantum signals independently of any computing hardware. In photonic quantum computing, integrated on-chip sources produce the photons that serve as both the computing qubits and the signals transmitted between modules.

U.S. companies are developing core hardware for high-rate, high-fidelity entanglement distribution, with many focused on connecting quantum processors for distributed quantum computing. A few of them are pictured here (for more details, see Table 1). Icarus Quantum's optical cavity chip contains 40,000 quantum-dot photon sources (top left). CavilinQ's photonic interfaces based on micromirror cavities sit inside processors and concentrate and direct photons emitted by qubits to improve collection efficiency (top middle). MemQ's network interface controller chip converts photons from quantum processors to telecom bands for transmission over optical fiber (top right). IonQ's chip-integrated quantum memory temporarily stores photons to improve entanglement success rates between processors (bottom left). Qunnect's quantum memory module is part of a broader rack-mounted system that supports long-distance quantum networking (bottom right). Sustained progress in performance, manufacturability, and system integration will be essential to meet the demands of high-impact quantum networking applications. (Courtesy of Icarus Quantum, CavilinQ, memQ, IonQ, and Qunnect)









Converting signal frequencies. Quantum networking often requires converting quantum signals from one frequency (or wavelength) to another for efficient fiber transmission, interaction with memory nodes, or interfacing between different qubit types. For trapped ions, neutral atoms, and photonic systems, which already operate in the optical regime, this means shifting between nearby optical frequencies, a process that has been demonstrated but still introduces signal loss that requires further improvement. Superconducting qubits pose a fundamentally different challenge because they operate using microwave signals, far lower in energy than light, making conversion to optical frequencies (known as transduction) orders of magnitude harder. Current superconducting architectures sidestep this by connecting processors through cryogenic microwave links, but these have only been demonstrated at distances approaching one meter. Scaling beyond that would require solving the microwave-to-optical transduction problem, which remains a major unsolved challenge.

Establishing entangled connections. Entanglement between nodes can be established in several ways: a processor's qubit may emit a photon that travels directly to another node, photons from each node may be sent to a shared measurement point for a joint measurement, or a separate entanglement source may send photons to each node independently. In all cases, single-photon detectors must confirm whether the connection succeeded. Most attempts fail because one or both photons are lost along the way. Of those that arrive, success further depends on how reliably detectors register photons (detection efficiency), avoid false signals (dark-count rate), and determine arrival time (timing

jitter). First-generation QKD does not require entanglement but still depends on detector performance for key-generation rates and security.

Quantum memories can improve success rates by allowing different stages of the connection process to succeed independently rather than simultaneously. Each node establishes entanglement with the memory node independently, and the memory stores the first successful result until the second succeeds; a joint measurement then connects the two into a single entangled link. At longer distances, memories become essential for repeater architectures that extend entanglement across multiple segments beyond the reach of any single connection. Memory performance depends on how long a state can be held before degrading (storage time), how much of the stored information can be recovered (retrieval efficiency), and how much quality is preserved in the process (fidelity).

Classical Infrastructure and Control Layer

Transmission infrastructure. Optical fiber is the most broadly applicable medium for transmitting quantum states, but signal loss accumulates with distance. For data center–scale modular computing, fiber runs are short enough that transmission loss is secondary to the challenges of generating and extracting the signal at the processor, and operators typically control the fiber and can optimize performance. For metropolitan and longer-distance networking, transmission loss becomes the dominant constraint. Not all existing fiber is suitable as loss, vibration, and competing classical traffic disturb the quantum signals. Free-space and satellite optical links offer alternatives where fiber is impractical, though they are sensitive to weather, pointing accuracy, and line-of-sight constraints.

Timing and synchronization. Many quantum protocols require nodes to coordinate with extremely tight timing, in some cases to within a trillionth of a second or better.[44] Timing and synchronization systems provide this coordination and are foundational across all applications.

Control and orchestration. Real-time control systems must coordinate entanglement generation, error correction, and routing across all quantum networking applications. For modular quantum computing, the control layer must keep pace with processor speeds to avoid wasting short-lived entangled connections. For long-distance networks, control systems must manage entanglement across multiple intermediate nodes and adapt to changing link conditions. These demands grow substantially for heterogeneous architectures coordinating across qubit types with different speeds and operating characteristics.

Ongoing Technical Challenges

The components and infrastructure described above do not operate in isolation, and several overarching challenges cut across the full technology stack. Quantum networking 2.0 applications generally face greater technical challenges than first-generation QKD, especially at longer distances, and near-term QKD deployments do not necessarily translate into infrastructure ready for entanglement distribution.

Compounding loss and noise. Errors and signal loss accumulate at every stage of the quantum networking chain, from signal generation through frequency conversion, transmission, and detection. Where and why loss matters vary by application. First-generation QKD transmits individual signals from sender to receiver; lost signals simply reduce the key generation rate without preventing the protocol from working, which is why QKD can operate over long distances despite high loss. Entanglement-based applications require both sides of a connection to succeed in coordination and must maintain quantum coherence long enough for the result to be used, making them far less tolerant of loss. Fault-tolerant quantum computing generally requires end-to-end connection fidelity above 98 or 99 percent.

Timing synchronization demands. Distributed quantum operations often require nodes to coordinate with extremely tight timing.[45] In modular computing, photons from different processors must arrive at a shared measurement point within extremely narrow time windows, and classical control must keep pace with fast processor cycles. In distributed sensing, timing and phase stability can be even more demanding, as minor errors distort the measurements entanglement is meant to enhance. In long-distance networking, coordinating entanglement across multiple intermediate nodes adds further complexity. In most cases, the required precision exceeds what commercial products currently offer.[46]

System integration. Individual components are advancing, but assembling them into working systems is a complex challenge. For data center–scale modular computing, this means integrating photon-extraction hardware with operational processors, combining frequency conversion with memory nodes, and building control systems fast enough to orchestrate the full pipeline. For long-distance networking, the challenge is greater still, as all of the above components must work over distances where transmission loss is severe, with quantum memories and entanglement swapping coordinated across multiple intermediate nodes while maintaining synchronization and fidelity across the entire chain. This full repeater architecture has not yet been demonstrated.

A Comparative Assessment of U.S. and Chinese Ecosystems

THE PRECEDING CHAPTER ESTABLISHED that quantum networking applications differ substantially in their value propositions, maturity, and infrastructure demands. This chapter applies those technical insights to the competitive landscape, comparing U.S. and Chinese national strategies, programs, and industrial bases, and concluding with an analysis of the strategic implications for the United States.

- **China** has made quantum communications a national strategic priority and has deployed the world's most extensive QKD infrastructure. However, there are signs of a reassessment: The country launched its own PQC standardization process, and a prominent government advisory body acknowledged QKD's commercial limitations relative to PQC while highlighting the strategic importance of next-generation quantum networking for scaling quantum computing and sensing. These signals suggest that implementation of China's 15th Five-Year Plan may seek to push capabilities beyond QKD. China's academic laboratories have demonstrated progress on key building blocks for next-generation quantum networks, although no Chinese companies are yet commercializing these technologies.
- **The United States** has taken a more selective approach to quantum networking, deprioritizing first-generation QKD in favor of next-generation technologies with higher potential strategic returns. Federal programs—exceeding half a billion dollars in the five years after the 2018 National Quantum Initiative—support a wide variety of efforts across distributed quantum computing, sensing, and communications, including about twenty long-distance network testbeds. A growing private sector ecosystem of start-ups and established firms is also advancing core quantum networking hardware. These assets position the United States to lead in the highest-impact quantum networking applications, but sustaining that advantage will require sharpened priorities and targeted action.

China

Government Strategy and Programs

China has made quantum communications a national strategic priority and the central pillar of its quantum ambitions, often above computing and sensing. Although Chinese scientists have pursued the field since at least the 1990s, analysts have pointed to Edward Snowden's 2013 disclosures about NSA surveillance as a catalyst for Beijing's interest in quantum-enabled information security.[47] Prominent scientists including Pan Jianwei and Guo Guangcan have advocated for quantum communications as a domain where China could achieve global leadership while addressing national security needs, and Chinese Communist Party General Secretary Xi Jinping has expressed support for the field in several speeches.[48]

Successive Chinese five-year plans (FYPs) have included quantum communication programs of increasing ambition.[49] The 13th and 14th FYPs (2016–2020 and 2021–2025, respectively) called for the development of "metro-area, intercity, and free-space quantum communication technologies," while the 15th FYP (2026–2030), adopted in March 2026, directs the construction of an "integrated space-ground quantum communications network (天地一体化量子通信网络)."[50]

Chinese programs have focused on long-distance communications infrastructure, primarily QKD, rather than on next-generation applications for distributed quantum computing or sensing. The Beijing-Shanghai Backbone Network, built between 2013 and 2017 with Pan Jianwei as chief scientist, established a 2,000 km fiber-optic QKD link through 32 relay nodes at a reported cost of approximately $80 million.[51] A subsequent national expansion in 2016—the China Quantum Communication Network (CN-QCN)—added over 10,000 km of fiber, 145 nodes, and 20 metropolitan networks covering 17 provinces and 80 cities.[52] Phase I of the CN-QCN, covering about a third of the network, cost approximately $112 million, and provincial governments and state-owned enterprises funded additional metropolitan networks.[53]

China has also led space-based first-generation QKD experiments. The Micius satellite (2016) and the smaller Jinan-1 microsatellite (2022) have demonstrated satellite-to-ground key distribution and intercontinental quantum communication with partners in Austria and South Africa.[54] The 15th FYP's quantum communications provisions signal ambitions to further integrate space and terrestrial infrastructure, potentially including Pan Jianwei's stated plans for a geostationary-orbit satellite in 2027, a constellation of low Earth orbit satellites, and even experiments between the Earth and the Moon.[55]

Notably, there are signs that parts of the Chinese government may be reassessing the balance of support between near-term QKD infrastructure and more advanced quantum networking applications like those pursued in the United States. A November 2025 report from the China Academy of Information and Communications Technology (CAICT)—an influential technical advisory body for the Chinese Ministry of Industry and Information Technology—emphasized the challenges for QKD's commercial prospects: Core performance has stagnated, cost remains high, and—echoing the position of the United States and allied governments—PQC, which China also started developing in 2025, "is a cost-effective solution that can meet information system security compliance requirements for the vast majority of scenarios and users; therefore, integrating QKD is not a necessity."[56]

The report goes on to highlight "quantum information networks" ("量子信息网络") as an emerging field that could enable new capabilities in quantum computing and sensing, noting recent early progress in key enabling technologies in China, the United States, and Europe. These signals suggest that

the 15th FYP implementation may seek to push China's capabilities beyond QKD toward interconnecting quantum computers and sensors.

Industrial Base

In line with the central strategic goals outlined above, China's industrial organizations have focused on first-generation QKD, with a small core of hardware manufacturers and a broader ecosystem of state-owned deployers.[57] The CN-QCN was built and is operated by the Chinese Academy of Sciences (CAS) Quantum Network Company (国科量子通信网络有限公司, sometimes shortened to QuantumNet or Guoke Quantum) using domestic hardware.[58] The dominant supplier is QuantumCTek (科大国盾量子), a 2009 spin-off from Pan Jianwei's and Guo Guangcan's groups at USTC that also develops superconducting quantum computing hardware. The company has been a continued beneficiary of state support, went public in 2020, and is now controlled by China Telecom Quantum Group (中电信量子).[59] The combined entity manufactures QKD terminals, satellite ground stations, and key management systems, and has recently expanded into PQC and hybrid QKD-PQC products.[60] It also operates metropolitan QKD networks in 16 cities as well as application platforms for secure messaging and government workflows.[61]

China's quantum communications industrial base may soon expand beyond QKD and toward quantum networking as a longer-term strategic focus.

Additional QKD hardware developers include XT Quantech (循态量子), founded by Shanghai Jiao Tong University Professor Zeng Guihua; Qasky (问天量子), cofounded by Guo Guangcan and colleagues from his CAS quantum information laboratory; Guoteng Quantum (国腾量子); and QuDoor (启科量子, sometimes rendered as Qike), which also develops trapped-ion quantum computing hardware and was founded in 2019 by a former chief engineer at MagiQ, a U.S. company based in Massachusetts.[62]

China's quantum communications industrial base may soon expand beyond QKD and toward quantum networking as a longer-term strategic focus. As discussed above, the 2025 CAICT report suggested doubts about QKD's commercial viability given its cost and performance challenges relative to PQC, while also signaling growing government interest in quantum networking as a means to scaling quantum computing and sensing.[63]

Although the authors of this report did not identify Chinese companies commercializing entanglement sources or quantum interconnects, memories, or relays for next-generation quantum networking applications, academic laboratories have demonstrated progress on many of these key building blocks in recent years and may have a path to commercialization through ties to QuantumCTek or new spin-offs. Notable institutions leading this research include the Hefei National Laboratory and USTC (both in Hefei), which have demonstrated advances in single-photon sources, quantum memories, quantum interconnects (including for heterogeneous modalities), and multinode network architectures, along with Tsinghua University (error-correctable relay nodes) and Beijing University (entanglement sources and chip interconnects) in Beijing, and Sun Yat-sen University (entanglement sources) in Guangzhou.[64] Several results involve cross-institutional collaboration with partners including Zhejiang University (Hangzhou) and Shanxi University (Taiyuan).

United States

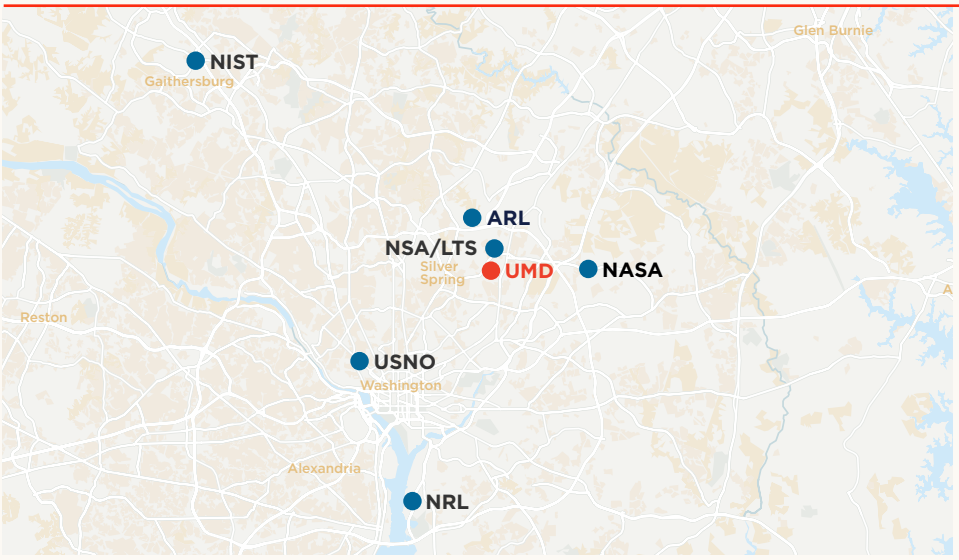
Government Strategy and Programs

The United States has taken a more measured approach to quantum networking than China. Although U.S. scientists and DARPA programs pioneered breakthroughs in first-generation secure communications applications such as quantum key distribution, these technologies "do not currently motivate the U.S. Government to build large quantum networks" like China's, given their narrow applications, persistent implementation vulnerabilities, and cost relative to classical alternatives such as PQC.[65]

The United States is interested in next-generation quantum networking technologies, but frames the field as nascent and multidecade, in contrast to nearer-term priorities in quantum sensing and computing.[66] The national strategy document *A Coordinated Approach to Quantum Networking Research*, developed by interagency experts in 2021, identifies the controlled distribution of entanglement across quantum devices as a high-value capability that would enhance the performance and scale of quantum computing, sensing, and secure communications.[67] However, the strategy notes that substantial foundational work remains, calling for clearer definition of high-value use cases, development of core components such as single-photon sources, quantum memories, and transducers, improvement of classical enabling technologies such as timing protocols, photonics, and electronics, and "right-sized" network testbeds that avoid premature spending.

Although published five years ago, the strategy's core framing and recommendations remain broadly consistent with subsequent reports by the White House National Quantum Coordination Office and the National Quantum Initiative Advisory Committee (NQIAC), as well as with the views of the subject matter experts across the U.S. government, industry, and research organizations interviewed for this report.[68]

Figure 2 | The Washington Metropolitan Quantum Network (DC-QNet) Testbed Links Six Federal Sites for the Characterization and Development of Next-Generation Quantum Networks



The United States supports about 20 quantum networking testbeds spanning federal agencies, national laboratories, universities, and private-sector partners, varying widely in geographical scale and objectives in ways that complicate assessment of collective progress and may obscure gaps and redundancies (for more details, see Table A2 in the appendix). DC-QNet exemplifies cross-agency collaboration and coordination, connecting the Naval Research Laboratory (NRL), Army Research Laboratory (ARL), National Institute of Standards and Technology (NIST), National Security Agency's Laboratory for Telecommunication Sciences (NSA/LTS), U.S. Naval Observatory (USNO), and National Aeronautics and Space Administration (NASA) with a central hub at the University of Maryland (UMD).

Source: Map adapted from "DC-QNet Map," in O. Slattery et al., DC-QNet: Introduction and Overview (NASA, September 2025), https://www.nasa.gov/wp-content/uploads/2025/09/dc-qnet-at-wqrn-2022-8-20-22-letter.pdf; and "Quantum Communications and Networks," NIST, accessed April 12, 2026, https://www.nist.gov/programs-projects/quantum-communications-and-networks.

