Quantum-safe networking: how the telecoms industry is preparing for new security threats

July 2026

Michelle Lam

Quantum computing is advancing faster than anticipated and its implications for network security are profound. The 'harvest now, decrypt later' threat – where adversaries collect encrypted data today in anticipation of future decryption – means the security risks to highly sensitive data are already present, even before cryptographically relevant quantum computers become widely available. In response, leading telecoms operators around the world are investing in quantum-safe networking (QSN) solutions to futureproof their network security and launch new service offerings.

What is QSN?

Telecoms operators are pursuing two principal QSN technologies: post-quantum cryptography (PQC) and quantum key distribution (QKD).

PQC involves deploying cryptographic algorithms designed to resist attacks from quantum computers. It involves replacing classical public-key cryptographic algorithms such as RSA and ECC, whose security depends on mathematical problems that quantum computers can solve efficiently.

On the other hand, QKD uses the principles of quantum mechanics to distribute encryption keys between two parties in a way that any eavesdropping attempt is, in principle, detectable. The quantum keys are transmitted as individual photons over optical fibre.

More advanced operators are also deploying hybrid QKD–PQC architectures that create multi-layer quantum security protection: PQC handles scalable algorithm-based protection across the broader network estate, while QKD provides information-theoretic security for the highest-sensitivity links and use cases.

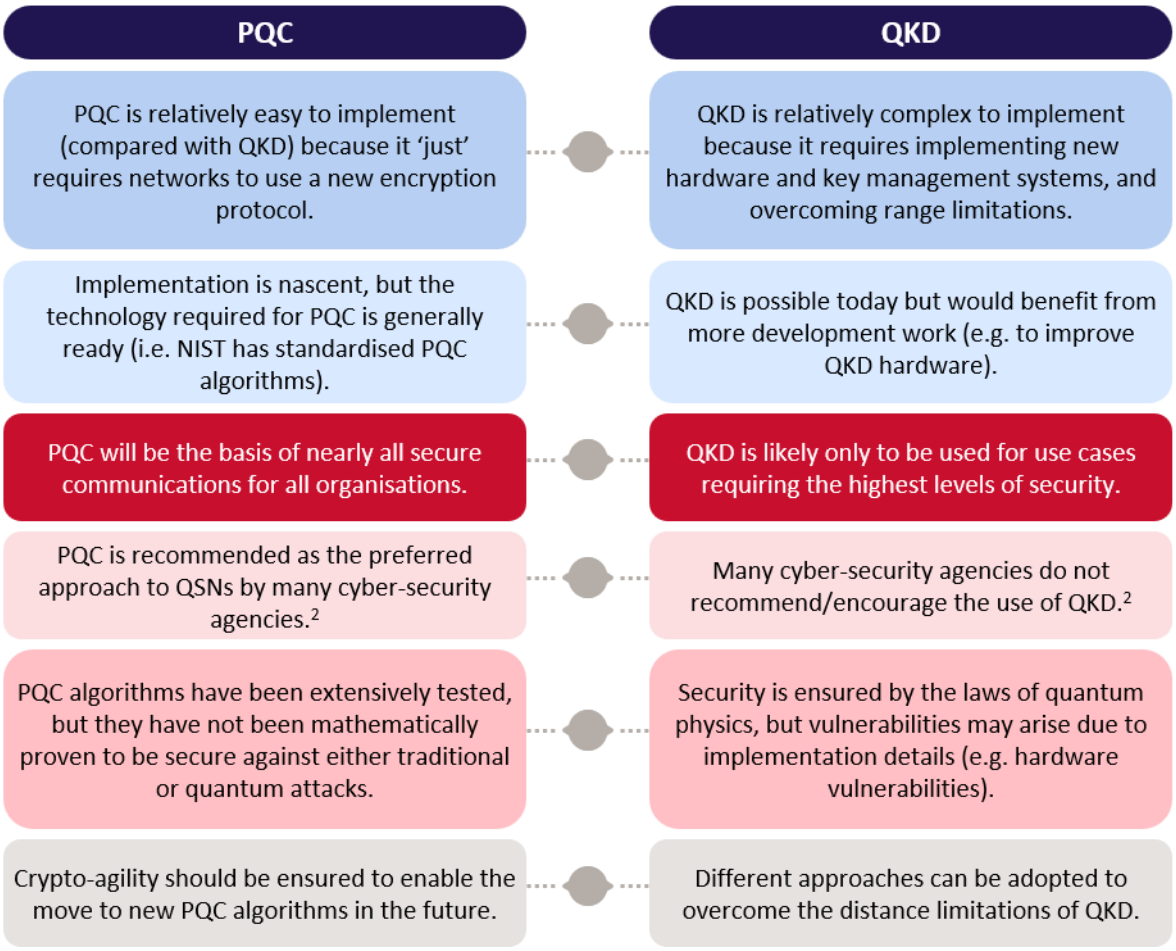
For more information, refer to Analysys Mason's *Quantum-safe networking: considerations and strategies* report.

