SECURING THE FUTURE

Quantum Computing's Impact on Telecom Security

Insights Report

September 2025

GLOBAL CYBERSECURITY FORUM | stc

Foreword

Mazen Alahmadi
stc;
Chairman of the 'Safeguarding Future Networks and Emerging Technologies' Knowledge Community

As quantum computing advances at a transformative pace, its implications for telecommunications and cybersecurity are profound. This emerging technology has the potential to revolutionize industries while simultaneously introducing unprecedented challenges to data security – meaning that organizations must adopt a proactive and forward-thinking approach to navigate the opportunities and risks posed by it.

This report represents the collective expertise and dedication of the 'Safeguarding Future Networks and Emerging Technologies' Knowledge Community. It is a timely resource for industry leaders, providing the tools and strategies needed to thrive while ensuring the integrity and security of global communications.

Contributors

- **Soufiane Zrira,** stc
- **Mahmood S. Elrefai,** stc
- **AbdulRazzak Shaikh,** stc
- **Zaki Alowini,** stc
- **Ian Keller,** Ericsson
- **Zygmunt Lozinski,** International Business Machines Corporation (IBM)
- **Lory Thorpe,** International Business Machines Corporation (IBM)
- **Marin Ivezic,** KPMG

Knowledge Community: Safeguarding Future Networks and Emerging Technologies

In an increasingly interconnected world, the evolution of next generation ICT technologies, such as 6G, has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities, safeguard its deployment, and to harness its capabilities for the benefit of society. The Knowledge Community "Safeguarding the Future Networks & Emerging Technologies" is committed to promoting and safeguarding current and future ICT networks, bringing together a diverse array of expertise from multiple stakeholder groups.

The community welcomes ICT providers, telecom companies, telecom industry players, cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of the ICT networks.

Contents

Useful Acronyms

Acronym	Definition
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
CRQC	Cryptographically Relevant Quantum Computer
QC	Quantum Cryptography
NISQ	Noisy Intermediate-Scale Quantum
FTQC	Fault-Tolerant Quantum Computing
QIS	Quantum Information Science
RSA	Rivest-Shamir-Adleman (Asymmetric cryptography)
ECC	Elliptic Curve Cryptography (Asymmetric cryptography)
AES	Advanced Encryption Standard (Symmetric cryptography)
DSA	Digital Signature Algorithm
NIST	United States' National Institute of Standards and Technology
APT	Advanced Persistent Threat
IoT	Internet of Things
CNI	Critical National Infrastructure
DV-QKD	Discrete Variable Quantum Key Distribution
CV-QKD	Continuous Variable Quantum Key Distribution
AQC	Adiabatic Quantum Computing
HNDL	Harvest Now, Decrypt Later
HSM	Hardware Security Module
PKI	Public Key Infrastructure
KMS	Key Management System
CA	Certificate Authority
CI/CD	Continuous Integration / Continuous Deployment
IR	Incident Response
DR	Disaster Recovery
SDO	Standard Development Organization

Executive Summary

Although in its infancy compared to other emerging technologies, such as artificial intelligence, quantum computing represents a groundbreaking shift in computational capabilities. It promises to usher in the long-anticipated 'quantum future,' an era of transformative advancements across industries, driven by the principles of quantum mechanics.

However, while quantum computing brings with it countless opportunities for telecommunications companies, it also presents challenges to traditional cryptographic standards and the security and confidentiality of data and communications. Cryptographically-relevant quantum computers (CRQC) will render widely used encryption algorithms obsolete, making calls, messages and broadband connections vulnerable to decryption. The catastrophic potential of this prospect, often referred to as Q-Day, means telecom providers must be proactive in adopting quantum-safe encryption that protects their infrastructure before threats materialize.

This insights paper explores the risks to telecom companies posed by a rapidly evolving quantum landscape, and proposes responses to mitigate them. It assesses the positive implications of quantum computing, including the potential to enhance real-time data analysis, traffic management, routing, and resource allocation – which will be essential for enabling more efficient services for applications such as augmented reality, cloud gaming, and mission-critical communications. The paper also examines the ability of quantum computing to break traditional encryption and compromise data integrity and confidentiality, underscoring the importance of transitioning to quantum-resistant cryptography to safeguard data transmission across mobile, cloud-based, and broadband networks.