U.S. government investments in quantum networking R&D have been accordingly smaller than other quantum technology areas, but they remain substantial. In the five years following the 2018 National Quantum Initiative (NQI), the government invested over half a billion dollars in quantum networking—a significant sum, if smaller than the $1.20 billion invested in sensing and $1.36 billion invested in computing, considering networking's longer-term horizon relative to the nearer-term maturity and utility of those fields.[69] Looking ahead, draft congressional legislation in early 2026 to reauthorize the NQI Act includes quantum networking alongside computing and sensing in authorized prize competitions, supply chain assessments, and newly proposed NIST Quantum Research Centers, signaling continued federal support.[70]

Recent government programs have supported quantum networking R&D across several applications. Major programs advancing the interconnection of quantum computing units at short distances include DARPA's HARQ, the National Science Foundation (NSF) Quantum Leap Challenge Institute for Quantum Hybrid Quantum Networks and Architectures—led by the University of Illinois Urbana-Champaign and a consortium of universities and industry partners—and certain workstreams under the Department of Energy (DOE) Quantum Information Science Research Centers anchored at Brookhaven National Laboratory and Fermi National Accelerator Laboratory.[71] The NSF and DOE have also funded modular quantum computing research through smaller grants and programs, and NIST and the United States Army, Navy, and Air Force research labs conduct related intramural and some extramural research as well.[72]

About 20 additional programs—typically identified as "testbeds"—support the networking of multiple nodes over longer distances via fiber optic and, in some cases, open air or free space (see Table A2 in the appendix). These programs are operated by a combination of government agencies, such as NIST, the Department of Defense (DoD), and NASA; DOE-funded national labs; NSF-funded universities; and private companies. They also range widely in scale and objectives, from early testing of quantum information distribution and timing synchronization over a few kilometers to the development of quantum repeaters for cross-city distributed computing, sensing, and secure communications. Several programs have reported early results—primarily point-to-point proofs of principle across two nodes—although the diversity of objectives and reported performance metrics complicates a direct comparison of progress.

This heterogeneity has prompted calls for sharper definitions and goals to ensure quantum networking testbeds target technical gaps at the appropriate maturity level, and for greater coordination to reduce redundancy.[73] In 2024, the NQIAC recommended that future testbed funding require clearly articulated research objectives and progress metrics, as well as demonstrated need for a testbed—which denotes iterative system-level testing of relatively mature components and subsystems—over laboratory-scale prototypes or demonstrators. The committee noted that many core components such as quantum interconnects and memories still require substantial R&D, and that long-distance testbeds "should only be funded when technological maturity can support promising economic or scientific applications."[74]

The U.S. government is also supporting early quantum networking experiments in space. In November 2024, NASA—in partnership with investigators at the University of Illinois Urbana-Champaign—launched the Space Entanglement and Annealing Quantum Experiment, a small payload mounted on the exterior of the International Space Station that reliably generated entangled photon pairs in orbit, claiming to outperform similar Chinese and Singaporean experiments.[75] Reliable entanglement generation in space is a prerequisite for developing orbital quantum network nodes that could transmit quantum information over vast geographical distances.

Industrial Base

In addition to the federal and university laboratories driving quantum networking 2.0 R&D highlighted above, the United States has a growing private sector ecosystem that contrasts with China's ecosystem focused on QKD (see Table 1). Around a dozen U.S. companies are developing hardware and software for the quantum networking stack. Most products remain in prototyping and demonstration phases, although a handful have entered early commercialization.

THE UNITED STATES HAS A GROWING PRIVATE SECTOR ECOSYSTEM THAT CONTRASTS WITH CHINA'S ECOSYSTEM FOCUSED ON QKD.

Several companies are primarily focused on distributed quantum computing, building elements of quantum interconnects to enable high-rate, high-fidelity entanglement between quantum processors. These include memQ, Cisco Quantum Labs, IonQ's Lightsynq, CaviLinQ, and Icarus Quantum, which are developing products spanning quantum network interfaces, frequency converters, switches, photon sources, and compiler software to connect processors into modular architectures within a data center and could also support longer-distance connections. Some were recently announced as performers in DARPA's HARQ program, which seeks to connect heterogeneous qubit modalities into unified computing systems.[76]

Other companies have focused on long-distance quantum communications systems and enabling hardware. Qunnect and Cisco recently demonstrated entanglement swapping over commercial fiber in New York City.[77] (Additional organizations, including EPB and the Quantum Corridor, also operate dedicated fiber testbed infrastructure for quantum networking demonstrations and are included in Table A2 in the appendix.) A few companies have specialized on specific enabling technologies—including photon sources, single-photon detectors, network simulation software, and optical clocks—that serve multiple quantum networking applications at various distances.

Many of these companies are spinouts from universities and federal laboratories—Lightsynq, CavilinQ, and Aliro from Harvard University; Icarus Quantum from NIST Boulder; memQ from the University of Chicago and Argonne National Laboratory; Qunnect from Stony Brook University; and NuCrypt from Northwestern University—and maintain research collaborations.[78] In addition to private capital, most have also received substantial federal R&D dollars to advance their technologies—through Small Business Innovation Research/Small Business Technology Transfer awards, contracts, and research grants via the NSF, NIST, NASA, DOE, and DoD—underscoring the role of government R&D support in seeding private sector innovation in this space.[79]

A few defense primes also engage in quantum networking R&D. Both Leidos and RTX BBN Technologies hold contracts under DARPA's Quantum Augmented Network (QuANET) program, which seeks to integrate quantum and classical networking approaches.[80] Boeing, in partnership with HRL Laboratories, is developing the Q4S satellite to demonstrate entanglement swapping in space for a 2026 launch.[81]

Table 1 | U.S.-Headquartered Companies Developing Quantum Networking and Enabling Technology

Company	Year Founded	Headquarters	Products or Prototypes in Development
memQ[82]	2021	Chicago, IL	▪ Quantum networking hardware system for distributed quantum computing: network interface controller chip that extracts entangled photons from quantum processors, converts them to telecom band, and routes them onto optical networks; quantum memory module (cryogenically cooled; erbium-doped titanium dioxide thin films on foundry silicon photonics); photonic control systems for switching and routing ▪ Software compiler for partitioning and scheduling workloads across networked processors
Cisco Quantum Labs[83]	2025	Santa Monica, CA	▪ Quantum networking hardware for distributed quantum computing: entangled photon-pair source chip (room temperature, telecom band); reconfigurable quantum interfaces that convert photons to telecom band and multiplex them onto optical networks; universal quantum switches for routing entangled photons across heterogeneous quantum devices ▪ Software compiler for partitioning and scheduling workloads across networked processors ▪ Software for network simulation and development
IonQ (via acquisitions)	2015	College Park, MD (HQ); various U.S. locations	IonQ acquired several companies developing quantum networking and enabling technologies: ▪ **Lightsynq** (Boston, MA):[84] Quantum memory (cryogenically cooled; silicon-vacancy centers in diamond thin films on foundry-compatible silicon photonics) that temporarily stores photons to improve entanglement rates for distributed quantum computing ▪ **Qubitekk** (Vista, CA):[85] Long-distance quantum communications system*: entangled photon-pair source (telecom and near-infrared bands), single-photon detector, quantum switches, automatic polarization compensator, timing electronics, and software ▪ **Vector Atomic** (Pleasanton, CA):[86] Optical atomic clocks* and synchronization hardware* ▪ **Skyloom** (Broomfield, CO):[87] Optical communication terminals for satellite links*
CavilinQ[88]	2025	Cambridge, MA	▪ Quantum interfaces using micromirrors to improve entangled light collection from quantum processors and improve entanglement rates for distributed quantum computing
Icarus Quantum[89]	2022	Boulder, CO	▪ On-demand single-photon and entangled photon-pair sources for distributed photonic quantum computing and long-distance communications (semiconductor quantum dots inside optical cavities on chip) ▪ Optical-to-microwave transduction for distributed superconducting quantum computing (similar quantum dot platform with additional components)
Qunnect[90]	2017	Brooklyn, NY	▪ Long-distance quantum communications system (rack-scale modules):* probabilistic entangled photon-pair source, automatic polarization compensator, frequency-stabilized lasers, quantum memory module (warm rubidium [Rb] vapor), monitoring and validation module, and third-party single-photon detectors and time taggers
Infleqtion[91]	2007	Louisville, CO	▪ Quantum memory (laser-cooled Rb atoms)
Quantum Computing Inc. (via NuCrypt acquisition)[92]	2003	Park Ridge, IL	▪ Quantum optical and photonic instruments:* Entangled photon-pair source (telecom band); correlated photon detection system; polarization analyzer; electronic and optical pulse generator
Quantum Opus[93]	2013	Plymouth, MI	▪ Superconducting nanowire single-photon detector (near-infrared through telecom bands)*
Aliro Quantum[94]	2019	Boston, MA	▪ Software for quantum network simulation, control, and orchestration*
RTX BBN Technologies[95]	1948	Cambridge, MA	▪ Hybrid quantum-classical networking R&D under DARPA's Quantum Augmented Network (QuANET) program
Leidos[96]	1969	Reston, VA	▪ Hybrid quantum-classical networking R&D under DARPA's QuANET program
Boeing[97]	1916	Arlington, VA	▪ Preparing 2026 satellite mission to demonstrate entanglement generation and distribution in space, with the quantum networking subassembly built by HRL Laboratories

Note: Asterisk (*) denotes the product is already commercialized; no asterisk denotes the product is in development.

Strategic Implications for the United States

The U.S.-China comparison above yields several insights into each country's approach, assets, and progress, as well as the implications for U.S. quantum networking policy going forward.

Multiple strategic functions beyond securing communications may help explain Beijing's strong support for first-generation quantum networks despite their well-documented limitations. First, these investments may reflect a deliberate gradual approach to technology development, building deployable infrastructure and workforce expertise as a foundation for more sophisticated emerging quantum networking applications. Second, China's large-scale QKD fiber deployments and pioneering satellite-based demonstrations have cemented a widespread perception of Chinese leadership in quantum communications, a source of international prestige Beijing may be motivated to sustain regardless of real-world impact. Additionally, considering the Chinese Communist Party's authoritarian regime, it is possible that a first-generation QKD network that offers no end-to-end security against the network operator may be seen as an asset rather than a flaw.

MULTIPLE STRATEGIC FUNCTIONS BEYOND SECURING COMMUNICATIONS MAY HELP EXPLAIN BEIJING'S STRONG SUPPORT FOR FIRST-GENERATION QUANTUM NETWORKS DESPITE THEIR WELL-DOCUMENTED LIMITATIONS.

Industry-led QKD pilots in China and other countries in Asia and Europe also warrant careful interpretation. To date, QKD pilots supported by certain banks, telecom operators, and technology firms remain primarily R&D exercises rather than operational deployments driven by validated cybersecurity requirements. Motivations may include both hedging against the possibility that PQC algorithms may one day prove vulnerable—though, as noted earlier, QKD itself still relies on classical algorithms for authentication—as well as the reputational appeal of early quantum adoption. Given the inherent limitations of current QKD systems, these pilots likely serve less as a near-term security solution than as a means to build general familiarity with quantum and enabling technologies and to stake an early position in the quantum ecosystem as it matures.

Notably, no country—China included—is pursuing QKD as its sole or even primary approach to secure communications. Even the strongest QKD supporters—China, South Korea, and Japan—are pursuing QKD alongside PQC. China announced a call for domestic PQC standards development in 2025, and both Korea and Japan have set deadlines for PQC migration by 2035, even as they continue to fund QKD demonstrations. This pattern suggests their assessment is not that QKD is the best cryptographic solution but rather one element of a broader strategy that may also serve to advance technical expertise and a competitive posture in quantum technology.

Importantly, however, China's quantum communications capabilities are not limited to first-generation QKD. Prominent Chinese scientists are actively developing the building blocks for quantum 2.0 networking technologies that underpin the higher-impact applications for scaling quantum computing and enhancing sensors that the United States cares about, with notable recent laboratory demonstrations. These emerging capabilities require far stricter timing, fidelity, and routing performance than QKD, as well as entirely new enabling systems like quantum interconnects and memories, and current demonstrations remain far from operational deployment. China's first-generation QKD infrastructure is therefore not directly compatible with quantum 2.0 networks, but it does provide a foundation of deployed fiber, operational ground stations, and skilled teams that the country can build on as next-generation technology matures. No other country has yet matched this combination of operational scale and frontier quantum 2.0 development.

The United States, for its part, holds substantial assets that position it to secure strategic leadership in quantum networking: a strong research and industry ecosystem making substantial technical progress paired with a discerning government investment strategy. Rather than overcommitting financial or human resources to first-generation applications that offer near-term deployment but limited strategic value, U.S. efforts have prioritized next-generation technologies that could enable more powerful quantum computers, more capable quantum sensors, and more resilient communications infrastructure—that is, areas with more credible stakes for both economic competitiveness and national security.

The U.S. position in quantum networking is strong, but not self-sustaining. Securing and extending this leadership will require additional steps.

Recommendations

THIS REPORT'S ANALYSIS REVEALS both strengths and gaps in the U.S. approach to quantum networking. The United States benefits from an evidence-driven posture that has avoided premature commitment of limited federal dollars to quantum applications of uncertain value, fostered a growing industrial base, and supported several testbeds advancing the building blocks that could enable high-value applications such as more powerful quantum computing and sensing. At the same time, additional steps could help the United States reap greater benefits from these investments, from refined definitions and performance benchmarks to strategic investments in hardware and infrastructure.

The following recommendations aim to advance U.S. leadership in high-priority quantum networking applications while maintaining the flexibility to scale programs as the technology matures. Specifically, they call for rigorous application assessments to guide investments, near-term prioritization of quantum interconnects for modular quantum computing within data centers, a calibrated R&D portfolio for longer-distance networking, infrastructure investments that hedge against uncertainty by serving fields beyond quantum networking, and continued urgency in migrating digital systems to post-quantum cryptography. The United States should:

1

Develop standard definitions, performance bench-marks, and assessments of quantum networking applications.

Quantum networking encompasses applications with widely divergent scopes, requirements, and maturity levels, yet the field lacks clear definitions and performance metrics to characterize this heterogeneity. Without them, it is difficult to assess utility, progress, and capability gaps—whether against classical alternatives, across organizations, or relative to other countries—and to strategically allocate limited federal dollars. Clearer definitions and benchmarks could also sharpen the objectives and evaluation of the more than a dozen federally funded long-distance quantum networking testbeds, making it easier to assess their contributions and reduce redundancy across programs.

Federal agencies—such as NIST, given its role in standards, or DARPA, modeled after its computing-focused Quantum Benchmarking Initiative—are well positioned to lead necessary efforts to:

- establish clear, consensus definitions for key quantum networking terms and application categories;
- develop technical performance benchmarks that define meaningful capabilities for each application; and
- direct comprehensive assessments of each application's quantified advantages over alternative approaches, encompassing both technical performance benchmarks and pragmatic cost-benefit analyses.

Other agencies that fund quantum networking efforts should also contribute, such as the DOE, NSF, and NASA. Expert bodies to consult outside the federal government are the Quantum Economic Development Consortium, whose volunteer technical advisory committees have undertaken preliminary work on definitions and benchmarking, as well as the NQIAC, which has also issued recommendations to clarify definitions and objectives for quantum networking.[98]

This work could serve as a basis to guide government priorities and additional assessment programs, with nonexhaustive examples of underdefined topics listed below.

- **QKD:** Performance metrics for practical security and key rates; security assessment of emerging approaches such as measurement-device-independent and device-independent QKD; and cost and infrastructure requirements compared to PQC
- **Distributed quantum computing:** Technical requirements for within–data center interconnects relative to between–data center networking; and how these differ across hardware modalities—such as superconducting, atomic, and photonic platforms—and associated interoperability challenges
- **Distributed sensing:** Network configurations and entanglement properties required for clocks and sensing modalities; performance thresholds that would constitute meaningful advantage over classical networks of quantum sensors; and minimum network scale required for defense-relevant applications
- **Quantum internet:** A rigorous definition differentiating it both from local- and wide-area quantum networks and from the classical internet, specifying what unique functions a global network of quantum networks would perform

2

Accelerate quantum interconnects for scalable quantum computing.

Quantum computing companies across hardware modalities identify modular quantum interconnects—links that enable separate processors or chips within a data center to function as a single, more powerful system—as essential for scaling to the performance levels needed for high-impact applications, from materials discovery to cryptanalysis. Unlike other quantum networking applications, whose value remains more speculative or niche, quantum interconnects are critical to realizing the economic and national security potential of quantum computing

and to sustaining U.S. leadership. Federal agencies should prioritize them accordingly as the most pressing focus of quantum networking efforts.

Although leading companies have placed quantum interconnect demonstrations on their near-term roadmaps, the enabling hardware stack remains immature. The specific bottlenecks vary by modality, and components and processes needed across modalities—including enhanced photon emission and collection, frequency conversion, quantum memories, and photonic integration—require sustained investment. Moreover, connecting processors across different qubits modalities would harness the strengths of each platform, but poses greater technical difficulties, and firms deprioritize it in favor of same-modality interconnects. This makes heterogeneous interconnects a high-impact target for federal investment.

- The DoD should expand DARPA's HARQ program, which targets the interconnection of qubits across diverse hardware modalities. Current funding levels and timelines (up to $2 million per performer over two years) will likely be insufficient for the magnitude of the technical challenge.[99] The program could also expand its scope to the interconnection of quantum sensors and quantum computers, which remains exploratory but could yield transformative returns for intelligence and defense applications.
- National labs, NSF, and NIST should lead complementary advanced quantum science and engineering programs to advance additional critical components in the quantum interconnect hardware stack, including quantum interfaces and transducers, memories, and single-photon detectors, as well as their photonic integration.

Although the near-term priority is data center–scale connectivity, these programs would also generate spillover benefits for longer-distance quantum networking applications, which draw on some of the same underlying components, even if they must also overcome substantial additional challenges—especially increased signal loss over distance—and require first demonstrating a full quantum repeater architecture as well as dedicated fiber or satellite infrastructure.

3

Maintain a calibrated R&D portfolio for geographically distributed quantum networking.