What are the strategic implications of PQC and QKD?

PQC has inherent scalability advantages because it requires no dedicated quantum channels or specialised hardware deployment. This allows operators to mitigate long-term cryptographic risk without fundamental changes to network architectures. PQC is widely regarded as suitable for broad deployment across enterprise and consumer services.

QKD has the advantage of being theoretically secure, given that it derives its properties from quantum mechanics rather than computational hardness (that is, the difficulty of solving specific computational problems). However, QKD deployments involve significant hardware investments and integration costs. QKD technology is also still nascent and requires a lot more R&D to advance its capabilities – for example, the range of qubit transmission and QKD's interoperability with classical channels. Operators offering the technology tend to only provide it to premium customers, often on a use-case basis, rather than deploying it at scale.

Figure 1: Strategy considerations when using PQC and QKD



Source: Analysys Mason

What QSN solutions are available to telecoms operators?

QSN solutions comprise both hardware and software components.

Hardware includes:

- routers and switches with PQC support
- encryption appliances such as hardware security modules (HSMs) that implement PQC algorithms
- QKD hardware appliances deployed at endpoints and intermediary nodes

- satellites equipped to support QKD over long distances.

Software includes:

- platforms that implement and manage PQC algorithms
- key management system (KMS) software for QKD networks
- cryptographic bill of materials (CBOM) tools and scanning software capable of identifying the use of non-PQC algorithms across an organisation's estate.

What does the QSN supply chain look like?

The QSN ecosystem is highly fragmented due to the diversity of underlying technologies. Vendors typically fall into four categories:

- quantum technology specialists, including QKD hardware vendors and quantum key-management providers
- optical network equipment suppliers, which integrate QSN features into transport, routing and switching platforms
- cyber-security vendors, which embed PQC into firewalls, VPNs and security management systems
- cloud and platform providers, which enable quantum-safe connectivity across multi-cloud environments.

Figure 2: Key players in the QSN supply chain

Category	Vendor	QSN solution details
Quantum technology specialists	ID Quantique	A pioneer in QKD hardware, now acquired by IonQ
	Toshiba	Announced an integrated PQC + QKD solution in March 2025
	QuantumCTek	A leading Chinese QKD provider that deploys hybrid PQC/QKD infrastructure to support China Telecom's backbone network across 16 metropolitan areas
	QuantumXchange	Offers the Phio Trusted Xchange platform, which integrates PQC and QKD for secure key delivery
	CUbIQ	Developing a continuous-variable QKD (CV-QKD) transceiver in a compact QSFP-28 pluggable form factor, which would enable QKD integration directly into standard routers and switches
Optical network equipment suppliers	Cisco	Partnered with Orange Business in February 2026 to launch a managed PQC WAN offering on its 8000 Series Secure Routers, and is embedding PQC into its SD-WAN platform
	HPE Juniper Networking	Completed a proof-of-concept in September 2025 with CUbIQ, Coherent and Liberty Global on plug-and-play QKD on PTX Series Routers
Cyber security	Palo Alto Networks	Announced PQC support in PAN-OS 12.1 Orion in August 2025 for its fifth-generation firewalls, covering ML-KEM, ML-DSA, SLH-DSA, HQC, Classic McEliece, BIKE and FrodoKEM, and launched a joint Quantum-Safe Readiness solution with IBM in November 2025
	Fortinet	Updated FortiOS 7.6 in July 2025 with quantum-safe features, including ML-KEM and HQC support for FortiGate firewalls and Secure SD-WAN, plus QKD integration and hybrid mode capabilities

Category	Vendor	QSN solution details
	Thales	Prominent in digital security for government and enterprise, offering PQC-enabled hardware security modules (HSMs) and identity solutions
Cloud platform providers	Microsoft	Shipped PQC algorithms (ML-KEM, ML-DSA) natively into Windows 11 and .NET 10 as of November 2025. Actively collaborating with NIST, IETF, ISO and ETSI on standards alignment.
	IBM	Offers the Quantum Safe Migration Orchestrator (QSMO), an AI-driven platform used by IBM Consulting to help enterprises plan and execute multi-year quantum-safe transformations

Source: Analysys Mason

Other notable players include:

- Qunnect and LuxQuanta, which are focused on entanglement-based networking
- Nokia, Huawei, Ciena and Adtran are all upgrading optical and routing platforms with QSN capabilities, and are likely to be the primary channel through which operators make their transport and switching infrastructure quantum-safe
- Entrust, Zscaler, F5, Check Point are at various stages of embedding PQC into their security platforms and certificate management systems
- AWS and Google are both embedding PQC into TLS and key management services across their cloud platforms
- QuSecure provides end-to-end PQC orchestration for critical infrastructure and government systems via a cloud-based quantum-safe overlay.