Telecom providers should also modernize their infrastructure and business models to enable them to stay ahead of rapidly emerging quantum advances. The process of replacing or adapting legacy systems will require significant investment in upgrading network architectures, enhancing security frameworks, and aligning with changing regulatory requirements.

This insights paper outlines a strategic roadmap for telecom companies to become quantum-resilient. This includes implementing post-quantum cryptographic solutions, integrating quantum key distribution (QKD) where feasible, conducting cryptographic risk assessments, and fostering industry-wide collaboration to establish security standards. By taking proactive measures now, telecom operators can safeguard their networks, ensure regulatory compliance, and maintain customer trust in an era of rapid technological change.

1. Introduction

Scope and Objectives

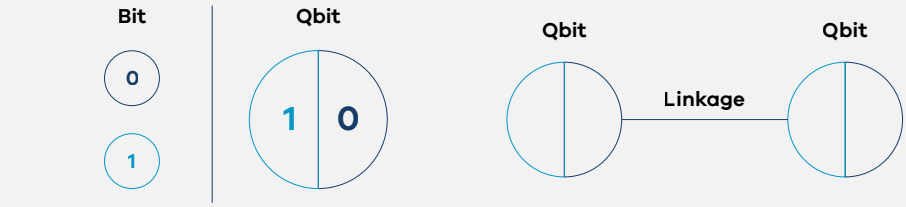
In providing a strategic overview of quantum computing and cybersecurity, this insights paper addresses a global audience spanning all fields within information and communications technology (ICT) and telecommunications. Quantum computing is evolving rapidly, and understanding its impacts will prove essential to capitalizing on opportunities, addressing challenges, and adapting to the transformation the technology is poised to deliver across various industries and security protocols.

The primary goal of this report is to equip its readers with the knowledge and insights needed to navigate the quantum landscape and make informed decisions about security strategies and investments. We will explore key concepts within quantum computing, its potential applications and disruptions in the technology and telecommunications industries, and the security challenges it poses.

Additionally, we will outline strategies for securing critical infrastructure, data and communications in the quantum era to ensure that organizations remain resilient and adaptive in the face of evolving cyber threats.

2. Understanding Quantum Computing

By using quantum mechanics to perform calculations at speeds that significantly outpace current computing technology, the emerging field of quantum computing has the potential to revolutionize the way telecoms companies store, process, and exchange information – presenting both opportunities and threats.



Superposition

You can add two or more quantum states and the result will be another valid quantum state. Conversely, you can also represent every quantum state as a sum of two or more other distinct states. This superposition of qubits gives quantum computers their inherent parallelism.

Process millions of operations simultaneously

Entanglement

The ability of qubits to correlate their state with other qubits. Quantum processors can draw conclusions about one particle by measuring another one.

Solve complex problems faster

Figure 1: Quantum computing's novel approach to computing

2.1 Quantum Computing's Mechanics

Quantum computers utilize the principles of quantum mechanics (Figure 1) to perform computations at speeds that significantly exceed those of classical computers for specific types of problems.

In contrast to existing computers, which process data sequentially using binary bits (0s and 1s), quantum computers use qubits to represent and manipulate information. By harnessing quantum phenomena, quantum computers can tackle complex challenges in fields such as optimization, cryptography, and materials science with unmatched efficiency.

2.2 Why Quantum Computing Matters to Telecommunications

Quantum technology has the potential to reshape telecom networks that rely on encryption, data transmission, and infrastructure security, unlocking new efficiencies in network optimization, spectrum management, and ultra-fast data processing. However, advancements in quantum technology could also make current encryption standards for securing mobile networks, IoT devices, and enterprise communications obsolete, exposing telecom providers to new security risks. As the industry progresses toward 6G and cloud-based telecommunications infrastructure, industry leaders must ready themselves for both the risks and opportunities that quantum computing will introduce.

Beyond revolutionizing encryption and computing capabilities, quantum technology is laying the foundation for a new type of secure global network: The quantum internet. Unlike existing networks, which depend on encryption methods that quantum computers could eventually break, a quantum internet would leverage quantum entanglement and Quantum Key Distribution (QKD) to establish end-to-end encryption that is inherently resistant to eavesdropping. This concept envisions a future where data is transmitted and stored securely using the fundamental laws of quantum mechanics, ensuring communication security that remains intact even in the face of powerful quantum adversaries.

Although still in its early stages, significant progress is already being made toward making the quantum internet a reality.