Compared to data center–scale quantum computing interconnects, whose economic and national security value are clear and pressing, long-distance quantum networking remains uncertain and longer term. Next-generation QKD protocols with enhanced security have limited value and are capital intensive relative to classical cryptography. Distributed quantum computing across facilities is less efficient than scaling locally and likely serves only niche use cases. Improved individual or classical networks of sensors may be sufficient for most sensing applications. Long-distance networking is also dependent on unlocking prior breakthroughs in the quantum devices it seeks to network and in enabling hardware that remains immature, such as quantum interfaces and long-lived quantum memories.

At the same time, the competitive landscape also warrants attention. China and several allied countries are backing long-distance quantum networking 2.0 capabilities. Maintaining U.S. technical situational awareness is important, especially considering the capital-intensive nature of the required quantum and classical hardware that would be hard to recreate quickly.

This uncertainty justifies a calibrated rather than aggressive investment posture: sustaining enough capability to remain competitive and make informed decisions as the technology evolves, without overcommitting resources to applications that may not materialize.

The United States has already built a meaningful foundation. More than a dozen quantum networking testbeds—anchored at DOE national laboratories, NSF-funded university centers, and NIST and DoD facilities—are making technical progress on the core components of quantum 2.0 networks.

- Federal agencies should sustain a robust testbed ecosystem at the frontier of entanglement-distribution research, while coordinating across programs to minimize redundancy and maximize coverage of distinct technical challenges.
- Testbed priorities should also extend to longer-term applications with potentially high national security returns and spillover commercial value—such as connecting quantum sensors to quantum computers for enhanced signal detection and classification—where early integration work could build on progress in both computing interconnects and sensing hardware, and where private sector incentives alone are unlikely to drive development.
- To generate decision-relevant evidence, testbeds should prioritize research that directly informs future investment decisions, such as:
  - characterizing entanglement-distribution rates and fidelity over real-world deployed fiber under operational conditions;
  - benchmarking enabling component and subsystem integration and identifying the most tractable paths to full quantum repeater architectures; and
  - rigorously comparing quantum networking performance against the best available alternatives (e.g., classical encryption, locally connected quantum processors, and improved individual or classically connected sensors).
- These efforts should be guided by the definitions and performance benchmarks called for in Recommendation 1, and

their results should feed back into that assessment framework to enable evidence-based decisions about whether and when to scale investment in specific long-distance networking applications.

4

Secure enabling technologies' supply chains and infrastructure with spillovers beyond quantum networking.

Both data center–scale quantum interconnects and longer-distance quantum networking rely on enabling technologies and infrastructure that share substantial overlap with other quantum technologies, as well as with classical communications, defense, and space applications. Critically, many of these inputs face supply chain vulnerabilities, representing areas of risk for quantum networking and beyond.[100] Investments that advance the technical readiness and domestic or trusted sourcing of these inputs represent strategic opportunities with cross-cutting returns regardless of whether specific quantum networking applications fully materialize.

Several inputs provide cross-cutting value and merit additional support.

- **Photonic integrated circuits and high-efficiency single-photon sources and detectors** are critical across both data center–scale interconnects and longer-distance networking, while also serving quantum computing, quantum sensing, and defense applications. U.S. supply chains for advanced photonics depend on foreign sources for key materials and limited domestic foundry capacity, as well as immature heterogeneous integration pathways that hinder yield quality and scalable manufacturing.[101]
- **Precision timing and synchronization systems** are essential for entanglement-based protocols at all distances, and independently underpin GPS-resilient navigation, financial infrastructure, and military operations. Advanced quantum networking applications will require subpicosecond timing and frequency alignment beyond current commercial capabilities, along with specialized hardware to distribute timing without degrading quantum channels.[102]
- **Ultralow-loss fiber and terrestrial free-space optical links** are particularly important for longer-distance quantum links, while simultaneously serving classical long-haul network bandwidth demands and laser communications for defense and intelligence. Ultralow-loss fiber relies on ultrapure silica and advanced, costly fabrication processes and manufacturing concentrated among a few domestic firms, while emerging alternatives such as hollow-core fiber are technically promising but remain immature.[103]
- **Space-based optical terminals** support satellite-based quantum communications and broader military and intelligence space applications, which rely on high-precision laser communication technologies for satellite-to-ground, intersatellite, and space-to-air communications.[104] Scaling these systems will require continued advances in precision pointing, acquisition, and tracking of optical beams between terminals, as well as more resilient ground architectures to mitigate cloud cover and atmospheric interference.[105]
- **Specialized materials and domestic manufacturing processes** for the above components would strengthen supply chain resilience with broad strategic value beyond quantum networking. Examples include thin-film lithium niobate wafers, sourced primarily from China, where the United States has limited processing capacity; III–V semiconductors (e.g., indium phosphide and gallium arsenide), where domestic epitaxial growth capacity is limited; and superconducting materials such as niobium and tantalum, often sourced from nonallied suppliers.[106]

Maximizing the strategic value of these investments requires coordination across existing and new programs. For example, DARPA's QuANET program and NASA's Space Communications and Navigation Program office already fund relevant work on fiber-integrated and free-space quantum links, and the Space Development Agency is developing optical communication terminals with direct relevance to space-based quantum communications.[107]

Where materials and components remain underdeveloped or foreign-dependent, the Department of Commerce (including via NIST), DoD, and NSF should launch targeted advanced R&D or domestic production programs to address gaps.[108] Structuring these efforts from the outset to serve adjacent fields will maximize strategic returns and hedge against the risk that specific quantum networking applications may take longer to materialize.

5

Accelerate PQC migration at home and coordinate with allies abroad.

As the government prioritizes quantum networking technologies that could accelerate quantum computing capabilities, it must also pursue the migration to PQC with equal urgency. More powerful quantum computers may not only unlock significant economic opportunities across materials science and drug discovery, but also break the public-key cryptographic algorithms safeguarding broad swathes of digital assets across national security systems, critical infrastructure, and the broader civilian economy.

NIST finalized the first PQC standards in 2024 and federal policy directs agencies to complete migration by 2035. However,

several challenges remain: Interim milestones and sector-specific guidance are underdeveloped, and migration is expected to take several years and cost billions.

- Agencies such as NIST, NSA, the Cybersecurity and Infrastructure Security Agency, and the Office of the National Cyber Director should continue shepherding a coordinated and timely migration for both the public and private sectors by issuing authoritative guidance, setting interim milestones, and vetting PQC security vendors.

Ensuring allied alignment on NIST PQC standards adoption is also critical. Several allies—including South Korea, Japan, and the European Union—are developing independent PQC algorithms and pursuing QKD and hybrid QKD-PQC approaches (see Table A1 in the appendix). Divergent standards risk undermining interoperability in allied military communications and shared critical infrastructure.[109]

- The White House and the Department of State should make PQC migration a priority topic for bilateral and multilateral engagements on quantum and other critical and emerging technologies, including the Quantum Development Group and emerging frameworks like Pax Silica.
- Additionally, an interagency body, such as the NSTC Subcommittee on the Economic and Security Implications of Quantum Information Science, should assign dedicated resources to monitoring accelerating quantum computing timelines that may warrant policy changes, allied approaches to quantum-safe communications that could create interoperability risks, and the evolving landscape of alternative cryptographic approaches.

Conclusion

QUANTUM NETWORKING ENCOMPASSES a diverse set of applications with different value propositions, technical demands, and maturity timelines. This report has shown that early quantum communications systems, such as QKD, are already deployed but are narrow in utility and constrained by significant practical limitations. By contrast, the more strategically consequential applications of quantum networking—linking quantum computing processors within data centers, enabling higher-performance distributed sensing, and distributing entanglement over longer distances—remain technically immature but potentially far more important to long-term economic and national security advantage. The central policy task facing the United States is to clearly identify the pathways most likely to deliver meaningful strategic value and to align U.S. support accordingly.

This report concludes that the strongest near-term case for quantum networking lies in modular quantum computing within data centers, where quantum interconnects will be essential to scaling useful quantum computers within the next three to five years. Longer-distance quantum networking—whether for secure communications, distributed quantum computing over wider geographic distances, or distributed sensing—warrants continued support, but in a more calibrated posture. These applications may yet prove consequential, and China's extensive first-generation QKD deployments and continued progress in next-generation applications make it unwise for the United States to fully disengage. At the same time, their practical value remains uncertain, their infrastructure demands are higher, and in several cases, they face strong classical or lower-cost alternatives.

The United States' comparative advantage over China lies in the combination of a more selective focus on higher-impact capabilities with a world-class innovation ecosystem of researchers and companies, positioning it to move faster and capture greater strategic returns where they matter most.

Ultimately, the United States' comparative advantage over China lies in the combination of a more selective focus on higher-impact capabilities with a world-class innovation ecosystem of researchers and companies, positioning it to move faster and capture greater strategic returns where they matter most.

The recommendations in this report outline how to convert these U.S. assets into meaningful quantum leadership. The United States should sharpen definitions and benchmarks for quantum networking applications, prioritize data center–scale quantum interconnects as the clearest path to strategic payoff, sustain enough longer-horizon R&D to remain informed and competitive as the technology evolves, and invest in enabling technologies and infrastructure that generate returns across quantum networking and adjacent strategic sectors. At the same time, it must accelerate migration to PQC domestically and with allies, and discourage the treatment of quantum communications as a substitute for urgently needed cybersecurity modernization.

Quantum networking remains nascent, but its highest-value pathways are becoming clearer. With focused action, the United States can preserve a strategic quantum edge while avoiding costly overinvestment in applications whose utility remains uncertain.

Appendix

Methodology

Research for this report was conducted in 2025 and into March 2026. The methodology combined primary and secondary research approaches, including a private roundtable hosted at the Center for a New American Security in January 2026 with subject matter experts and relevant stakeholders in quantum networking technology and policy; more than 20 semistructured interviews with experts from federal and state government, industry, and academia; and reviews of existing literature, government documents, and publicly available information of quantum and enabling-technology companies. Two subject matter experts reviewed a draft of the report and provided feedback.

Table A1 | Country Positions on Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC)

Countries ordered by proximity to the United States' position on QKD and PQC

Country	Official Position on QKD and PQC	QKD Activity Level
United States	**Advises against QKD; prioritizes PQC.**[110] The National Security Agency has concluded that QKD is unsuitable for protecting national security systems and recommends PQC as more cost-effective and maintainable. The National Institute of Standards and Technology's (NIST's) PQC standards, developed through an open global competition and the primary international PQC reference, include three standards finalized in August 2024, with additional standards in development.	**R&D testbeds.**[111] Multiple federal agencies fund metropolitan testbeds for quantum communications and networking, some of which support QKD demonstrations. No nationwide deployment.
United Kingdom	**Advises against QKD; prioritizes PQC.**[112] The United Kingdom (UK) National Cyber Security Centre recommends PQC as the primary mitigation against cryptographically relevant quantum computers. It does not support QKD for government or military systems and recommends that other sectors not rely solely on QKD for key distribution. It supports quantum networking research and development (R&D) with a focus on applications for distributed quantum computing and sensing.	**Metro pilot networks.**[113] UK activities include a 2022 BT-Toshiba commercial QKD metro network trial in London, a 2025 410 km Bristol-Cambridge network demonstration integrating QKD and entanglement distribution, and the 2025 launch of the UK-Singapore SpeQtre satellite.
Australia	**Advises against QKD; prioritizes PQC.**[114] The Australian Signals Directorate does not support QKD for secure communications due to practical limitations.	**R&D testbeds.**[115] In 2025, the national science agency and private sector partners deployed a QKD link over telecom-grade dark fiber in Sydney, with plans to extend to Canberra.
Canada	**QKD not recommended for national security systems; prioritizes PQC.**[116] The Department of National Defence does not recommend QKD until significant technical hurdles are overcome, although it frames this as a call-to-action for R&D investment. The Cyber Centre recommends PQC as the best option for quantum safety.	**National pilot network.**[117] Activities include the Kirq QKD testbed spanning Sherbrooke, Montreal, and Quebec City on live telecom fiber, with a satellite link planned for 2026.
France	**QKD suitable only for niche cases; prioritizes PQC.**[118] The French National Cybersecurity Agency is coauthor of a January 2024 joint position paper concluding QKD has functional limitations and that clear priority should be given to PQC.	**National pilot network.**[119] As part of the European Quantum Communication Infrastructure (EuroQCI), the FranceQCI program is deploying QKD testbeds in Paris, Nice, and Toulouse through a 13-partner consortium including Orange, Thales, and Airbus, with the Toulouse node testing end-user services for the French civil aviation authority.
Germany	**QKD suitable only for niche cases; prioritizes PQC.**[120] The Federal Office for Information Security is coauthor of a January 2024 joint position paper concluding QKD has functional limitations and that clear priority should be given to PQC. Lead signatory of a November 2024 joint statement from 18 (now 21) European Union (EU) member state agencies calling for PQC migration of most sensitive assets by 2030.	**National pilot network.**[121] The Federal Ministry of Research–funded QuNET initiative has demonstrated QKD over metropolitan fiber, including a multi-institution network in Berlin. The EuroQCI-sponsored Q-net-Q project is integrating QKD key management into standard network architectures across multiple cities.
Netherlands	**QKD suitable only for niche cases; prioritizes PQC.**[122] The Netherlands National Communications Security Agency is coauthor of a January 2024 joint position paper concluding QKD has functional limitations and that clear priority should be given to PQC.	**National pilot network.**[123] Under EuroQCI, the QCINed program operates three QKD networks with government ministry participation, and a new project connects to four EU member states via satellite and fiber. Company Q*Bird deployed a multiuser commercial QKD network in 2023.

Country	Official Position on QKD and PQC	QKD Activity Level
Sweden	**QKD suitable only for niche cases; prioritizes PQC.**[124] The Swedish National Communications Security Authority is coauthor of a January 2024 joint position paper concluding QKD has functional limitations and that clear priority should be given to PQC.	**Field testbeds.**[125] Under EuroQCI, the National Quantum Communication Infrastructure in Sweden program is building a national QKD testbed with Ericsson and others centered in Stockholm, with long-distance fiber links and free-space communication pilots.
Japan	**Dual approach: pursues both PQC and QKD.**[126] Japan's 2025 Cybersecurity Strategy targets government PQC migration by 2035, while also committing to accelerating QKD toward operational deployment around 2030, including expanded testbeds and business model development.	**National pilot network.**[127] The National Institute of Information and Communications Technology has operated the Tokyo QKD interoperability testbed since 2010, and in 2025 demonstrated QKD integration over existing telecom infrastructure with Toshiba and NEC. Japan is planning a 600 km national QKD fiber network to be fully deployed by 2030.
Singapore	**PQC is the mainstream solution; QKD is complementary for niche applications.**[128] Draft government guidance states QKD does not replace digital signatures, is more expensive and complex, and requires additional testing due to side-channel vulnerabilities. A senior minister of state reaffirmed PQC as the mainstream solution in March 2026.	**National pilot network.**[129] The National Quantum-Safe Network Plus (NQSN+) has deployed nationwide networks integrating QKD and PQC through operators Singtel and SPTel. Singapore's central bank and four major banks completed a QKD sandbox in 2024–2025. Singapore coleads International Telecommunication Union standardization of QKD protocols with Japan.
European Union	**Supports QKD alongside PQC in hybrid architectures.**[130] The April 2024 European Commission recommendation calls for PQC deployment via hybrid schemes that may combine PQC with QKD, in contrast to more skeptical member state cybersecurity agencies. PQC roadmap sets 2030 deadline for high-risk system migration.	**Continental-scale deployment program.**[131] EuroQCI initiative (all 27 member states) includes national networks, cross-border fiber links, QKD testing and certification infrastructure, and the Eagle-1 satellite demonstrator (launch planned for late 2026). EuroQCI is integrated into IRIS^2, the EU's secure satellite constellation.
South Korea	**Dual-track approach with sovereign PQC and QKD accreditations.**[132] The Ministry of Science and ICT explicitly encourages swift government and public institution adoption of QKD alongside PQC. The National Intelligence Service has accredited two QKD systems as meeting national security standards and also operates its own PQC standardization effort, which selected four domestic PQC algorithms in 2025 for national use alongside NIST standards.	**National pilot network.**[133] Government-funded programs have driven QKD deployment, including an 800 km network securing 48 government ministries completed by SK Broadband in 2022.
China	**Dual-track approach with strong state support for QKD.**[134] Quantum communications has been a strategic priority across multiple five-year plans, with the state actively promoting QKD deployment for government, finance, and critical infrastructure. On PQC, China's Institute of Commercial Cryptography Standards launched a sovereign standardization process in February 2025, pursuing independent algorithms rather than adopting NIST standards.	**Nationwide operational deployment.**[135] The China Quantum Communication Network spans over 10,000 km of optical fiber across 80 cities. Satellite QKD demonstrations include an intercontinental link between China and South Africa in March 2025.