Professional services providers and system integrators also play an important role in ensuring the interoperability of deploying solutions from various technology providers and multi-vendor solutions.

Where are operators today in their QSN deployments worldwide?

QSN adoption is advancing across all major regions, though deployment maturity varies significantly.

Asia–Pacific

- China Telecom's quantum communication network spans 16 major urban centres. Its 2030 Action Plan commits to a national space–ground integrated quantum communication network.
- SK Telecom has QKD deployed across 330km of 5G backbone infrastructure in South Korea alongside PQC for wireless and endpoint connections.
- Singtel's Hybrid Quantum-Safe Network integrates QKD and PQC to provide a flexible managed service solution for enterprises and critical industries.

Europe

- BT has moved from government-backed QKD trials to the commercial launch of a quantum-safe VPN in December 2023, developed in partnership with Arqit and Fortinet.

- Colt completed what it described as a world-first transatlantic PQC trial, transmitting 100Gbit/s traffic from London to New York over Google's Grace Hopper subsea cable.
- Deutsche Telekom leads the EU's EuroQCI programme and has demonstrated entangled photon transmission over 30km of metropolitan fibre.
- Vodafone UK is integrating PQC into its consumer-facing Secure Net service. It also co-founded the GSMA Post-Quantum Telco Network Taskforce with IBM.

North America

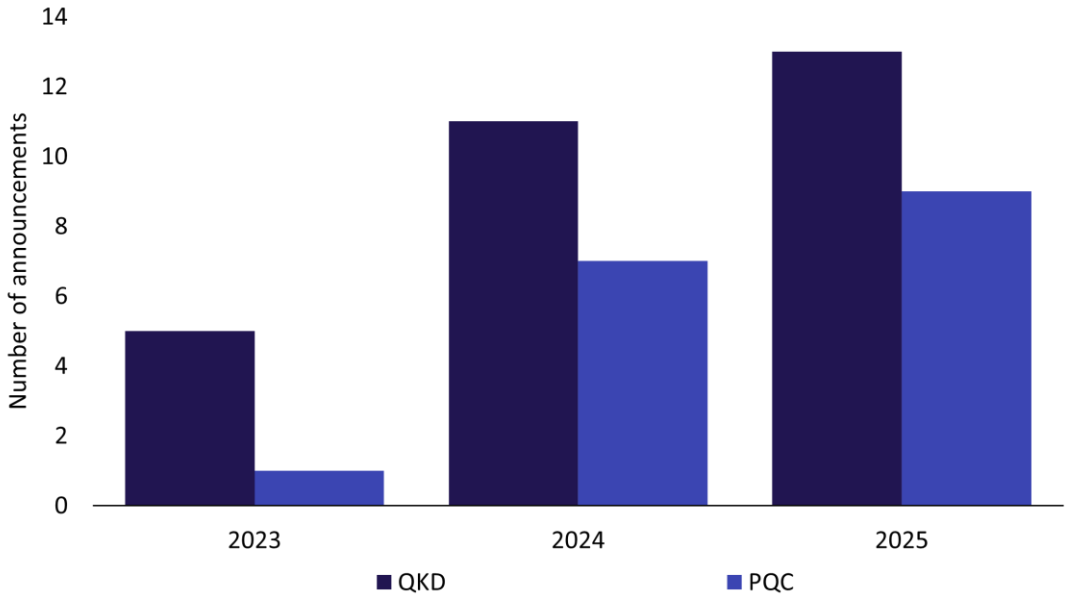
- AT&T has focused on PQC integration across its enterprise VPN and managed security portfolio, extending quantum-safe capabilities to its FirstNet public safety network.
- Verizon completed PQC trials on its backbone network and is contributing to the NIST and IETF standards processes.
- TELUS has positioned itself as Photonic's preferred Canadian telecoms partner for quantum data centres and encrypted quantum networking.

For more information, see Analysys Mason's *Operator quantum-safe networking strategies: case studies and analysis*, which evaluates 14 operators across Western Europe, North America, the Middle East and Asia–Pacific.