Researchers and industry pioneers are working on interconnecting quantum computers through entangled states, a breakthrough that could radically transform data security across telecom infrastructure. Some of the first real-world prototypes of quantum internet nodes are expected imminently with early testbeds already being developed across multiple regions.

3. The Quantum Security Threat

Quantum cyber-attacks have the potential to unravel the most advanced data encryption methods, endangering sensitive customer data and placing telecoms companies at risk of violating privacy and data protection regulations.

3.1 Breaking Traditional Encryption

The rise of quantum computing presents a serious threat to 5G network security due to its potential to break the encryption that safeguards these systems. Current encryption methods, like RSA and Elliptic Curve Cryptography (ECC), rely on complex mathematical problems that quantum computers could solve quickly using Shor's algorithm (Figure 2). If powerful quantum computers become a reality, they would easily crack the encryption protecting 5G networks, allowing attackers to intercept communications, access sensitive information, impersonate users, and compromise network integrity.

"Harvest Now, Decrypt Later" (HNDL) attacks are already intercepting and storing encrypted data today in anticipation of decrypting it once quantum computing reaches sufficient power. Sensitive communications, financial transactions, and national security data that rely on long-held encryption standards could be at risk even before large-scale quantum computers become a reality.

Industry estimates suggest that an advanced quantum computer could break RSA-2048 encryption within the next decade, increasing the urgency for organizations to transition to quantum-safe cryptography. Transitioning to quantum-resistant encryption methods will prove vital in ensuring the security of 5G as well as the next generation of networks.

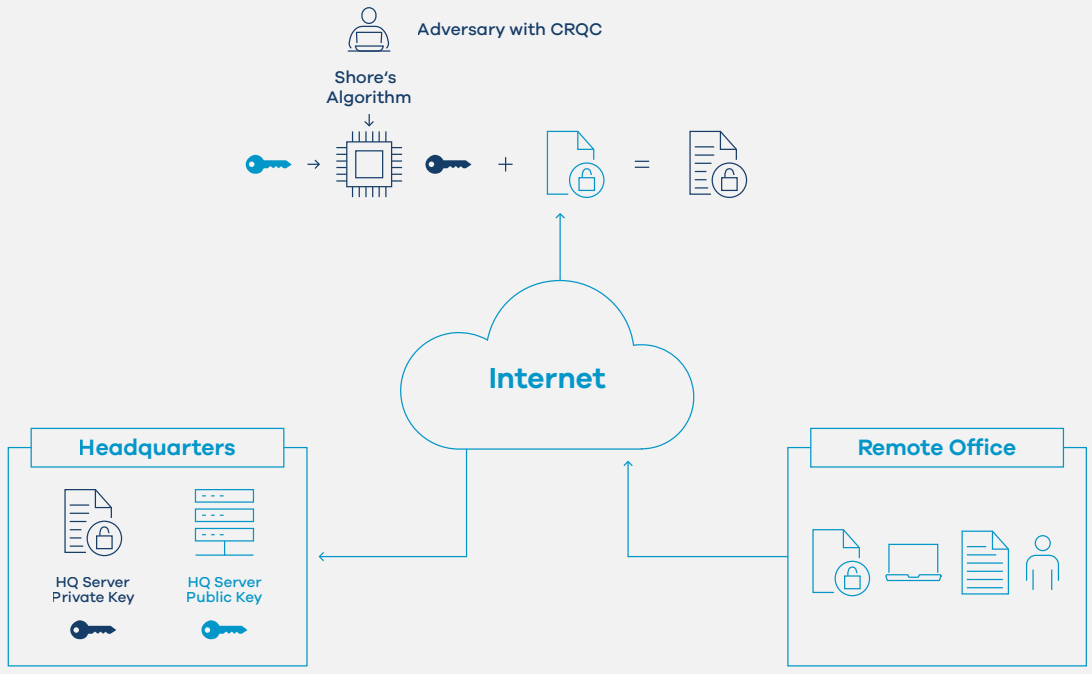


Figure 2: Quantum computing threatens the current state of cryptographic data protection

3.2 Risks to Data Integrity and Confidentiality

The rise of quantum computing presents significant risks to the privacy of subscribers. Customer communications and sensitive user data, such as customer records, mobile traffic, and 5G encryption keys could potentially be intercepted today and decrypted in the future.