Table A2 | Quantum Network Testbeds in the United States

Testbed, Year Established, Main Location(s)	Lead Operators & Key Partners	Scale	Research Areas	Nonexhaustive Results
FEDERAL GOVERNMENT–LED TESTBEDS				
DC-QNet[136] ***Washington Metropolitan Quantum Network*** 2022 Washington, D.C. metro	Core members: National Institute of Standards and Technology (NIST); U.S. Naval Research Laboratory; U.S. Army Research Laboratory; Laboratory for Telecommunication Sciences; U.S. Naval Observatory; National Aeronautics and Space Administration University of Maryland (UMD) serves as central hub Associate members: Naval Information Warfare Center–Pacific; Air Force Research Lab (AFRL)	Seven sites (some with multiple nodes); fiber links ~3–60 km each	Network synchronization and metrology; components such as quantum memories and single-photon devices; transduction and frequency conversion; entanglement distribution; classical network management, routing, and control software; integration testbed for the Quantum Augmented Network program by the Defense Advanced Research Projects Agency	▪ Subpicosecond clock synchronization over 53 km of fiber for months of continuous operation ▪ Entanglement distribution over 62 km link of partially aerial fiber, with quantum correlations verified continuously over 24 hours
NG-QNet[137] ***NIST Gaithersburg Quantum Network*** 2019 Gaithersburg, MD	NIST Information Technology Laboratory; Communications Technology Laboratory; Physical Measurement Laboratory	Five buildings (some with multiple nodes); fiber links ~1 km each	Entanglement distribution; quantum network control plane and protocol development; classical-quantum coexistence; time synchronization; component development and testing (photon sources, interfaces, memories); vulnerability and robustness testing	▪ Entanglement distributed over 100 km (250 m campus fiber extended with spools) with 87 percent fidelity while coexisting with classical timing signals on the same fiber
Boulder-QNet[138] ***NIST Boulder Quantum Network*** 2023 (infrastructure dates back to ~2000) Boulder, CO	NIST Boulder; University of Colorado (CU) Boulder; JILA (joint institute NIST–CU Boulder)	Three buildings (some with multiple nodes); 3.6 km fiber link and 1.5 km free space link between NIST and JILA	Optical atomic clock synchronization; entanglement distribution	▪ Compared three optical atomic clocks over fiber and free-space links, with agreement to 18 digits ▪ Demonstrated two 2.1 km deployed fiber links with nearly identical single-photon transport quality (sub-100 attosecond timing jitter and >99 percent indistinguishability between paths)
AFRL QLANs[139] ***Quantum Local Area Networks*** 2023 Rome and Stockbridge, NY	AFRL	Griffiss QLAN: four nodes, 15 km buried fiber in total Stockbridge QLAN: ~30 pads, fiber links ~1.5–3.2 km each; free space links 100–300 m each Rome QLAN: three labs and a walkup tower, indoor fiber links ~10m each; aerial fiber links ~1 km each	Entanglement distribution over heterogeneous platforms (trapped ions, superconducting, photonic integrated circuits); quantum frequency conversion and transduction; distributed quantum computing; component development with quantum integrated photonics; demonstrations in challenging environments	▪ Griffiss: Maintained ~99 percent photon signal quality over 10 km buried fiber for ~three continuous days ▪ Stockbridge: Entanglement verified over 4.88 km deployed fiber at near-maximum quantum correlation strength in rugged wooded environment

Testbed, Year Established, Main Location(s)	Lead Operators & Key Partners	Scale	Research Areas	Nonexhaustive Results
NATIONAL LABORATORY AND UNIVERSITY-LED TESTBEDS				
AQNET-SD[140] ***Advanced Quantum Networks for Scientific Discovery*** 2023 (extends a 2019 testbed) Chicago, IL metro	Fermi National Accelerator Laboratory (Fermilab); Argonne National Laboratory (NL); Northwestern University; University of Illinois Urbana-Champaign (UIUC); California Institute of Technology (Caltech)/Jet Propulsion Laboratory	~Nine locations; >150 km fiber in total	Entanglement distribution over metropolitan fiber; coexistence with conventional fiber networks; synchronization, control, and management of remote nodes; squeezed-light protocols to improve entanglement distribution rates.	▪ Entangled photons distributed over 24 km with 94 percent fidelity while sharing fiber with high-throughput classical internet traffic
Chicago Quantum Network[141] 2022 (extends a 2020 testbed) Chicago, IL metro	Argonne NL; University of Chicago; Chicago Quantum Exchange	Six nodes; 200 km fiber in total	Quantum key distribution (QKD); new communications devices; security protocols and algorithms	▪ QKD over fiber at >80,000 quantum bits per second between Chicago and western suburbs
QUANT-NET[142] ***Quantum Application Network Testbed for Novel Entanglement Technology*** 2021 Berkeley, CA	Lawrence Berkeley NL; University of California, Berkeley; Caltech; University of Innsbruck (Austria)	Three nodes; ~5 km fiber in total	Distributed quantum computing and repeaters; heterogeneous networking (trapped ions, silicon color centers); quantum frequency conversion; control plane and software stack	▪ Automated system maintained >99.5 percent signal quality over the 5 km deployed fiber link, and signals sent through the fiber remained nearly identical to lab references—a prerequisite for future entanglement operations
QuAInT[143] ***Quantum-Accelerated Internet Testbed*** 2021 Oak Ridge, TN	Oak Ridge NL (ORNL); Los Alamos NL; University of Tennessee, Knoxville (UTK); Purdue University; Qubitekk; Amazon Web Services (AWS)	Three nodes at ORNL; ~1.5 km fiber in total; planned fiber link to UTK and satellite links	Flexible-grid entanglement distribution; frequency-domain encoding and logic gates; tunable single-photon sources; all-optical quantum repeaters; quantum memory; quantum-secured communications (digital signatures)	▪ Demonstrated across the three ORNL nodes: entangled photons with up to 95 percent fidelity and remote state preparation, a building block for "blind" (secure remote) quantum computing ▪ Characterized quantum digital signature hardware over deployed ORNL fiber for 25 continuous hours; simulations suggest signatures feasible at ~50 km
QUCSON/CQN Tucson Testbed[144] 2021 Tucson, AZ	University of Arizona	Ten nodes across five buildings; ~4 km of fiber in total	Multiuser entanglement distribution; silicon photonics chips; quantum frequency conversion; resource allocation and management protocols	▪ Entanglement distributed and dynamically routed among three buildings (~1 km links); software-defined platform demonstrated concurrent multi-user resource sharing
BARQNET/CQN Boston Testbed[145] ***Boston-Area Quantum Network/Center for Quantum Networks Boston Testbed*** 2022 Boston, MA metro	Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL); MIT; Harvard University; RTX BBN Technologies	Three nodes; ~50 km fiber in total	Diamond silicon-vacancy quantum memories; memory-aided repeater architectures for deployed fiber networks	▪ Photons transmitted over 50 km of deployed fiber with 97.7 percent fidelity ▪ Photons transmitted over 50 km fiber, frequency converted, and entangled with a diamond quantum memory with 87 percent fidelity
MARQI Testbed[146] ***Mid-Atlantic Regional Quantum Internet Testbed*** 2021 College Park, MD	UMD; ARL; IonQ	Five locations; few km of fiber	Interconnects for ion trap quantum computers over kilometer distances	▪ Quantum modem and router prototypes tested on the network: the modem converted photons from trapped-ion system to telecom band; the router directed signals to multiple endpoints
CQN Maryland Testbed[147] 2025 College Park, MD	UMD	Four locations; few km of fiber	Entanglement distribution; integrating trapped-ion quantum processors and diamond color center quantum memories; quantum frequency conversion	▪ Frequency conversion of photons emitted by barium ions to telecom band with >33 percent efficiency and 97 percent fidelity

Testbed, Year Established, Main Location(s)	Lead Operators & Key Partners	Scale	Research Areas	Nonexhaustive Results
NATIONAL LABORATORY AND UNIVERSITY–LED TESTBEDS				
SCY-QNet[148] ***Stony Brook–Columbia–Yale Quantum Network*** 2024 (extends a previous, 2019 testbed) Long Island and New York City, NY; New Haven, CT	Stony Brook University; Brookhaven NL; Columbia University; Yale University	Plans for 10 nodes over >350 km of fiber in total	Quantum repeater-based long-distance entanglement; heralded quantum memories (atomic/rubidium-based [Rb]); atom-based quantum processing units; quantum frequency conversion	▪ Laser pulses converted to telecom band (via Rb-based frequency converters) remained near-indistinguishable after traversing deployed fiber between two locations (158 km total)—a prerequisite for long-distance quantum memory entanglement
ASPEN-Net[149] ***Attosecond Synchronized Photonic Entanglement Network*** 2024 Eugene, OR; Boulder, CO; Urbana, IL	University of Oregon; CU Boulder; NIST Boulder; UIUC; University of New Orleans; University of North Dakota; HRL Laboratories; Boeing	Plans for three network locations: Boulder (16 nodes), Oregon (four nodes), and Illinois (four nodes), with fiber links up to 100 km long.	Modular, all-optical networking architecture; high-rate entanglement distribution; single-photon sources; all-optical quantum memories; attosecond-level synchronization; photon-counting detectors; network management and feedback control systems	No results identified
INDUSTRY-LED TESTBEDS				
EPB Quantum Network[150] 2023 Chattanooga, TN	Electric Power Board (EPB); IonQ/Qubitekk; ORNL; University of Tennessee at Chattanooga;	Up to 10 nodes; 8 km fiber loop	Commercial quantum technology validation and interoperability testing; quantum computing integration and access; entanglement distribution and polarization stabilization research	▪ Entanglement distributed continuously for ~30 hours to two nodes (~3.5 km fiber links) with automatic polarization stabilization and no downtime; ~94 percent entanglement stability throughout ▪ Demonstrated signatures of four-photon interference—building block for quantum repeaters—over 5 and 10 km loops, but photon source quality and signal loss prevented entanglement verification
GothamQ[151] 2023 New York, NY	Qunnect; New York University; Columbia University; Cisco; QTD Systems	Six nodes; ~300 km fiber in total	Entanglement distribution; network orchestration (with Cisco)	▪ Entanglement distribution over 34 km fiber for 15 continuous days; up to 500,000 entangled pairs per second (>84 percent fidelity) or ~99 percent fidelity at 20,000 pairs per second ▪ Entanglement swapping over 17.6 km fiber with independent sources at each node; swapping rates >0.65 per second
Quantum Corridor[152] 2023 Chicago, IL; Hammond, IN	Quantum Corridor Inc.; Ciena; Juniper; C1; Toshiba International Corporation	Two nodes; ~22 km operational fiber; ~277 km additional fiber in ground along Indiana Toll Road	QKD over commercial fiber; high-speed classical networking infrastructure for future quantum applications	▪ Demonstrated QKD (Toshiba equipment) on 21.8 km fiber; continuous key generation over 48 hours, producing enough key material (~1,500 kbps) to refresh keys every 90 seconds
ABQ-Net[153] ***Albuquerque Quantum Network*** 2026 Albuquerque, NM	Qunnect; Roadrunner Venture Studios; Center for Integrated Nanotechnologies (Sandia NL and LANL)	Two nodes; ~25 km fiber link	Open-access user facility for entanglement distribution on existing telecom fiber	No results identified

1. David Awschalom et al., *From Long-Distance Entanglement to Building a Nationwide Quantum Internet* (Department of Energy, Office of Science, February 2020), 10, https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt-20FINAL_Nav_0.pdf; Seth Lloyd et al., "Infrastructure for the Quantum Internet," *ACM SIGCOMM Computer Communication Review* 34, no. 5 (2004): 9–20, https://dl.acm.org/doi/abs/10.1145/1039111.1039118; H. J. Kimble, "The Quantum Internet," *Nature* 453 (2008): 1023–1030, https://www.nature.com/articles/nature07127; and Stephanie Wehner et al., "Quantum Internet: A Vision for the Road Ahead," *Science*, 362, no. 6412 (2018), https://www.science.org/doi/10.1126/science.aam9288.

2. Davide Castelvecchi, "Major Turing Computing Award Goes to Quantum Science for First Time," *Nature*, March 18, 2026, https://doi.org/10.1038/d41586-026-00818-z; Charles H. Bennett and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Theoretical Computer Science* 560, part 1 (2014): 7–11, https://doi.org/10.1016/j.tcs.2014.05.025.

3. Peter Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994): 124–134, https://ieeexplore.ieee.org/document/365700; William Barker et al., *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms* (National Institute of Standards and Technology [NIST], April 28, 2021), 2, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf.

4. "Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," The American Presidency Project, May 4, 2022, https://www.presidency.ucsb.edu/documents/memorandum-promoting-united-states-leadership-quantum-computing-while-mitigating-risks; *Quantum-Readiness: Migration to Post-Quantum Cryptography* (Cybersecurity and Infrastructure Security Agency, National Security Agency, National Institute of Standards and Technology, August 17, 2023), 1–3, https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf.

5. Bennett and Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing"; Peter W. Shor and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters* 85, no. 2 (2000): 441–444, https://doi.org/10.1103/PhysRevLett.85.441; Joseph M. Lukens et al., "Hybrid Classical-Quantum Communication Networks," *Progress in Quantum Electronics* 103 (2025): 100586, https://doi.org/10.1016/j.pquantelec.2025.100586.

6. "Beyond QKD", SURF's Quantum Team, accessed April 30, 2026, https://knowledge-bank-972a03.gitlab.io/beyond-qkd/.

7. *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ* (National Security Agency, December 2024), 16, https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF; "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," National Security Agency, accessed 18 April 2026, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/; and *Quantum Networking: Findings and Recommendations for Growing American Leadership* (National Quantum Initiative Advisory Committee, September 2024), 4, https://www.quantum.gov/wp-content/uploads/2024/09/NQIAC-Report-Quantum-Networking.pdf.

8. "Quantum Networking Technologies," National Cyber Security Centre, August 25, 2025, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies; "The Department of National Defence and Canadian Armed Forces Quantum Science & Technology Strategy Implementation Plan," Government of Canada, March 27, 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/overview-quantum-2030/quantum-s-t-strategy-implementation-plan.html; "Preparing Your Organization for the Quantum Threat to Cryptography (ITSAP.00.017)," Government of Canada, February 2025, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017; *Position Paper on Quantum Key Distribution* (French Cybersecurity Agency; Federal Office for Information Security; Netherlands National Communications Security Agency; and Swedish National Communications Security Authority, Swedish Armed Forces, January 2024), 3, https://cyber.gouv.fr/sites/default/files/document/Quantum_Key_Distribution_Position_Paper.pdf; and "Senior Minister of State, Tan Kiat How, Committee of Supply 2026 Speech, Safeguarding Our Digital Space in a Digital Age," Cyber Security Agency of Singapore, March 2, 2026, https://www.csa.gov.sg/news-events/speeches/senior-minister-of-state-tan-kiat-how-committee-of-supply-2026-speech/.

9. Lars Lydersen et al., "Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination," *Nature Photonics* 4 (2010): 686–689, https://doi.org/10.1038/nphoton.2010.214.

10. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, August 13, 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

11. In July 2024, the Office of Management and Budget estimated that migrating federal civilian agency information systems to post-quantum cryptography would cost approximately $7.1 billion between 2025 and 2035. The report notes this figure excludes national security systems and that it is a rough order of magnitude estimate with a "high, but expected, level of uncertainty." See: *Report on Post-Quantum Cryptography* (Executive Office of the President of the United States, July 2024), 11, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

12. The American Presidency Project, "Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems"; *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*, 11–12.

13. Official statements by United Kingdom (UK) agencies capture the idea of supporting Quantum Key Distribution (QKD) as a

near-term application that can support the development of more advanced quantum networks in the future, even if QKD itself has limited value. In its 2025 guidance, the UK National Cyber Security Centre reiterated its stance against the use of QKD for military and government systems and its caution against sole reliance on QKD for other sectors, while also placing QKD as the least promising application of quantum networking compared to distributed quantum computing and sensing. However, it also acknowledged that technologies and expertise underpinning QKD could contribute to future quantum networks, even if as "one of a number that are needed to address broader network security challenges." This framing echoes the UK government's 2023 national quantum strategy, which identifies deploying the world's most advanced quantum network by 2035 as one of five missions, and positions near-term quantum communications as a stepping stone: "This mission will support further testing, demonstration, and evaluation of near-term commercial opportunities in quantum communications and component technologies . . . [to] build the supply chain and operational learnings, providing the stepping-stone needed for future networks." See: *National Quantum Strategy Missions* (UK Department for Science, Innovation & Technology, updated December 14, 2023), https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-missions.

14. Hua-Lei Yin et al., "Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber," *Physical Review Letters* 117 (2016): 190501, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.117.190501.

15. "George Siopsis," University of Tennessee, Knoxville, Department of Physics and Astronomy, accessed April 26, 2026, https://physics.utk.edu/people/instructional-faculty/siopsis-george/; "Advancing Cybersecurity: Ohio's Leap into Long-Distance Quantum Networks," Ohio State University, College of Engineering, February 1, 2024, https://engineering.osu.edu/news/2024/02/advancing-cybersecurity-ohios-leap-long-distance-quantum-networks; "Quantum Network Testbed Research Directives," Stony Brook University, Figueroa Research Group, accessed April 26, 2026, https://www.stonybrook.edu/commcms/physics/figueroa-research-group/research/testbed_research/index.php; Zhenghao Yao et al., "Continuous-Variable Measurement-Device-Independent Quantum Key Distribution over Fluctuated Free Space Quantum Channels," *Optics Communications* 572 (2024): 131294, https://doi.org/10.1016/j.optcom.2024.131294.

16. Bo-Wei Lu et al., "Device-Independent Quantum Key Distribution over 100 km with Single Atoms," *Science* 391, no. 6785 (2026): 592–597, https://www.science.org/doi/10.1126/science.aec6243.

17. Interviews with quantum networking scientists and technologists in March 2026. The interviews were conducted in confidentiality, and the names of the interviewees are withheld by mutual agreement.

18. D. Main et al., "Distributed Quantum Computing Across an Optical Network Link," *Nature* 638 (2025): 383–388, https://doi.org/10.1038/s41586-024-08404-x; Sagnik Saha et al., "High-Fidelity Remote Entanglement of Trapped Atoms Mediated by Time-Bin Photons," *Nature Communications* 16 (2025): 2533, https://doi.org/10.1038/s41467-025-57557-4; and "IonQ's Accelerated Roadmap: Turning Quantum Ambition into Reality," IonQ, accessed March 25, 2026, https://www.ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality.

19. Jameson O'Reilly et al., "Fast Photon-Mediated Entanglement of Continuously Cooled Trapped Ions for Quantum Networking," *Physical Review Letters* 133 (2024): 090802, https://doi.org/10.1103/PhysRevLett.133.090802; Joshua Ramette et al., "Fault-Tolerant Connection of Error-Corrected Qubits with Noisy Links," *npj Quantum Information* 10 (2024): 58, https://doi.org/10.1038/s41534-024-00855-4.