What are the main telecoms operator partnerships with QSN vendors?

Operators are partnering with vendors across the QSN ecosystem to accelerate innovation and deployment.

Figure 3: Number of PQC and QKD announcements from telecoms operators



Source: Analysys Mason

Several operators have taken the extra step of investing in equity stakes with key technology partners. This allows them to ensure deeper integration and have greater supply chain control, which in turn provides them with long-term influence over their quantum networking roadmap.

- SK Telecom invested USD65 million in ID Quantique in 2018. This equity stake established a co-development relationship that has underpinned most of SK Telecom's QKD deployment since.
- TELUS Global Ventures took a direct equity stake in Photonic as part of a CAD180 million funding round, converting what began as a network access arrangement into a full strategic investment. The deal positions TELUS as Photonic's preferred Canadian telecoms partner for quantum data centres and encrypted quantum networking.
- China Telecom acquired a 21.86% equity stake in QuantumCTek in March 2024. This deepened its integration with China's primary quantum research institutions and allowed it to secure direct control over its quantum hardware supply chain.

For more information, see Analysys Mason's *Telecoms operator quantum technologies partnership tracker*, which provides an overview of the partnerships between operators and vendors in the quantum technologies space.

What QSN solutions are operators offering enterprises and consumers today?

Enterprise-focused offerings currently dominate the market, driven by regulatory requirements and enterprise demand for forward-looking security. Many operators offer quantum-safe VPNs that embed PQC algorithms into managed firewall or VPN services. Others are launching quantum-secure

data centre interconnect (DCI) services, which combine QKD and PQC to protect sensitive workloads between facilities.

Some operators are also exploring quantum-safe services for consumers, typically by embedding PQC into existing mobile security products. However, consumer willingness to pay for quantum-safe features remains uncertain.

For more information, see Analysys Mason's *Operators' quantum-technology solutions for enterprises: trends and analysis 4Q 2025*.

Which standards are shaping the development and deployment of QSN solutions?

NIST published finalised standards for three PQC algorithms in August 2024: ML-KEM, for secure key exchange, and ML-DSA and SLH-DSA, both digital signature schemes used to verify the authenticity and integrity of messages and support quantum-safe certificate authorities. NIST has mandated that US federal agencies deprecate traditional public key encryption by 2030 and disallow it entirely by 2035, creating a hard timeline that will filter down through supply chains and international partners.

At the protocol level, the IETF has been instrumental in integrating PQC into TLS 1.3 and IPsec (IKEv2), the two most widely used protocols for securing internet and enterprise communications. This work ensures that widely used cryptographic libraries such as OpenSSL can support PQC, making the transition largely a software update for many organisations.

In mobile networks, 3GPP is working to incorporate quantum-safe algorithms into mobile network standards, with Release 20 set to introduce PQC support for 5G. 6G networks are expected to be quantum-safe by design from the outset.

Government cyber-security guidelines across multiple jurisdictions are adding further regulatory pressure. The EU recommends completing PQC migration for high-risk use cases by 2030 and for medium-risk use cases by 2035. The UK targets highest-priority migration by 2031, with full completion by 2035. In the USA, the National Security Agency's (NSA's) Commercial National Security Algorithm Suite 2.0 mandates that national security systems transition exclusively to NIST-standardised PQC algorithms by 2030 and explicitly excludes QKD from approved approaches for classified government use.

What should operators consider when building a QSN strategy?

Operators must determine whether to prioritise PQC, QKD or hybrid architectures, and how these would integrate with existing network infrastructure. Key considerations include scalability, cryptographic agility, operational complexity and alignment with standards timelines. A crypto-agile architecture where operators can substitute algorithms without redesigning the underlying system is increasingly a baseline requirement.

Operators should also align quantum-safe capabilities with defined customer needs and clear go-to-market strategies. This includes identifying target verticals, packaging QSN features into existing managed security or connectivity services, and using internal cryptographic migration programmes as the basis for commercially offered managed services.

Strategic partnerships with vendors and research institutions, and participation in standards bodies and national quantum initiatives, are essential to accelerate innovation. Joint pilots and testbeds allow operators to build operational experience and credibility. Operators that take an active role in shaping the ecosystem are better positioned to influence market direction and secure early commercial advantage.

Michelle Lam *(Senior Analyst) is a member of the Networks and Cloud research practice. She leads the Network Automation and Orchestration programme. Her research covers the competitive and strategic assessment of emerging technologies that are shaping next-generation network evolution, spanning network management, automation, orchestration and security. She particularly focuses on autonomous networking and quantum-safe networking.*