This prospect highlights the critical need for telecommunications companies to counter the risks posed by quantum advancements by proactively adopting quantum-safe cryptography. Failing to do so may expose their systems, including digital signature schemes and even blockchain technology, to breaches that jeopardize both the confidentiality and integrity of user data.

3.3 Heightened Regulatory Compliance

In addition to technical vulnerabilities, telecoms companies may face regulatory and compliance pressures to adopt quantum-safe security standards.

As governments and regulatory bodies recognize the potential dangers of quantum computing, they are likely to implement frameworks that require telecoms to transition to enhanced encryption methods capable of withstanding quantum attacks. This approach aims to ensure that telecom networks remain resilient and secure, ultimately protecting customer data and maintaining trust in digital communications.

4. Reshaping Telecom Security

Quantum computing presents a serious risk to current cybersecurity methods and best practices, requiring telecoms companies to proactively adopt newer technologies and train employees to safeguard sensitive data, as the challenges become ever more sophisticated.

4.1 How Quantum Computing Will Proliferate

Telecom providers will need to integrate post-quantum encryption to safeguard against quantum-powered cyber threats, ensuring that sensitive data remains protected even as quantum decryption capabilities advance.

Recognizing that IoT networks and connected devices will be particularly susceptible to quantum-enabled attacks, key industry players have begun developing and testing quantum-safe security solutions. These initiatives focus on integrating post-quantum cryptography into telecom infrastructure, ensuring long-term resilience against emerging cryptographic vulnerabilities. For instance, one emerging solution is quantum key distribution (QKD), which offers theoretically unbreakable encryption by detecting any attempts to intercept transmitted keys.

Beyond individual initiatives, industry-wide collaborations are also accelerating the transition to quantum-safe telecom security. Leading global telecom and technology firms have formed a dedicated task force comprising dozens of operators and technology providers to establish industry-wide guidelines for assessing and mitigating quantum risks.

Service providers and operators are likely to experience a domino effect as they grapple with the overall impact of quantum computing on telecommunications: The possibility of enhanced communications and a theorized 'quantum internet' will drive efforts to develop more secure networks while also proliferating new technologies and services, fostering innovation and economic growth.

4.2 Key Risks for 5G and Cloud-Based Telecom Services

The immense potential of quantum computing comes hand-in-hand with the need to anticipate and adapt to potential disruptions in existing telecommunications technologies.

The first major wave of disruption will likely take the form of a 'cryptographic catastrophe,'[1] where the core cryptographic infrastructure used to protect customer data and communications becomes vulnerable to quantum attacks, making existing encryption standards redundant and requiring a mass transition to quantum-resistant cryptography. Telecom companies, many of which are already moving to cloud-based infrastructure on platforms like Amazon Web Services (AWS) and Azure, must prioritize quantum-safe encryption before quantum computers reach the scale necessary to break current encryption standards – a prospect often referred to as Q-Day.

Beyond security, legacy infrastructure built for classical computing may struggle to handle the demands of a quantum-powered future, necessitating substantial investments in modernization. To stay ahead, telecom providers will need to invest in future-proof security frameworks, upgrade network architectures and adapt business models to remain competitive in the quantum era.

4.3 Additional Challenges and Risks

The shift to quantum computing in telecommunications presents significant operational and investment challenges. The development and subsequent deployment of quantum-resistant cryptography across vast telecommunication networks and upgrading legacy infrastructure to support quantum protocols will require substantial capital and careful execution to avoid service disruption.

Workforce readiness is another pressing concern. Existing skillsets currently focused on classical cryptography and network management will need to be augmented with an understanding of post-quantum cryptography and the unique challenges of managing quantum-enabled networks. Additionally, the persistence of a skills shortage will prolong the industry's vulnerability window, during which data can be stolen and decrypted as a result of quantum advances.

This vulnerability window poses a significant security risk, making it imperative for telecom companies to integrate quantum-safe encryption into their networks and ensure a seamless and time-bound migration to post-quantum security standards.

5. Securing Critical Infrastructure

A measured approach to securing telecoms infrastructure that ensures organizations are in lockstep with global protocols and have considered every contingency is critical to building a more resilient security architecture.