20. Andreas Reiserer and Gerhard Rempe, "Cavity-Based Quantum Networks with Single Atoms and Optical Photons," *Reviews of Modern Physics* 87, no. 4 (2015): 1379, https://doi.org/10.1103/RevModPhys.87.1379; M. K. Bhaskar et al., "Experimental Demonstration of Memory-Enhanced Quantum Communication," *Nature* 580 (2020): 60–64, https://doi.org/10.1038/s41586-020-2103-5; and Jiapeng Zhao et al., "Scalable Low-Latency Entanglement Distribution For Distributed Quantum Computing," *Optica Quantum* 3, no. 6 (2025): 606–616, https://doi.org/10.1364/OPTICAQ.569352.

21. Uday Saha et al., "Low-Noise Quantum Frequency Conversion of Photons from a Trapped Barium Ion to the Telecom O-Band," *ACS Photonics* 10 (2023): 2861, https://doi.org/10.1021/acsphotonics.3c00581; Reiserer and Rempe, "Cavity-Based Quantum Networks with Single Atoms and Optical Photons."

22. Chris Monroe et al., "Large-Scale Modular Quantum-Computer Architecture with Atomic Memory and Photonic Interconnects," *Physical Review A* 89, no. 2 (2014): 022317, https://doi.org/10.1103/PhysRevA.89.022317; Jacob P. Covey et al., "Quantum Networks with Neutral Atom Processing Nodes," *npj Quantum Information* 9 (2023): 90, https://doi.org/10.1038/s41534-023-00759-9.

23. Dolev Bluvstein et al., "Logical Quantum Processor Based on Reconfigurable Atom Arrays," *Nature* 626 (2024): 58–65, https://doi.org/10.1038/s41586-023-06927-3; Neng-Chun Chiu et al., "Continuous Operation of a Coherent 3,000-Qubit System," *Nature* 646 (2025): 1075–1080, https://doi.org/10.1038/s41586-025-09596-6; and Josiah Sinclair et al., "Fault-Tolerant Optical Interconnects for Neutral-Atom Arrays," *Physical Review Research* 7, no. 1 (2025): 013313, https://doi.org/10.1103/PhysRevResearch.7.013313.

24. CavilinQ, "Unlocking Photonics for Scalable Quantum Systems," Chain Reaction Innovations, Argonne National Laboratory, accessed April 24, 2026, https://chainreaction.anl.gov/unlocking-photonics-for-scalable-quantum-systems/; Nanofiber Quantum Technologies, "Entanglement Boosting: Hardware-Efficient Logical Interconnects," accessed April 24, 2026, https://nano-qt.com/entanglement-boosting-hardware-efficient-logical-interconnects/.

25. Ryan Mandelbaum et al., "IBM Lays Out Clear Path to Fault-Tolerant Quantum Computing," IBM Quantum, June 10, 2025, https://www.ibm.com/quantum/blog/large-scale-ftqc.

26. Sergey Bravyi et al., "The Future of Quantum Computing with Superconducting Qubits," *Journal of Applied Physics* 132, no. 16 (2022): 160902, https://doi.org/10.1063/5.0082975; Theodore J. Yoder et al., "Tour de Gross: A Modular Quantum Computer Based on Bivariate Bicycle Codes," arXiv:2506.03094 (2025), https://arxiv.org/abs/2506.03094; Kentaro Heya et al., "Randomized Benchmarking of a Remote CNOT Gate via a Meter-Scale Microwave Link," *Physical Review Letters* 135 (2025): 200801, https://doi.org/10.1103/xx24-r7q6; P. Kurpiers et al., "Deterministic Quantum State Transfer and Remote Entanglement Using Microwave Photons," *Nature* 558 (2018): 264–267, https://doi.org/10.1038/s41586-018-0195-y; P. Magnard et al., "Microwave Quantum Link Between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems," *Physical Review Letters* 125 (2020): 260502, https://doi.org/10.1103/PhysRevLett.125.260502; and Simon Storz et al., "Loophole-Free Bell Inequality Violation with Superconducting Circuits," *Nature* 617 (2023): 265–270, https://doi.org/10.1038/s41586-023-05885-0.

27. Akihiko Sekine et al., "Microwave-to-Optical Quantum Transduction of Photons for Quantum Interconnects," arXiv:2509.26349 (2025), https://doi.org/10.48550/arXiv.2509.26349; Han Zhao, "Building Photonic Links for Microwave Quantum Processors," *Nanophotonics* 14, no. 11 (2025): 1895–1906, https://doi.org/10.1515/nanoph-2024-0599.

28. H. Aghaee Rad et al., "Scaling and Networking a Modular Photonic Quantum Computer," *Nature* 638 (2025): 912–919, https://www.nature.com/articles/s41586-024-08406-9.

29. J. Eli Bourassa et al., "Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer," *Quantum* 5 (2021): 392, https://doi.org/10.22331/q-2021-02-04-392; Aghaee Rad et al., "Scaling and Networking a Modular Photonic Quantum Compute"; and PsiQuantum Team, "A Manufacturable Platform for Photonic Quantum Computing," *Nature* 641, 876–883 (2025), https://doi.org/10.1038/s41586-025-08820-7.

30. "For Quantum Computing, Different Qubits Are Better Together," Defense Advanced Research Projects Agency (DARPA), April 14, 2026, https://www.darpa.mil/news/2026/quantum-computing-different-qubits-better-together.

31. Interviews with quantum science and technology researchers in January and March 2026. The interviews were conducted in confidentiality, and the names of the interviewees are withheld by mutual agreement.

32. K. A. G. Fisher et al., "Quantum Computing on Encrypted Data," *Nature Communications* 5 (2014): 3074, https://doi.org/10.1038/ncomms4074; P. Drmota et al., "Verifiable Blind Quantum Computing with Trapped Ions and Single Photons," *Physical Review Letters* 132 (2024): 150604, https://doi.org/10.1103/PhysRevLett.132.150604; and Y.-C. Wei, "Universal Distributed Blind Quantum Computing with Solid-State Qubits," *Science* 388, no. 6746 (2025): 509–513, https://doi.org/10.1126/science.adu6894.

33. Constanza M. Vidal Bustamante, *Atomic Advantage: Accelerating U.S. Quantum Sensing for Next-Generation Positioning, Navigation, and Timing* (Center for a New American Security, May 28, 2025), https://www.cnas.org/publications/reports/atomic-advantage.

34. Henry Semenenko et al., *Quantum Communication 101* (NASA, July 2024), 64–67, https://www.nasa.gov/wp-content/uploads/2024/07/quantum-communication-101-final.pdf?emrc=b0a13c.

35. P. Kómár et al., "A Quantum Network of Clocks," *Nature Physics* 10 (2014): 582–587, https://www.nature.com/articles/nphys3000; P.-J. Stas et al., "Entanglement-Assisted Non-Local Optical Interferometry in a Quantum Network," *Nature* 651 (2026): 326–332, https://www.nature.com/articles/s41586-026-10171-w.

36. *Assessment of Time Distribution Systems and Protocols* (Quantum Economic Development Consortium, March 12, 2026), ii, 1, 11, 17, https://quantumconsortium.org/publication/assessment-of-time-distribution-systems-and-protocols/.

37. Interviews with quantum sensing experts working at research organizations and companies in November and December 2025 and in March 2026. The interviews were conducted in confidentiality, and the names of the interviewees are withheld by mutual agreement.

38. Vidal Bustamante, *Atomic Advantage: Accelerating U.S. Quantum Sensing for Next-Generation Positioning, Navigation, and Timing*.

39. Jonathan D. Roslund et al., "Optical Two-Tone Time Transfer," *Physical Review Applied* 24 (2025): 014001, https://doi.org/10.1103/9w7h-zzyd; Emily Caldwell et al., "Quantum-Limited Optical Time Transfer for Future Geosynchronous Links," *Nature* 618 (2023): 721–726, https://doi.org/10.1038/s41586-023-06032-5.

40. Hsin-Yuan Huang et al., "Quantum Advantage in Learning from Experiments," *Science* 376, no. 6598 (2022): 1182–1186, https://doi.org/10.1126/science.abn7293; Saeed A. Khan et al., "Quantum Computational-Sensing Advantage," arXiv:2507.16918 (2025), https://doi.org/10.48550/arXiv.2507.16918; and Saeed A. Khan et al., "Quantum Computational Sensing Using Quantum Signal Processing, Quantum Neural Networks, and Hamiltonian Engineering," arXiv:2507.15845 (2025), https://doi.org/10.48550/arXiv.2507.15845.

41. Huang et al., "Quantum Advantage in Learning from Experiments."

42. "HARQ: Heterogeneous Architectures for Quantum," DARPA, accessed April 12, 2026, https://www.darpa.mil/research/programs/heterogeneous-architectures-for-quantum.

43. *A Coordinated Approach to Quantum Networking Research* (National Science and Technology Council Subcommittee on Quantum Information Science, January 19, 2021), 1, https://www.quantum.gov/wp-content/uploads/2021/01/A-Coordinated-Approach-to-Quantum-Networking.pdf; Awschalom et

al., *From Long-Distance Entanglement to Building a Nationwide Quantum Internet*, 14.

44. *Assessment of Time Distribution Systems and Protocols*, 1, 11.

45. *Assessment of Time Distribution Systems and Protocols,* 17–18.

46. *Assessment of Time Distribution Systems and Protocols,* ii, 1, 11.

47. Elsa B. Kania and John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership* (Center for a New American Security, September 12, 2018), 6, https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNASReport-Quantum-Tech_FINAL.pdf; Elsa Kania and John Costello, "Quantum Leap (Part 1): China's Advances in Quantum Information Science," *China Brief* 16, no. 18 (December 2016): 11–16, https://jamestown.org/program/quantum-leap-part-1-chinas-advances-quantum-information-science-elsa-kania-john-costello/; 邱晨辉 [Qiu Chenhui], "揭秘全球首颗量子卫星——迈向'无条件安全通信'的大门 [Uncovering the World's First Quantum Satellite: Opening the Door to 'Unconditionally Secure Communications']," 中国青年报 [China Youth Daily], August 17, 2016, https://www.cas.cn/zt/kjzt/lzwx/jzjd/201608/t20160817_4571527.shtml.

48. Kania and Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, 6–7.

49. Kania and Costello, "Quantum Leap (Part 1): China's Advances in Quantum Information Science," 11–16.

50. 中华人民共和国国民经济和社会发展第十四个五年规划和*2035*年远景目标纲要 *[Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Objectives Through the Year 2035]* (National Development and Reform Commission, March 2021), https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202103/P020210323538797779059.pdf; 中华人民共和国国民经济和社会发展第十五个五年规划纲要 *[Outline of the 15th Five-Year Plan for National Economic and Social Development of the People's Republic of China]* (National People's Congress of the People's Republic of China, March 13, 2026), http://www.npc.gov.cn/npc/c2/c30834/202603/t20260316_453274.html.

51. May Wang, "CAS Center for Excellence in Quantum Information and Quantum Physics: Exploring Frontiers of Quantum Physics and Quantum Technology," National Science Review 4, no. 1 (2017): 144–152, https://doi.org/10.1093/nsr/nwx025; Yu-Ao Chen et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," Nature 589 (2021): 214–219, https://doi.org/10.1038/s41586-020-03093-8; and 中安在线 [Anhui News Online], "刚刚，省长李国英与北京视频通话，世界首条量子保密通信'京沪干线'正式开通 [Just Now: Governor Li Guoying Video Calls Beijing, World's First Quantum Secure Communication 'Beijing–Shanghai Trunk Line' Officially Opens]," October 2, 2017, https://news.ustc.edu.cn/info/1056/53438.htm.

52. Hao-Ze Chen et al., "Implementation of Carrier-Grade Quantum Communication Networks Over 10000 km," *npj Quantum Information* 11 (2025): 137, https://www.nature.com/articles/s41534-025-01089-8.

53. 关于科大国盾量子技术股份有限公司首次公开发行股票并在科创板上市之补充法律意见书（十） *[Supplementary Legal Opinion (No. 10) on the Initial Public Offering and Listing on the STAR Market of QuantumCTek Co., Ltd.]* (安徽天禾律师事务所 [Anhui Tianhe Law Office], 2019), https://www.csrc.gov.cn/csrc/c100090/c1520330/1520330/files/8-3%20%E8%A1%A5%E5%85%85%E6%B3%95%E5%BE%8B%E6%84%8F%E8%A7%81%E4%B9%A6%EF%BC%88%E5%8D%81%EF%BC%89.pdf; "山东省量子通信技术实用化取得重大进展 [Major Progress in the Practical Application of Quantum Communication Technology in Shandong Province]," 山东省科技厅 [Shandong Provincial Department of Science and Technology], November 8, 2013, https://www.most.gov.cn/dfkj/sd/zxdt/201311/t20131107_110215.html; "激光技术与产业发展创新论坛在光谷召开 [Laser Technology and Industrial Development Innovation Forum Held in Guanggu]," 湖北省科技厅 [Hubei Provincial Department of Science and Technology], December 8, 2016, https://www.most.gov.cn/dfkj/hub/zxdt/201612/t20161207_129443.html; 姚燕清 [Yao Yanqing], "量子通信'武合干线'开建：商业化推进惠及全产业链 [Construction of Quantum Communication 'Wuhan-Hefei Trunk Line' Begins: Commercial Advancement Benefits the Entire Industry Chain]," 上海证券报 [Shanghai Securities News], November 24, 2016, https://news.cnstock.com/industry,rdjj-201611-3959521.htm; and 齐鲁网 [Qilu News], "华中地区首个量子通信城域网启动运营 [Central China's First Quantum Communication Metropolitan Area Network Begins Operations]," October 31 2017, https://news.iqilu.com/china/gedi/2017/1031/3729094.shtml.

54. Sheng-Kai Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters* 120 (2018): 030501, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.030501; "Real-World Intercontinental Quantum Communications Enabled by the Micius Satellite," Phys.org, January 19, 2018, https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html; Elizabeth Gibney and Nature Magazine, "Mini-Satellite Sends Encrypted Quantum Message a Record-Breaking Distance," *Scientific American*, March 26, 2025, https://www.scientificamerican.com/article/mini-satellite-sends-encrypted-quantum-message-a-record-breaking-distance/; and Joseph Federici, *Vying for Quantum Supremacy: U.S.–China Competition in Quantum Technologies* (U.S.–China Economic and Security Review Commission, November 18, 2025), 10, https://www.uscc.gov/research/vying-quantum-supremacy-us-china-competition-quantum-technologies.

55. Ling Xin, "China's New Dawn: Pan Jianwei Reveals High-Orbit Quantum Satellite for Global Network," *South China Morning Post*, June 26, 2025, https://www.scmp.com/news/china/science/article/3315963/new-dawn-pan-jianwei-reveals-high-orbit-quantum-satellite-global-network.

56. "量子信息技术发展与应用 研究报告 (2025) [Research Report on the Development and Application of Quantum Information Technology (Year 2025)]," China Academy of Information and Communications Technology, November 2025, 43, https://www.caict.ac.cn/kxyj/qwfb/bps/202512/P020260123416917309848.pdf; "Announcement on Launching the Next-Generation Commercial Cryptographic Algorithms Program," Institute of Commercial Cryptography Standards, February 5, 2025, https://www.niccs.org.cn/niccs/Notice/pc/content/content_1937428197396713472.html.

57. Other carriers and state-owned enterprises deploy QKD services but do not manufacture the hardware, and deployments remain limited. For example, China Mobile offers an encrypted mobile service that preloads quantum-generated keys onto SIM cards, but the quantum security layer applies only to key generation, not to subsequent storage or transmission on the device. In the power sector, State Grid has deployed quantum communications equipment produced through a joint venture with QuantumCTek at a demonstration substation in Hefei. See: "中移量子密讯 [China Mobile Quantum Secure Messaging]," China Mobile, accessed April 26, 2026, https://dev.10086.cn/superSIM/portal-main/infoDetail/quantumConfidential; "我国首座量子应用示范变电站建成投用 [China's First Quantum Application Demonstration Substation Built into Service]," Xinhua News Agency, November 29, 2024, https://www.xinhuanet.com/tech/20241129/2cd393249bb54093b3713fb3bd39baaa/c.html.

58. "Our Company," 量子网络 [QuantumNet], accessed April 26, 2026, https://www.qtict.com/english/about/company; Ivy Delaney, "China Quantum Computing Companies: 2026 Guide," Quantum Zeitgeist, March 8, 2026, https://quantumzeitgeist.com/china-quantum-computing-companies-2026/.

59. Antonia Hmaidi and Jeroen Groenewegen-Lau, "China's Long View on Quantum Tech Has the US and EU Playing Catch-Up," Merics, December 12, 2024, https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch; Ma Si, "Vital Business Starts at Subatomic Level," *China Daily*, March 30, 2022, https://global.chinadaily.com.cn/a/202203/30/WS6243baa9a310fd2b29e541f6.html.

60. "Products," QuantumCTek, accessed April 10, 2026, https://www.quantum-info.com/English/product/.

61. Matt Swayne, "China Telecom Launches Hybrid Quantum-Safe Encryption System, Completes 1,000-Kilometer Secure Call," Quantum Insider, May 20, 2025, https://thequantuminsider.com/2025/05/20/china-telecom-launches-hybrid-quantum-safe-encryption-system-completes-1000-kilometer-secure-call/.