5.1 Proactivity is Key

Given the elevated levels of risk posed by cryptographic-relevant quantum computers (CRQC) to telecommunications infrastructure, quantum-resistant solutions should be broad-based and must include:

- **Updating security standards:** International telecom standards bodies (3GPP, ETSI) are already adapting for a post-quantum world. Telecoms companies must align with these evolving standards to maintain global interoperability
- **Securing software and hardware:** Suppliers must integrate Post-Quantum Cryptography (PQC) into firmware updates, authentication mechanisms, and critical software to prevent vulnerabilities
- **Cloud and network security:** Telecom providers migrating to cloud services must ensure post-quantum encryption is embedded in their security architecture to protect sensitive customer data
- **Managing the transition:** A phased, strategic rollout of PQC is essential to avoid security gaps. Companies should verify vendor roadmaps, upgrade cryptographic libraries, and test solutions across their networks for seamless integration

6. Protecting Data and Communications

Ensuring the seamless integration and resilience of telecom networks across borders is vital for safeguarding data and communications. To address emerging quantum threats, several initiatives are leveraging cutting-edge encryption technologies to enhance security, but challenges remain.

6.1 Maintaining Data and Network Integrity

In today's interconnected world, telecommunications companies are critical in facilitating seamless communication and data exchange across global networks. Protecting data and communications is vital not only for ensuring customer trust but also for maintaining the integrity of the network infrastructure. Protecting data and communications includes:

- **Data confidentiality:** Protection from unauthorized access or disclosure
- **Data authentication:** Certifying the origin of the data
- **Data integrity:** Protecting data accuracy and consistency over the data lifecycle
- **Data non-repudiation:** Providing assurance that a communication was sent and received by communicating parties

As digital services evolve, telecoms must prioritize robust security measures to safeguard sensitive information against both current and emerging threats, particularly in the context of quantum advancements. The value of data within the telecommunications sector cannot be understated. Data acts as a vital asset for telecoms companies, influencing decision-making and driving business strategies. With the increasing threat of malicious actors – including those with quantum computing capabilities – telecoms companies face unique challenges in securing data at rest, in transit, and in use.

This section examines how effective protection technologies can ensure data confidentiality, authentication, integrity and non-repudiation throughout their lifecycle. As technologies evolve, telecoms companies must adopt a comprehensive security strategy that accounts for both current cybersecurity threats and future quantum risks, ensuring networks remain resilient and reliable.

6.2 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a secure technology that generates and shares encryption keys between two parties (a transmitter and a receiver) through specialized communication links, such as optical fibers or free space. While optical fibers provide more stability and lower signal loss, free space offers better range and flexibility.

QKD is notable for its ability to detect eavesdropping attempts and is not influenced by an adversary's computing power due to the fundamental laws of quantum mechanics.

The deployment of QKD networks is no longer theoretical – real-world implementations are already taking shape across multiple regions. Some notable examples include:

- **The Beijing-Shanghai QKD Backbone:** One of the largest quantum-secure networks in the world, providing ultra-secure communication between major cities in China
- **The SwissQuantum Network:** A long-standing QKD testbed demonstrating secure quantum communication applications
- **The EU OpenQKD Initiative:** A multi-country effort to test and integrate QKD solutions into modern telecom networks

Future advancements in QKD are also being actively researched, with significant industry focus on reducing infrastructure costs. Innovations like photonic integration, satellite-based QKD, and co-propagation of quantum and classical signals in optical fiber networks are expected to drive widespread adoption, making quantum-secure communications more accessible and scalable for telecom providers.

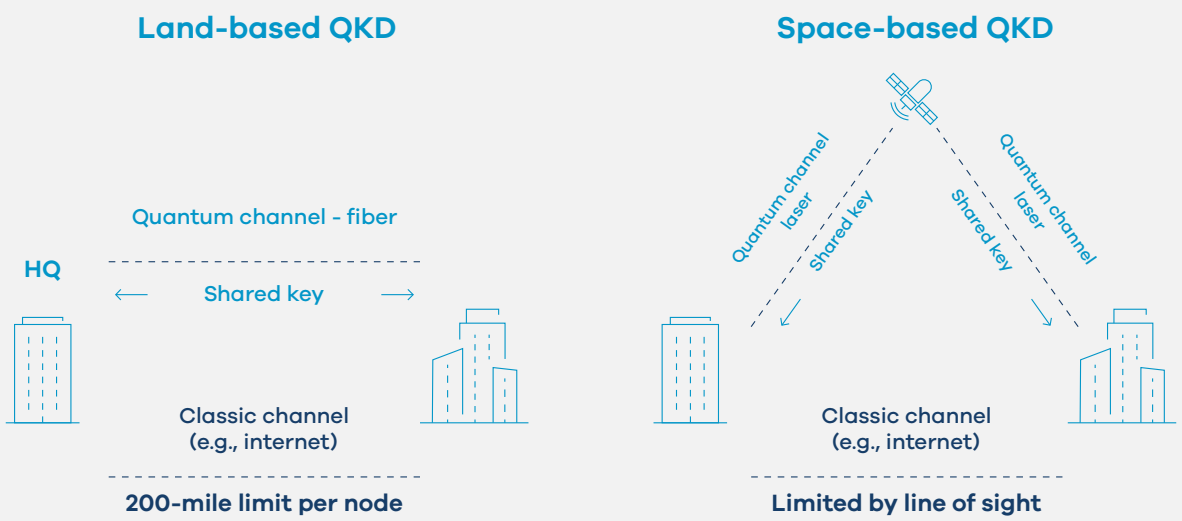


Figure 3: Quantum Key Distribution encryption keys are shared through specialized communications links

While recent advancements in QKD have paved the way for its application in telecoms, challenges remain. These include compatibility with existing systems, high costs of necessary technology, and ongoing standardization efforts. Addressing these challenges is crucial for the wider adoption of QKD in secure communications.

6.3 Quantum-Secure Communication Protocols

QKD utilizes principles of quantum mechanics to ensure secure communication without relying on the difficulty of specific mathematical problems. The main types of QKD are discrete variable (DV-QKD) and continuous variable (CV-QKD), both of which offer unique advantages for secure data transmission. Hybrid systems combining both methods are also being researched.

Standardization of QKD is crucial for its broader adoption in telecommunications, facilitating industrial-scale deployment and interoperability. Various organizations, including ETSI and ISO/IEC, are working on establishing QKD standards to enhance security in telecommunications networks and contribute to the overall cybersecurity landscape, addressing key issues like module security and network interoperability.

7. Regulatory and Compliance Considerations

As global stakeholders begin to respond to the incoming challenges posed by quantum computing, telecoms companies must continuously assess and invest where necessary to stay ahead of emerging threats. It is equally critical that they channel efforts towards remaining compliant in an ever-evolving regulatory landscape.

7.1 How Regulation Will Shape Telecom's Quantum Security Strategy

Governments and regulatory bodies are responding to emerging quantum challenges by introducing more comprehensive standards and security measures. The anticipated release of the United States' National Institute of Standards and Technology's Post-Quantum Cryptography (PQC) standards is a significant impetus for telecom leaders to reassess their security measures and align with upcoming technological advancements.

Several major telecommunications standards organizations have already introduced frameworks and guidelines to assist operators in transitioning to quantum-safe networks.

The Global System for Mobile Communications (GSMA), for instance, has published 'Post Quantum Cryptography – Guidelines for Telecom Use Cases,' outlining best practices for adopting quantum-resistant cryptographic methods across mobile networks, cloud-based services, and IoT infrastructure.

Similarly, the International Telecommunication Union (ITU) has developed ITU Y.3800, a foundational standard defining the architecture of Quantum Key Distribution (QKD) networks to ensure that telecom security can evolve alongside quantum advancements.

These initiatives highlight a clear regulatory shift that demands early compliance efforts from telecom operators to avoid security and operational disruptions as quantum computing evolves.

To remain competitive and compliant, telecom decision-makers should focus on enhancing their infrastructure to support quantum-resistant cryptographic systems, prioritizing investments in technology and talent.

7.2 How Telecom Leaders Can Stay Ahead?

The rapid pace of quantum computing advancements necessitates an agile approach to security, where firms must regularly evaluate and adapt their strategies. By viewing these regulatory challenges as opportunities for innovation rather than obstacles, telecom leaders can effectively navigate the complexities of quantum security.

8. Building Quantum-Resilient Organizations

The accelerated rate of progress toward quantum computing necessitates a swift and versatile approach to securing the resiliency of telecom operators, encompassing international standards and developments, continuous testing, and workforce readiness.

8.1 Why Telecom Providers Must Act Now

While earlier cryptographic upgrades evolved gradually, the significant technological advance that quantum computing represents requires a rapid, industry-wide shift to post-quantum cryptography. Delaying action will expose networks to data breaches, regulatory penalties, and operational disruptions, while competitors who prioritize quantum resilience will gain a security and business advantage.