62. "Product Center," XT Quantech, accessed April 10, 2026, https://www.xtquantech.com/; James Dargan, "China: The Rising Star of Quantum Communication," Quantum Insider, June 11, 2024, https://thequantuminsider.com/2022/07/26/china-the-rising-star-of-quantum-communication/; "Product Series," Qasky, accessed April 10, 2026, http://www.qasky.com/wentianliangzi/vip_doc/26893214_0_0_1.html###; "产品 [Products]," Guoteng Quantum, accessed March 27, 2026, https://www.nqctek.com/ProductInfoCategory?categoryId=558655&PageInfoId=0; "Guoteng Quantum," Crunchbase, accessed April 10, 2026, https://www.crunchbase.com/organization/guoteng-quantum; "公司介绍 [About Us]," Qudoor, accessed May 30, 2026, https://www.qudoor.com/index.php?c=category&id=21; Delaney, "China Quantum Computing Companies: 2026 Guide"; Li Nianzhen, "切入千亿元量子信息技术市场，「启科量子」要做行业的综合产品研发商 [Entering the Trillion-Yuan Quantum Information Technology Market, 'Qike Quantum' Aims to Be the Industry's Comprehensive Product Developer]," 36Kr, November 18, 2019, https://36kr.com/p/1724696461313; and "国内初创公司研制离子阱可扩展分布式量子计算机：专访 [Domestic Startup Develops Ion Trap Scalable Distributed Quantum Computer: An Interview]," MIT Technology Review China, January 29, 2021, https://www.mittrchina.com/news/detail/5567.

63. 量子信息技术发展与应用 研究报告 *(2025) [Research Report on the Development and Application of Quantum Information Technology (Year 2025)]* (China Academy of Information and Communications Technology, November 2025), 43, https://www.caict.ac.cn/kxyj/qwfb/bps/202512/P020260123416917309848.pdf.

64. Xing Ding et al., "High-Efficiency Single-Photon Source Above the Loss-Tolerant Threshold for Efficient Linear Optical Quantum Computing," *Nature Photonics* 19 (2025): 387–391, https://doi.org/10.1038/s41566-025-01639-8; Wen-Zhao Liu et al., "Long-Lived Remote Ion–Ion Entanglement for Scalable Quantum Repeaters," *Nature* 652 (2026): 51–57, https://www.nature.com/articles/s41586-026-10177-4; Lan-Tian Feng et al., "Chip-to-Chip Quantum Photonic Controlled-Not Gate Teleportation," *Physical Review Letters* 135 (2025): 020802, https://doi.org/10.1103/d53g-v8q6; Chen-Xu Wang et al., "Heterogeneous Entanglement Between a Trapped Ion and a Solid-State Quantum Memory," arXiv:2603.05836, March 6, 2026, https://arxiv.org/abs/2603.05836; Mi Zou et al., "Realization of an Untrusted Intermediate Relay Architecture Using a Quantum Dot Single-Photon Source," *Nature Physics* 21 (2025): 1670–1677, https://doi.org/10.1038/s41567-025-03005-5; Yu-Ping Liu et al., "A Millisecond Integrated Quantum Memory for Photonic Qubits," *Science Advances* 11, no. 13 (2025), https://doi.org/10.1126/sciadv.adu5264; Xiu-Ying Chang et al., "Hybrid Entanglement and Bit-Flip Error Correction in a Scalable Quantum Network Node," *Nature Physics* 21 (2025): 583–589, https://doi.org/10.1038/s41567-025-02831-x; Jieshan Huang et al., "Integrated Optical Entangled Quantum Vortex Emitters," *Nature Photonics* 19 (2025): 471–478, https://doi.org/10.1038/s41566-025-01620-5; Xinyu Jia et al., "Continuous-Variable Multipartite Entanglement in an Integrated Microcomb," *Nature* 639 (2025): 329–336, https://doi.org/10.1038/s41586-025-08602-1; and Shunfa Liu et al., "Quantum Correlations of Spontaneous Two-Photon Emission from a Quantum Dot," *Nature* 643 (2025): 1234–1239, https://doi.org/10.1038/s41586-025-09267-6.

65. *A Coordinated Approach to Quantum Networking Research*, 4.

66. *A Coordinated Approach to Quantum Networking Research*, 1; *A Strategic Vision for America's Quantum Networks* (White House National Quantum Coordination Office, February 2020), 2–3, https://www.quantum.gov/wp-content/uploads/2021/01/A-Strategic-Vision-for-Americas-Quantum-Networks-Feb-2020.pdf; and *Bringing Quantum Sensors to Fruition* (Subcommittee on Quantum Information Science, Committee on Science of the National Science & Technology Council, March 2022), 8–9, 15, https://www.quantum.gov/wp-content/uploads/2022/03/BringingQuantumSensorstoFruition.pdf.

67. *A Coordinated Approach to Quantum Networking Research*, 1, 8.

68. *Summary of the 2023 Quantum Networking Interagency Working Group* (National Quantum Coordination Office,

January 2024), 2–7, https://www.quantum.gov/wp-content/uploads/2024/01/2023-QN-IWG-Workshop-Event-Summary.pdf; *Quantum Networking: Findings and Recommendations for Growing American Leadership*, 1–2, 8–9.

69. *National Quantum Initiative Supplement to the President's FY 2025 Budget* (Subcommittee on Quantum Information Science Committee on Science of the National Science & Technology Council, December 2024), 8, https://www.quantum.gov/wp-content/uploads/2024/12/NQI-Annual-Report-FY2025.pdf. Some networking-related funding for distributed quantum computing and sensing applications may also be captured in the "quantum computing" and "quantum sensing" budget categories.

70. National Quantum Initiative Reauthorization Act of 2026, S. 3597, 119th Cong. (2026), https://www.congress.gov/bill/119th-congress/senate-bill/3597.

71. "HARQ: Heterogeneous Architectures for Quantum," DARPA, accessed April 12, 2026, https://www.darpa.mil/research/programs/heterogeneous-architectures-for-quantum; "Hybrid Quantum Architectures and Networks: Propelling Quantum Information into a New Era," University of Illinois Urbana-Champaign, accessed April 12, 2026, https://hqan.illinois.edu/; "Energy Department Announces $625 Million to Advance the Next Phase of National Quantum Information Science Research Centers," U.S. Department of Energy, November 4, 2025, https://www.energy.gov/articles/energy-department-announces-625-million-advance-next-phase-national-quantum-information; Brookhaven National Laboratory, "DOE Renews Brookhaven Lab-Led Quantum Research Center," press release, November 4, 2025, https://www.bnl.gov/newsroom/news.php?a=122687; and Fermi National Accelerator Laboratory, "Fermilab's SQMS Center Funded with $125 Million to Shape the Future of Quantum Information Science," press release, November 4, 2025, https://news.fnal.gov/2025/11/fermilabs-sqms-center-funded-with-125-million-to-shape-the-future-of-quantum-information-science/.

72. "NSF 21-553: Enabling Quantum Leap: Quantum Interconnect Challenges for Transformational Advances in Quantum Systems (QuIC-TAQS)," National Science Foundation, accessed April 12, 2026, https://www.nsf.gov/funding/opportunities/qusec-taqs-quantum-sensing-challenges-transformational-advances-quantum/505860/nsf21-553/solicitation; Department of Energy, Office of Science, Scientific Computing Research, "Accelerated Research in Quantum Computing," notice of funding opportunity, February 7, 2024, https://science.osti.gov/grants/FOAs/-/media/grants/pdf/foas/2024/DE-FOA-0003265.pdf; "Quantum Communications and Networks," National Institute for Standards and Technology, accessed April 12, 2026, https://www.nist.gov/programs-projects/quantum-communications-and-networks; and "National Quantum Initiative Advisory Committee," slide deck, National Quantum Initiative Advisory Committee, November 3, 2023, https://www.quantum.gov/wp-content/uploads/2023/11/NQIAC-Slides-2023-11-03-Draft.pdf.

73. Private event discussion and additional interviews with U.S. quantum networking scientists, engineers, and program managers at government agencies, national laboratories, and universities in March 2026. The interviews were conducted in confidentiality, and the names of the interviewees are withheld by mutual agreement; *Quantum Networking: Findings and Recommendations for Growing American Leadership*, 5, 8; *Summary of the 2023 Quantum Networking Interagency Working Group*, 5, 7.

74. *Quantum Networking: Findings and Recommendations for Growing American Leadership*, 8.

75. Briley Lewis, "Scientists Test Quantum Mechanics in Outer Space," Advancing Physics, April 15, 2025, https://www.aps.org/apsnews/2025/04/quantum-mechanics-in-outer-space.

76. "For Quantum Computing, Different Qubits Are Better Together."

77. Qunnect, "Qunnect and Cisco Demonstrate First Metro-Scale, High-Speed Quantum Entanglement Swapping Over Commercial Fiber," press release, February 18, 2026, https://www.qunnect.inc/press-releases/2026-02-18.

78. Lightsynq Technologies, "Lightsynq Comes Out of Stealth with $18M in Series a Funding to Scale Quantum Computing," press release, Business Wire, November 19, 2024, https://www.businesswire.com/news/home/20241119908343/en/; CavilinQ, "CavilinQ Secures $8.8M Seed Round to Architect the Interconnect Layer for Scalable Quantum Computing," press release, April 2, 2026, https://www.cavilinq.com/post/seed-round; Aliro Quantum Technologies, "Aliro Surges Ahead as the Leader in Quantum Network Technologies with New Products, Research, and Funding," press release, PR Newswire, October 7, 2020, https://www.prnewswire.com/news-releases/aliro-surges-ahead-as-the-leader-in-quantum-network-technologies-with-new-products-research-and-funding-301147167.html; "Icarus Quantum Secures $400,000 SBIR Phase II Award to Scalable Quantum Interconnects," Quantum Computing Report, January 9, 2026, https://quantumcomputingreport.com/icarus-quantum-secures-400000-sbir-phase-ii-award-to-scalable-quantum-interconnects/; memQ, "memQ Announces Series A Funding to Drive Extensible Quantum Networking," press release, March 31, 2026, https://memq.tech/memq_announces_seriesa_funding/; Qunnect, "Quantum Networking Pioneer Qunnect Raises $10 Million in Oversubscribed Series A Extension Spearheaded by Airbus Ventures with Participation from Cisco Investments," press release, June 24, 2025, https://www.qunnect.inc/press-release-2025-06-24; Stony Brook University, "New Technology Designed to Prevent Network Hacking Licensed to LI Company," press release, October 24, 2018, https://news.stonybrook.edu/newsroom/press-release/general/new-technology-designed-to-prevent-network-hacking-licensed-to-li-company; and "Northwestern Startups," Northwestern University, accessed April 19, 2026, https://www.invo.northwestern.edu/technologies/startups/nucrypt.html.

79. IonQ, "IonQ Announces New $21.1 Million Project with United States Air Force Research Lab (AFRL) to Push Boundaries on Secure Quantum Networking," press release, January

13, 2025, https://www.ionq.com/news/ionq-announces-new-usd21-1-million-project-with-united-states-air-force; "Lightsynq Technologies Inc.," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/2665607; "Qubitekk, Inc.," America's Seed Fund, accessed April 19 2026, https://www.sbir.gov/portfolio/403856; "Vector Atomic Inc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/1424341; "Memq Inc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/2057771; memQ, "memQ Delivers Integration of Advanced Quantum Computing Components with Commercial Foundry Processes," press release, July 31, 2025, https://memq.tech/memq-delivers-integration-of-advanced-quantum-computing-components-with-commercial-foundry-processes/; "Icarus Quantum Inc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/2193439; "Reliable Entanglement Verification for Scalable and Deployable Quantum Networks," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/awards/216813; "Qunnect, Inc.," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/1404815; Stony Brook University, "New Technology Designed to Prevent Network Hacking Licensed to LI Company"; Kay Min, "From Theory to Reality: Cisco Investments Backs the Future of Quantum Networking Through Qunnect," Cisco Investments, June 23, 2025, https://www.ciscoinvestments.com/from-theory-to-reality-future-quantum-networking-qunnect; "Atomic System for Quantum Secure Communications," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/awards/174886; "Atom-Network Telecom Exchange," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/awards/173762; "Nucrypt Llc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/253022; "New $8 Million Grant to Fund Research in Quantum Communication," Northwestern Engineering, accessed April 19, 2026, https://www.mccormick.northwestern.edu/news/articles/2012/12/prem-kumar-grant-quantum-communication-research.html; "Quantum Opus Llc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/663108; "Aliro Quantum Technologies," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/1661905; Aliro Quantum, "Aliro Quantum Secures Contracts from U.S. Air Force to Accelerate Development of Quantum Network Simulation and Control Technologies," press release, PR Newswire, July 21, 2021, https://www.prnewswire.com/news-releases/aliro-quantum-secures-contracts-from-us-air-force-to-accelerate-development-of-quantum-network-simulation-and-control-technologies-301336652.html; Aliro Quantum, "Aliro Expands Relationship with U.S. Air Force for Quantum Networking," press release, Business Wire, September 10, 2024, https://www.businesswire.com/news/home/20240910658943/en/Aliro-Expands-Relationship-with-U.S.-Air-Force-for-Quantum-Networking; Aliro Quantum, "Aliro Quantum Receives Investment from Cisco Investments as Part of Funding Round," press release, Business Wire, October 25, 2023, https://www.businesswire.com/news/home/20231025195460/en/Aliro-Quantum-Receives-Investment-from-Cisco-Investments-as-Part-of-Funding-Round; and John Keller, "Leidos and Raytheon BBN to Devise Quantum Communications to Safeguard Networks Against Cyber Threats," Military & Aerospace Electronics, April 3, 2024, https://www.militaryaerospace.com/trusted-computing/article/55001597/leidos-quantum-communications-cyber.

80. Keller, "Leidos and Raytheon BBN to Devise Quantum Communications to Safeguard Networks Against Cyber Threats"; "QuANET: Quantum-Augmented Network," DARPA, accessed April 12, 2026, https://www.darpa.mil/research/programs/quantum-augmented-network.

81. Boeing, "Boeing Pioneering Quantum Communications Technology with In-Space Test Satellite," press release, September 10, 2024, https://boeing.mediaroom.com/2024-09-10-Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite; HRL Laboratories, "HRL Laboratories and Boeing Achieve Key Milestone in Quantum Entanglement Swapping Satellite Mission," press release, April 16, 2025, https://www.hrl.com/news/2025/04/16/hrl-laboratories-and-boeing-achieve-key-milestone-in-quantum-entanglement-swapping-satellite-mission.

82. memQ, "memQ Announces Series A Funding to Drive Extensible Quantum Networking," press release, March 31, 2026, https://memq.tech/memq_announces_seriesa_funding/; memQ, "memQ Delivers Integration of Advanced Quantum Computing Components with Commercial Foundry Processes," press release, July 31, 2025, https://memq.tech/memq-delivers-integration-of-advanced-quantum-computing-components-with-commercial-foundry-processes/; and Shobhit Gupta et al., "Erbium Quantum Memory Platform with Long Optical Coherence via Back-End-of-Line Deposition on Foundry-Fabricated Photonics," *Physical Review Applied* 24 (2025): 054037, https://journals.aps.org/prapplied/abstract/10.1103/xj8y-b6sl.

83. Vijoy Pandey, "Quantum Networking: How Cisco Is Accelerating Practical Quantum Computing," Cisco, May 6, 2025, https://blogs.cisco.com/news/quantum-networking-how-cisco-is-accelerating-practical-quantum-computing; Kevin Delaney, "At Cisco, Bold Steps Towards a Quantum Network," Cisco, August 1, 2025, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m07/at-cisco-bold-steps-towards-a-quantum-network.html; Zhao et al., "Scalable Low-Latency Entanglement Distribution for Distributed Quantum Computing"; Vijoy Pandey, "The Switch That Quantum Networking Has Been Waiting For," April 23, 2026; and Vijoy Pandey, "Cisco Quantum Labs Announces Software That Networks Quantum Computers Together," Cisco, September 25, 2025, https://blogs.cisco.com/news/cisco-quantum-labs-announces-software-that-networks-quantum-computers-together-and-enables-new-classical-applications.

84. IonQ, "IonQ Completes Acquisition of Lightsynq, Accelerating Quantum Computing and Networking Roadmap," press release, June 3, 2025, https://www.ionq.com/news/ionq-completes-acquisition-of-lightsynq-accelerating-quantum-computing-and; "Why We Founded Lightsynq," Lightsynq Technologies, November 19, 2024, https://www.lightsynq.com/why-we-founded-lightsynq.html; M. K. Bhaskar et al., "Experimental Demonstration of Memory-Enhanced Quantum Communication," *Nature* 580 (2020): 60–64, https://doi.org/10.1038/s41586-020-2103-5; IonQ, "IonQ Breakthrough in Synthetic Diamond Materials Accelerates Quantum Net-

working Scale and Production," press release, September 4, 2025, https://investors.ionq.com/news/news-details/2025/IonQ-Breakthrough-in-Synthetic-Diamond-Materials-Accelerates-Quantum-Networking-Scale-and-Production/default.aspx; and Daniel Riedel et al., "Scalable Photonic Quantum Interconnect Platform," *Physical Review X* 16 (2026): 011063, https://doi.org/10.1103/nfrg-zsts.

85. IonQ, "IonQ to Acquire Qubitekk, Furthering Leadership in Quantum Networking," press release, November 6, 2024, https://investors.ionq.com/news/news-details/2024/IonQ-to-Acquire-Qubitekk-Furthering-Leadership-in-Quantum-Networking/default.aspx; Oak Ridge National Laboratory, "EPB Quantum Network Powered by Qubitekk Hosts ORNL's First Run on Commercial Quantum Network"; John Russell, "EPB Offers Commercial Quantum Network for Quantum Developers," HPCwire, October 10, 2023, https://www.hpcwire.com/2023/10/10/epb-offers-commercial-quantum-network-for-quantum-developers/; and "Qubitekk: Quantum Networking and Sources," AusOptic, accessed April 12, 2026, https://ausoptic.com.au/production/qubitekk-quantum-products.html.

86. "Home Page," Vector Atomic, accessed April 19, 2026, https://vectoratomic.com/; IonQ, "IonQ Completes Acquisition of Vector Atomic, the Global Leader in Advanced Quantum Sensing," press release, October 7, 2025, https://www.ionq.com/news/ionq-completes-acquisition-of-vector-atomic-the-global-leader-in-advanced.

87. IonQ, "IonQ Completes Acquisition of Skyloom, Expanding Quantum Networking and Secure Communications Capabilities," press release, January 28, 2026, https://www.ionq.com/news/ionq-completes-acquisition-of-skyloom-expanding-quantum-networking-and-secure-communications-capabilities.

88. CavilinQ, "CavilinQ Secures $8.8M Seed Round"; "Unlocking Photonics for Scalable Quantum Systems," Argonne National Laboratory, accessed April 19, 2026, https://chainreaction.anl.gov/unlocking-photonics-for-scalable-quantum-systems/.

89. "Home Page," Icarus Quantum, accessed April 19, 2026, https://www.icarusquantum.com/; "Icarus Quantum Inc," America's Seed Fund, accessed April 19, 2026, https://www.sbir.gov/portfolio/2193439; and "Icarus Quantum Secures $400,000 SBIR Phase II Award."

90. "Product Overview," Qunnect, accessed April 12, 2026, https://www.qunnect.inc/products; Matt Swayne, "Qunnect Announces Sale of First Commercial Quantum Memory," Quantum Insider, April 22, 2024, https://thequantuminsider.com/2021/11/22/qunnect-announces-sale-of-first-commercial-quantum-memory; and "Carina," Qunnect, accessed April 12, 2026, https://www.qunnect.inc/carina.

91. Infleqtion's primary business focus is neutral atom quantum computing, quantum sensing, and software.; Jacqueline Minerd, "NASA's First-Ever Quantum Memory Made at Glenn Research Center," NASA, July 31, 2024, https://www.nasa.gov/general/nasas-first-ever-quantum-memory-made-at-glenn-research-center/.

92. Quantum Computing, "Quantum Computing Inc. Completes Acquisition of NuCrypt to Advance Quantum Communications Commercialization," press release, PR Newswire, March 5, 2026, https://www.prnewswire.com/news-releases/quantum-computing-inc-completes-acquisition-of-nucrypt-to-advance-quantum-communications-commercialization-302704847.html; "Quantum Optical Instrumentation," NuCrypt, accessed April 12, 2026, https://nucrypt.net/quantum-optical-instrumentation.html; and "Advanced Photonic Technology," NuCrypt, accessed April 12, 2026, https://nucrypt.net/advanced-photonic-technology.html.

93. "Product Info," Quantum Opus, accessed April 12, 2026, https://www.quantumopus.com/web/product-info/.

94. "Aliro Products and Solutions," Aliro Quantum, accessed April 12, 2026, https://www.aliroquantum.com/products.

95. Keller, "Leidos and Raytheon BBN to Devise Quantum Communications to Safeguard Networks Against Cyber Threats."

96. Keller, "Leidos and Raytheon BBN to Devise Quantum Communications to Safeguard Networks Against Cyber Threats"; *Annual Report on Form 10-K for the Fiscal Year Ended January 2, 2026* (Leidos Holdings, Inc., February 17, 2026), https://investors.leidos.com/static-files/2c9c2039-902e-4984-8260-a350ca33c780.

97. Boeing, "Boeing Pioneering Quantum Communications Technology with In-Space Test Satellite," press release, September 10, 2024, https://boeing.mediaroom.com/2024-09-10-Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite; HRL Laboratories, "HRL Laboratories and Boeing Achieve Key Milestone in Quantum Entanglement Swapping Satellite Mission."

98. "Standards & Performance Metrics," Quantum Economic and Development Consortium, accessed April 12, 2026, https://quantumconsortium.org/tac/standards/; *Quantum Networking: Findings and Recommendations for Growing American Leadership*, 1, 5, 7.

99. "Program Solicitation: Heterogeneous Architectures for Quantum (HARQ)," SAM.gov, accessed April 19, 2026, https://sam.gov/opp/967cd8f4c3554b448d7ba3325ed99de2/view.

100. Constanza M. Vidal Bustamante and John Burke, *Quantum's Industrial Moment: Strengthening U.S. Quantum Supply Chains for Scalable Advantage* (Center for a New American Security, March 12, 2026), https://www.cnas.org/publications/reports/quantums-industrial-moment.

101. Vidal Bustamante and Burke, *Quantum's Industrial Moment: Strengthening U.S. Quantum Supply Chains for Scalable Advantage*, 21–22, 27–28.

102. *Assessment of Time Distribution Systems and Protocols*, ii, 1, 11.

103. Lisa A. Moore and Charlene M. Smith, "Fused Silica As an Optical Material [Invited]," Optica Publishing Group, ac-

cessed April 19, 2026, https://opg.optica.org/ome/fulltext.cfm?uri=ome-12-8-3043; "Manufacturing Excellence in Optical Fiber, Corning, accessed April 23, 2026, https://www.corning.com/optical-communications/worldwide/en/home/products/fiber/manufacturing-excellence.html; Hesham Sakr et al., "Hollow Core Optical Fibres with Comparable Attenuation to Silica Fibres Between 600 and 1100 nm," *Nature Communications* 11 (2020): 6030, https://www.nature.com/articles/s41467-020-19910-7; and Semenenko et al., *Quantum Communication 101*.

104. Heather Monaghan, "Quantum Communications," NASA, April 13, 2022, https://www.nasa.gov/directorates/somd/space-communications-navigation-program/quantum-communications/; "Transport," Space Development Agency, accessed March 24, 2026, https://www.sda.mil/transport/; and "SDA Issues Request for Information for Future Space-to-Air Optical Communication Terminals," Space Development Agency, January 28, 2026, https://www.sda.mil/sda-issues-request-for-information-for-future-space-to-air-optical-communication-terminals/.

105. Catherine G. Manning and Katherine Schauer, "Optical Communications," NASA, September 20, 2023, https://www.nasa.gov/technology/space-comms/optical-communications-overview.

106. Vidal Bustamante and Burke, *Quantum's Industrial Moment: Strengthening U.S. Quantum Supply Chains for Scalable Advantage*, 27–28, 30; Lukas Kingma et al., *Official Summary: Critical Vulnerabilities in the Quantum Computing Supply Chain within the NATO Alliance* (NATO Transatlantic Quantum Community, May 12, 2025), 3, 7, https://www.fheijman.nl/QSC_report.pdf.

107. "Quantum Mechanics, Classical Backbone: DARPA's QuANET Advances Practical Quantum Networking," DARPA, August 7, 2025, https://www.darpa.mil/news/2025/quanet-advances-practical-quantum-networking; Monaghan, "Quantum Communications"; and "Resources," Space Development Agency, accessed April 19, 2026, https://www.sda.mil/home/work-with-us/resources/.

108. Vidal Bustamante and Burke, *Quantum's Industrial Moment: Strengthening U.S. Quantum Supply Chains for Scalable Advantage*, 9, 22, 32.

109. Edward Parker, "U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography," Just Security, May 28, 2025, https://www.justsecurity.org/113733/quantum-computing-cryptography/.

110. *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*, 16; National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)"; "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, August 13, 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards; and "Post-Quantum Cryptography," NIST, accessed April 19, 2026, https://csrc.nist.gov/projects/post-quantum-cryptography.

111. See Table A2 in the appendix for more details.

112. "Quantum Networking Technologies," UK National Cyber Security Centre, August 25, 2025, https://www.ncsc.gov.uk/whitepaper/quantum-networking-technologies; National Cyber Security Centre, "Quantum Security Technologies."

113. BT, "BT and Toshiba Launch First Commercial Trial of Quantum Secured Communication Services," press release, April 26, 2022, https://newsroom.bt.com/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services/; University of Bristol, "Researchers Demonstrate the UK's First Long-Distance Ultra-Secure Communication over a Quantum Network," press release, April 7, 2025, https://www.bristol.ac.uk/news/2025/april/quantum-communications-.html; and SpeQtral, "SpeQtre, the Entanglement-Based Quantum Comms Demonstrator Satellite Is Now on Orbit," press release, November 28, 2025, https://speqtralquantum.com/newsroom/speqtre-the-entanglement-based-quantum-comms-demonstrator-satellite-is-now-on-orbit.

114. "Planning for Post-Quantum Cryptography," Australian Signals Directorate, September 22, 2025, https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography.

115. *National Quantum Strategy* (Australian Government, Department of Industry, Science and Resources, May 3, 2023, https://www.industry.gov.au/publications/national-quantum-strategy; "Breakthrough Quantum-Secure Link Protects Data Using the Laws of Physics," CSIRO, October 16, 2025, https://www.csiro.au/en/news/all/news/2025/october/breakthrough-quantum-secure-link-protects-data-using-the-laws-of-physics.

116. Government of Canada, "The Department of National Defence and Canadian Armed Forces Quantum Science & Technology Strategy Implementation Plan"; Canadian Centre for Cyber Security, "Preparing Your Organization for the Quantum Threat to Cryptography (ITSAP.00.017)."

117. Numana, "Kirq Quantum Test Bed Opens in Québec City to Help Industry Test and Deploy Quantum-Safe Networks," press release, January 2026, https://numana.tech/en/kirq-quantum-test bed-opens-in-quebec-city-to-help-industry-test-and-deploy-quantum-safe-networks/; "Quantum Encryption and Science Satellite (QEYSSat)," Government of Canada, accessed April 19, 2026, https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp.

118. *ANSSI Views on the Post-Quantum Cryptography Transition*, position paper (République Française, January 4, 2022), https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition; *Position Paper on Quantum Key Distribution*, 3.

119. Orange, "France's Industry, Quantum Startups, Academic and Institutional Players Join Forces to Build the Future of the French Quantum Internet Communication System," press release, April 18, 2023, https://newsroom.orange.com/frances-industry-quantum-startups-academic-and-institutional-players-join-forces-to-build-the-future-of-the-french-quantum-internet-communication-system/; "European Quantum

Communication Infrastructure (EuroQCI)," European Commission, accessed April 19, 2026, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

120. "Quantum Technologies and Quantum-Safe Cryptography," Federal Office for Information Security, accessed April 19, 2026, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html; *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*, joint statement (German Federal Office for Information Security, June 27, 2024), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3.

121. Fraunhofer IOF, "Quantum Keys for Technological Sovereignty," press release, November 25, 2025, https://www.iof.fraunhofer.de/en/pressrelease/2025/QuNet_paper.html; Matthias Goy et al., "Ad-Hoc Hybrid-Heterogeneous Metropolitan-Range Quantum Key Distribution Network," *New Journal of Physics* 27 (2025): 114510, https://doi.org/10.1088/1367-2630/ae1864; and Fraunhofer IOF, "'There Is No Way Around Thuringia on the Future Quantum Highway,'" press release, August 31, 2023, https://www.iof.fraunhofer.de/en/pressrelease/2023/Launch-Q-net-Q-2023.html.

122. *Position Paper on Quantum Key Distribution*, 3.

123. "Innovation & Collaboration," QuTech, accessed April 19, 2026, https://qutech.h5mag.com/annual_report_2023/innovation_collaboration; "QCINED," Quantum Delta NL, accessed April 19, 2026, https://quantumdelta.nl/qcined; and "Towards a Secure Europe: The Netherlands at the Forefront to Build a Pan-European Quantum Network," TNO, October 1, 2025, https://www.tno.nl/en/newsroom/2025/10/the-netherlands-build-european-quantum/.

124. *Position Paper on Quantum Key Distribution*, 3.

125. "Home Page," National Quantum Communication Infrastructure in Sweden, accessed April 19, 2026, https://nqcis.eu/; "National Quantum Communication Infrastructure in Sweden," Vinnova, accessed April 19, 2026, https://www.vinnova.se/en/p/national-quantum-communication-infrastructure-in-sweden/; and "Building a Quantum Key Distribution Network in Sweden," Ericsson, August 15, 2023, https://www.ericsson.com/en/blog/2023/8/building-a-quantum-key-distribution-network-in-sweden.

126. サイバーセキュリティ戦略の概要 *[Overview of the Cybersecurity Strategy]* (国家サイバー統括室 [National Cybersecurity Office], December 23, 2025, 5, https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025_abstract.pdf.

127. "Quantum Cryptography and Physical Layer Cryptography," National Institute of Information and Communications Technology (NICT), accessed April 30, 2026, https://www.nict.go.jp/en/quantum/about/crypt/english.html; NICT, Toshiba Corporation, and NEC Corporation, "World's First Integrated System for Quantum Key Distribution and High-Speed Data Transmission in a Large-Capacity Optical Transmission System Demonstration Environment for IOWN Open APN," press release, September 16, 2025, https://www.nict.go.jp/en/press/2025/09/16-1.html; and "Japan to Test 600-km Quantum Encryption Network Linking Major Cities," Nikkei Asia, November 25, 2025, https://asia.nikkei.com/spotlight/cybersecurity/japan-to-test-600-km-quantum-encryption-network-linking-major-cities.

128. *Quantum-Safe Migration Handbook*, draft for public consultation, ver. 0.1 (Cyber Security Agency of Singapore et al., October 23, 2025), 31–32, https://isomer-user-content.by.gov.sg/36/11227d39-4350-4ded-9046-d62f99f561ab/Draft%20for%20Public%20Consultation%20-%20Quantum-Safe%20Handbook%20(Oct%202025).pdf; Cyber Security Agency of Singapore, "Senior Minister of State, Tan Kiat How, Committee of Supply 2026 Speech."

129. Infocomm Media Development Authority, "Singapore Launches Southeast Asia's First Quantum-Safe Network Infrastructure to Help Businesses Tap on Quantum-Safe Technologies," press release, June 6, 2023, https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure; "National Quantum-Safe Network Plus (NQSN+)," Infocomm Media Development Authority, accessed April 19, 2026, https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus; and Monetary Authority of Singapore, "MAS and Industry Partners Publish Technical Report on Proof-of-Concept Sandbox for Quantum-Safe Communications Within the Financial Sector," press release, September 29, 2025, https://www.mas.gov.sg/news/media-releases/2025/mas-and-industry-partners-publish-technical-report-on-proof-of-concept-sandbox.

130. *Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography* (European Commission, April 11, 2024), 2, https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography; *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography* (NIS Cooperation Group, June 11, 2025), 6–7, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

131. "European Quantum Communication Infrastructure—EuroQCI," European Commission, accessed April 19, 2026, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci; "Quantum Technologies," European Commission Joint Research Centre, accessed April 19, 2026, https://joint-research-centre.ec.europa.eu/projects-and-activities/quantum-technologies_en; and European Space Agency, "ESA and European Commission to Build Quantum-Secure Space Communications Network," press release, January 30, 2025, https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_and_European_Commission_to_build_quantum-secure_space_communications_network.

132. *Korea's National Quantum Strategy* (Ministry of Science and ICT, June 27, 2023), 42–43, https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023_c.pdf; IDQ, "Clavis XG Series QKD Obtains National Security Certification," press release, January 22, 2025, https://www.idquantique.com/clavis-xg-series-qkd-obtains-national-security-certification/; Kim Eun-jin, "KT Obtains NIS Security Certification for Quantum Key Distribution Equipment," *BusinessKorea*, August 25, 2025, https://www.businesskorea.co.kr/news/articleView.html?idxno=250192; Korean Post-Quantum Cryptography (KpqC), "Selected Algorithms from the KpqC Competition Round 2," January 16, 2025, https://www.kpqc.or.kr/competition_02.html; and "2035년까지 국내 암호체계 양자내성암호로 전환 [National Cryptography Systems to Transition to Post-Quantum Cryptography by 2035]," 전자신문 *(ETNews)*, July 12, 2023, https://www.etnews.com/20230712000182.

133. IDQ, "IDQ and SK Broadband Complete Phase One of Nation-Wide Korean QKD Network," press release, July 19, 2022, https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/; "Nation-Wide Quantum Safe Key Distribution Network in South Korea," IDQ, accessed April 19, 2026, https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/.

134. 中华人民共和国国民经济和社会发展第十五个五年规划纲要 *[Outline of the 15th Five-Year Plan for National Economic and Social Development of the People's Republic of China]*; National Institute of Commercial Cryptography Standards, "Announcement on Launching the Next-Generation Commercial Cryptographic Algorithms Program," press release, February 5, 2025, https://www.niccs.org.cn/niccs/Notice/pc/content/content_1937428197396713472.html; and Matt Swayne, "China Launches Its Own Quantum-Resistant Encryption Standards, Bypassing US Efforts," Quantum Insider, February 18, 2025, https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard-bypassing-us-efforts/.

135. Hao-Ze Chen et al., "Implementation of Carrier-Grade Quantum Communication Networks over 10,000 km"; Yang Li et al., "Microsatellite-Based Real-Time Quantum Key Distribution," *Nature* 640 (2025): 47–54, https://www.nature.com/articles/s41586-025-08739-z; and "Chinese-Led Team Achieves World's First 10,000km Quantum-Secured Communication," Chinese Academy of Sciences, March 19, 2025, https://english.cas.cn/newsroom/cas_media/202503/t20250320_908464.shtml.

136. O. Slattery et al., "DC-QNet: Introduction and Overview," DC-QNet, August 20, 2022, https://www.nasa.gov/wp-content/uploads/2025/09/dc-qnet-at-wqrn-2022-8-20-22-letter.pdf; *Summary of Activities for Fiscal Year 2024* (NIST, July 2025), 96, https://doi.org/10.6028/NIST.IR.8581; Wayne McKenzie et al., "Clock Synchronization Characterization of the Washington DC Metropolitan Quantum Network (DC-QNet)," *Applied Physics Letters* 125, no. 16 (2024): 164004, https://pubs.aip.org/aip/apl/article/125/16/164004/3316979; and Yicheng Shi et al., "Entanglement Distribution over a Polarization-Stabilized Aerial Fiber," arXiv:2601.11753, January 16, 2026, https://arxiv.org/abs/2601.11753.

137. "Quantum Communications and Networks," NIST, accessed April 12, 2026, https://www.nist.gov/programs-projects/quantum-communications-and-networks; Lijun Ma et al., "A Testbed for Quantum Communication and Quantum Networks," *Quantum Information Science, Sensing, and Computation XI* 10984, (2019): 1098407, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927689; Anouar Rahmouni et al., "100-Km Entanglement Distribution with Coexisting Quantum and Classical Signals in a Single Fiber," *Journal of Optical Communications and Networking* 16, no. 8 (2024): 781–787, https://doi.org/10.1364/JOCN.518226.

138. "The National Quantum Initiative and a Coordinated Approach to Quantum Networking," slide deck, National Quantum Initiative Advisory Committee, November 3, 2023, 22, https://www.quantum.gov/wp-content/uploads/2023/11/NQIAC-Slides-2023-11-03-Draft.pdf; Josh Rhoten, "Leadership Highlights Investment and Momentum for Collaboration, New Projects at Quantum Engineering Lab Ribbon Cutting," CUbit Quantum Initiative, University of Colorado Boulder, May 24, 2023, https://www.colorado.edu/initiative/cubit/2023/05/24/leadership-highlights-investment-and-momentum-collaboration-new-projects-quantum; Boulder Atomic Clock Optical Network (BACON) Collaboration, "Frequency Ratio Measurements with 18-Digit Accuracy Using an Optical Clock Network," Nature 591 (2021): 564–569, https://doi.org/10.1038/s41586-021-03253-4; and N. V. Nardelli et al., "Phase-Stable Optical Fiber Links for Quantum Network Protocols," Optica Quantum 4, no. 2 (2026): 138–147, https://doi.org/10.1364/OPTICAQ.582298.

139. Erin Sheridan et al., "Telecommunications Fiber-Optic and Free-Space Quantum Local Area Networks at the Air Force Research Laboratory," arXiv:2508.01030v2, September 4, 2025, https://arxiv.org/abs/2508.01030.

140. Fermilab, "Fermilab Receives DOE Funding to Further Develop Nationwide Quantum Network," press release, October 16, 2023, https://news.fnal.gov/2023/10/fermilab-receives-doe-funding-to-further-develop-nationwide-quantum-network/; "What Is IEQNET," Fermilab, accessed April 19, 2026, https://ieqnet.fnal.gov/; Madeleine O'Keefe, "Nobel-Winning Experiment Enables Fermilab-Led Quantum Network," Fermilab, February 2, 2023, https://news.fnal.gov/2023/02/nobel-winning-experiment-enables-fermilab-led-quantum-network/; Marcia Teckenbrock, "'Squeezed Light' Technology Could Accelerate Path to Quantum Networking," Fermilab, September 30, 2025, https://news.fnal.gov/2025/09/squeezed-light-technology-could-accelerate-path-to-quantum-networking/; and Gina M. Talcott et al., "Synchronized Distribution of Quantum Entanglement Coexisting with High-Rate, Broadband Classical Optical Communications over a Real-World Fiber Link," arXiv:2602.00253, January 30, 2026, https://arxiv.org/abs/2602.00253;.

141. Meredith Fore, "Chicago Expands and Activates Quantum Network, Taking Steps Toward a Secure Quantum Internet," Chicago Quantum Exchange, June 16, 2022, https://chicagoquantum.org/news/chicago-expands-and-acti-

vates-quantum-network-taking-steps-toward-secure-quantum-internet; "Argonne, UChicago Scientists Take Important Step in Developing National Quantum Internet," University of Chicago, February 19, 2020, https://news.uchicago.edu/story/argonne-uchicago-scientists-take-important-step-developing-national-quantum-internet.

142. Kathy Kincade, "Berkeley Lab, UC Berkeley, Caltech to Build Quantum Network Testbed," Berkeley Lab, August 31, 2021, https://newscenter.lbl.gov/2021/08/31/quantum-network-testbed/; "QUANT-NET Consortium Seeks to Establish a Distributed Quantum Computing Network," University of California, Berkeley, January 8, 2024, https://physics.berkeley.edu/news/quant-net-consortium-seeks-establish-distributed-quantum-computing-network; and Damian Schon et al., "The QUANT-NET Testbed Development and Preliminary Results," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Institute of Electrical and Electronics Engineers, 2024), https://www.osti.gov/servlets/purl/2572772.

143. Oak Ridge National Laboratory, "Three ORNL-Led Quantum Research Projects Receive $17.5 Million from DOE," press release, September 22, 2021, https://www.ornl.gov/news/three-ornl-led-quantum-research-projects-receive-175-million-doe; John Russell, "Q&A: ORNL's Early Steps in DOE's March to Build a Quantum Internet," HPCwire, February 2, 2022, https://www.hpcwire.com/2022/02/02/qa-ornls-early-steps-in-does-march-to-build-a-quantum-internet/; Oak Ridge National Laboratory, "Giant Leap Toward Quantum Internet Realized With Bell State Analyzer," press release, March 4, 2022, https://www.ornl.gov/news/giant-leap-toward-quantum-internet-realized-bell-state-analyzer; Oak Ridge National Laboratory, "Quantum Researchers Develop First-Of-Its-Kind Quantum Gate," press release, February 4, 2025, https://www.ornl.gov/news/quantum-researchers-develop-first-its-kind-quantum-gate; Muneer Alshowkan et al., "Reconfigurable Quantum Local Area Network Over Deployed Fiber," PRX Quantum 2, no. 4 (2021): 040304, https://doi.org/10.1103/PRXQuantum.2.040304; and Joseph C. Chapman et al., "Entanglement-Based Quantum Digital Signatures over a Deployed Campus Network," Optics Express 32, no. 5 (2024): 7521–7539, https://doi.org/10.1364/OE.510787.

144. "Testbeds," University of Arizona, accessed April 30, 2026, https://cqn-erc.arizona.edu/research/testbeds; "About CQN," University of Arizona, https://cqn-erc.arizona.edu/about/about-cqn; Photonic Quantum Systems Group, "Center for Quantum Networks (CQN)"; Chaohan Cui, "CQN Testbed: Tucson → Maryland," slide deck, Center for Quantum Networks, accessed April 30, 2026, 232–233, https://cqn-erc.org/wp-content/uploads/2024/04/1-Maryland-Testbed.pdf; and Zhaohui Yang and Chaohan Cui, "Reconfigurable Quantum Internet Service Provider," arXiv:2305.09048, May 15, 2023, https://doi.org/10.48550/arXiv.2305.09048.

145. University of Arizona, "Testbeds"; "Center for Quantum Networks (CQN)," Photonic Quantum Systems Group, accessed April 19, 2026, https://phoqus.us/projects/cqn; Ariana Gaines, "Quantum Repeaters Use Defects in Diamond to Interconnect Quantum Systems," Massachusetts Institute of Technology, September 27, 2023, https://news.mit.edu/2023/quantum-repeaters-use-defects-diamond-interconnect-quantum-systems-0927; Eric Bersin et al., "Development of a Boston-Area 50-km Fiber Quantum Network Testbed," *Physical Review Applied* 21, no. 1 (2024): 014024, https://doi.org/10.1103/PhysRevApplied.21.014024; and Eric Bersin et al., "Telecom Networking with a Diamond Quantum Memory," PRX Quantum 5, no. 1 (2024): 010303, https://doi.org/10.1103/PRXQuantum.5.010303.

146. "About," Quantum Networks to Connect Quantum Technology, accessed April 30, 2026, https://marqi.umd.edu/sample-page/; "About the Maryland Testbed", University of Arizona, accessed April 30, 2026, https://cqn-erc.arizona.edu/maryland-testbed; "Mid-Atlantic Regional Quantum Internet (MARQI) Testbed", University of Maryland, accessed April 30, 2026, https://www.maxgigapop.net/quantum/; IonQ, "IonQ and University of Maryland Expand QLab Collaboration to Advance Quantum Networking and Research," press release, April 13, 2026, https://www.ionq.com/news/ionq-and-university-of-maryland-expand-qlab-collaboration-to-advance-quantum-networking-and-research; and "NSF Convergence Accelerator Track C: Interconnecting Quantum Computers for the Next-Generation Internet," National Science Foundation, accessed April 30, 2026, https://www.nsf.gov/awardsearch/show-award/?AWD_ID=2040695.

147. University of Arizona, "About the Maryland Testbed"; Chaohan Cui, "CQN Testbed: Tucson → Maryland."

148. "Stony Brook University-Led Team Receives $4M NSF Grant to Develop 10-Node Quantum Network," Stony Brook University, September 4, 2025, https://news.stonybrook.edu/newsroom/stony-brook-university-led-team-receives-4m-nsf-grant-to-develop-10-node-quantum-network/; "SCY-Qnet," Stony Brook University, accessed April 19, 2026, https://www.stonybrook.edu/commcms/physics/figueroa-research-group/scy-qnet/; "NQVL:QSTD:Pilot: Wide-Area Quantum Network To Demonstrate Quantum Advantage (SCY-QNet)," National Science Foundation, accessed April 30, 2026, www.nsf.gov/awardsearch/show-award/?AWD_ID=2410725; and Dounan Du et al., "A Long-Distance Quantum-Capable Internet Testbed," arXiv:2101.12742v4, October 16, 2024, https://doi.org/10.48550/arXiv.2101.12742.

149. National Science Foundation, "Final 6 Pilot Projects Selected for NSF National Quantum Virtual Laboratory," press release, December 16, 2024, https://www.nsf.gov/news/final-6-pilot-projects-selected-nsf-national-quantum-virtual; "NQVL:QSTD:Pilot: Attosecond Synchronized Photonic Entanglement Network (ASPEN-Net)," National Science Foundation, accessed April 30, 2026, https://www.nsf.gov/awardsearch/show-award/?AWD_ID=2435378; Quantum ASPEN-Net, "Tutorial: Path-Entangled Quantum Networks," YouTube video, April 9, 2025, 1 hr., 3 min., 45 sec., 11:45–14:15, https://www.youtube.com/watch?v=bmQk1v9O0nM&list=PLix45fnyN1ocIuWmR42nEdLK5wtpI4gK-&index=7; and Kenna Castleberry, "New Project Aims to Advance Secure Communications Through Quantum Technology," University of Colorado Boulder, December 18, 2024, https://www.colorado.edu/today/2024/12/18/new-project-aims-advance-secure-communications-through-quantum-technology.

150. "EPB Quantum℠," EPB Quantum, accessed April 22, 2026, https://quantum.epb.com/about-us/; EPB, "EPB Quantum Network℠Powered By Qubitekk Adds Qunnect As First Customer For Quantum Collaboration," press release, December 5, 2023, https://epb.com/newsroom/press-releases/epb-quantum-networksm-powered-by-qubitekk-adds-first-customer/; Oak Ridge National Laboratory, "EPB Quantum Network Powered by Qubitekk Hosts ORNL's First Run on Commercial Quantum Network," press release, September 11, 2024, https://www.ornl.gov/news/epb-quantum-network-powered-qubitekk-hosts-ornls-first-run-commercial-quantum-network; EPB, "EPB and IonQ Partner to Establish Chattanooga as the First Quantum Computing and Networking Hub in the U.S.," press release, April 25, 2025, https://epb.com/newsroom/press-releases/epb-quantum-center/; "Quantum Technology Pioneers Qubitekk and Qunnect Achieve First Equipment Interoperability on EPB Quantum Network powered by Qubitekk," press release, December 19, 2023, https://epb.com/newsroom/press-releases/qubitekk-and-qunnect-achieve-first-equipment-interoperability-on-epb-quantum-network/; Oak Ridge National Laboratory, "ORNL Partnership With EPB Tests New Method For Protecting Quantum Networks", January 13, 2025, https://www.ornl.gov/news/ornl-partnership-epb-tests-new-method-protecting-quantum-networks; Joseph C. Chapman et al., "Continuous Automatic Polarization Channel Stabilization from Heterodyne Detection of Coexisting Dim Reference Signals," Optics Express 32, no. 26 (2024): 47589–47619, https://doi.org/10.1364/OE.543704; and Kazi Reaz et al., "Reconfigurable Four-Photon Interference in a Deployed Metropolitan Fiber Network," arXiv:2509.03701v4, March 19, 2026, https://arxiv.org/abs/2509.03701.

151. "Qunnect's Quantum Networking Testbed, GothamQ, Enters the Manhattan Borough," press release, PR Newswire, January 17, 2023, https://www.prnewswire.com/news-releases/qunnects-quantum-networking-testbed-gothamq-enters-the-manhattan-borough-301723595.html; "Qunnect Achieves Record-Breaking Performance for Distributing Polarization Qubits on GothamQ Network in NYC," press release, PR Newswire, April 15, 2024, https://www.prnewswire.com/news-releases/qunnect-achieves-record-breaking-performance-for-distributing-polarization-qubits-on-gothamq-network-in-nyc-302116594.html; Alexander N. Craddock et al., "Automated Distribution of Polarization-Entangled Photons Using Deployed New York City Fibers," PRX Quantum 5, 030330 (2024), https://doi.org/10.1103/PRXQuantum.5.030330; Dan Meyer, "Cisco Orchestrates Qunnect's Quantum Network Trial," SDxCentral, February 18, 2026, https://www.sdxcentral.com/news/cisco-orchestrates-qunnects-quantum-network-trial/; and Alexander N. Craddock et al., "High-Rate Scalable Entanglement Swapping Between Remote Entanglement Sources on Deployed New York City Fibers," arXiv:2602.15653v2, March 2, 2026, https://arxiv.org/abs/2602.15653v2.

152. "What Is a Quantum Corridor?," Quantum Corridor, accessed April 19, 2026, https://www.quantumcorridor.com/about-us/faqs; Bruce Chesley and Patrick Scully, "Quantum Corridor: The Commercialized Quantum-Ready Network" (white paper, Quantum Corridor, 2025), https://cdn.prod.website-files.com/65bd0da121861f1d79d65473/68bfe9600c201171a664cab7_The%20Commercialized%20Quantum-Ready%20Network.pdf; Toshiba, "Quantum Corridor, Toshiba Demonstrate First Cross-State Quantum Key Distribution over Live Commercial Metro Fiber Network," press release, accessed April 19, 2026, https://news.toshiba.com/press-releases/press-release-details/2025/Quantum-Corridor-Toshiba-Demonstrate-First-Cross-State-Quantum-Key-Distribution-Over-Live-Commercial-Metro-Fiber-Network/; and Bruce Chesley et al., "Quantum Key Distribution Over Metropolitan Fiber" (white paper, Quantum Corridor, December 2025), https://cdn.prod.website-files.com/65bd0da121861f1d79d65473/69330a5f10a1fdb52d556cee_Quantum%20Key%20Distribution%20Over%20Metropolitan%20Fiber.pdf

153. Roadrunner Venture Studios and Qunnect, "Roadrunner Venture Studios and Qunnect Launch ABQ-Net, New Mexico's First Quantum Network," press release, Roadrunner Venture Studios, November 19, 2025, https://roadrunnerventurestudios.com/insights/roadrunner-and-qunnect-launch-new-mexico-s-first-quantum-network; Qunnect, "25 kilometers today. And we're just getting started. ABQ-Net currently connects downtown Albuquerque to Sandia National Laboratories — on hardware Qunnect has already validated at over 100 kilometers in Berlin. The engineering is proven," LinkedIn, April 30, 2026, https://www.linkedin.com/posts/qunnectinc_25-kilometers-today-and-were-just-getting-activity-7455662509908328448-8KqV; Justin Horwath, "As a Quantum Network Goes Live, New Mexico Sees its Moment," Albuquerque Journal, March 1, 2026, https://www.abqjournal.com/business/as-a-quantum-network-goes-live-new-mexico-sees-its-moment/2990185; and Hannah Garcia, "Qunnect's ABQ-Net Launch Marks Latest Step in New Mexico's Bid to Be a Quantum Tech Hub," Albuquerque Journal, November 23, 2025, https://www.abqjournal.com/business/qunnects-abq-net-launch-marks-latest-step-in-new-mexicos-bid-to-be-a-quantum-tech-hub/2901477.

CNAS Editorial

DIRECTOR OF STUDIES
Katherine L. Kuzminski

PUBLICATIONS & EDITORIAL DIRECTOR
Maura McCarthy

SENIOR EDITOR
Emma Swislow

ASSOCIATE EDITOR
Caroline Steel

CREATIVE DIRECTOR
Melody Cook

Cover Art & Production Notes

LAYOUT & DESIGN
Nicole Hamam

COVER ILLUSTRATION
Melody Cook

PRINTER
CSI Printing & Graphics
Printed on an HP Indigo Digital Press

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts, and the public with innovative, fact-based research, ideas, and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, D.C., and was established in February 2007 by cofounders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and nonpartisan.

©2026 Center for a New American Security

All rights reserved.

New Rules

The old national security playbook no longer applies. As emerging technologies reshape the battlefield, great power rivalries intensify, and traditional frameworks evolve, the ground is no longer settled.

America should set **New Rules**. Pragmatic leaders at home and abroad can no longer afford to provide yesterday's answers to today's national security challenges.

From AI and drone warfare to global alliances and economic security, America and its allies need New Rules to compete, deter, and win in the 21st century. The Center for a New American Security develops bold, principled national security policies so that today's leaders can set the New Rules of tomorrow.

Center for a New American Security
1701 Pennsylvania Ave NW
Suite 700
Washington, D.C. 20006

CNAS.org

@CNASdc

CEO
Richard Fontaine

Executive Vice President
Paul Scharre

Senior Vice President of Development
Anna Saito Carson

Contact Us

202.457.9400
info@cnas.org

CNAS
New
Rules