Leading telecom security executives have already begun sounding the alarm on the urgency of preparing for quantum risks, and industry leaders emphasize that the finalization of quantum-safe standards will serve as a wake-up call for many organizations that have yet to take action. According to senior R&D executives at a major European telecom provider, regulatory clarity will accelerate adoption, prompting companies to start their transition to post-quantum security. Additionally, technology and security executives from a global telecom operator stress the importance of early experimentation with quantum technologies, stating that organizations must test quantum-resistant encryption solutions now to ensure a smooth and secure transition before quantum threats become a reality. These insights from industry leaders reinforce the growing consensus: Waiting is not an option, and proactive preparation will determine which telecom companies maintain security leadership in the post-quantum era.

The ability to swiftly transition between encryption standards – crypto-agility – will be key. Telecom operators must embed flexible, upgradeable cryptographic systems into their infrastructure to ensure long-term security and compliance with evolving global standards.

8.2 Key Actions for Telecom Companies to Ensure Quantum Resilience

To build quantum resilience, telecom providers must take the following key actions to safeguard their networks and ensure a smooth transition to post-quantum security:

- **Map and prioritize cryptographic vulnerabilities:** Identify critical telecom assets that rely on encryption, from mobile networks to cloud-based customer data
- **Adopt crypto-agile systems:** Ensure telecom infrastructure supports seamless cryptographic updates without disrupting operations
- **Engage with industry standards bodies:** Stay aligned with 3GPP, ETSI, and other telecom security frameworks adapting to quantum threats
- **Upgrade security across the supply chain:** Require hardware and software vendors to integrate quantum-resistant cryptography in firmware, authentication systems, and cloud services
- **Invest in workforce readiness:** Equip security teams with the knowledge to manage PQC transitions and anticipate evolving quantum threats

Given the uncertainty around the timeline for the development of large-scale quantum computing, telecom providers must prepare for a staged transition rather than a single overhaul. This means:

- **Mapping** out cryptographic dependencies across their entire infrastructure to understand which assets need post-quantum upgrades first
- **Testing** hybrid encryption models, where post-quantum cryptographic solutions run in parallel with classical encryption to ensure security during the transition period
- **Collaborating** with standards bodies to stay ahead of regulatory requirements and ensure a smooth migration to quantum-safe protocols

A phased approach to post-quantum security is critical, as large-scale cryptographic changes can take 5 -10 years to fully implement.

Telecom providers that take a proactive and structured approach to quantum security today will be far better positioned to mitigate risks compared to those that wait until the quantum threat is imminent - ensuring regulatory compliance and building long-term trust with customers in an increasingly digital world.

9. Conclusion

The rise of quantum computing is an imminent reality that will redefine data security and telecommunications.

The financial consequences of cybersecurity failure in the quantum era are significant. By 2031, cybercrime is projected to cost the global economy $265 billion annually, with weak encryption being a major contributing factor. As quantum advancements shorten the lifespan of traditional cryptographic protections, telecom providers face an urgent imperative to invest in quantum-safe solutions now, rather than react to crises later.

5-10
years to implement full cryptographic transitions

Cryptographic transitions are long-term projects, often requiring 5 - 10 years to implement fully. With the emergence of large-scale quantum computers, organizations must act quickly to transition to quantum-resistant cryptography, protecting critical infrastructure, communications, and sensitive data before the quantum threat materializes.

The transition to fault-tolerant quantum computing (FTQC) is already underway, with recent breakthroughs in logical qubits and error correction suggesting the timeline of development is accelerating. Some experts estimate that Q-day - the moment quantum computers break today's encryption – will occur within the next decade. As quantum capabilities scale, it is not a question of if but when they will become cryptographically relevant.

Organizations that delay preparations risk catastrophic data breaches, as attackers may already be stockpiling encrypted data to decrypt once quantum technology matures. Telecom providers, cloud operators, and enterprises handling vast amounts of private and financial information must proactively integrate quantum-safe encryption and develop crypto-agility strategies to stay ahead of evolving risks. This means conducting cryptographic risk assessments, upgrading legacy systems, and adopting emerging security technologies like quantum key distribution (QKD) where feasible.

The cost of inaction is clear: Failing to adapt will leave organizations exposed to irreversible data compromises. Now is the time to invest, innovate, and prepare. Organizations that embrace quantum security today will not only safeguard their operations but also position themselves as leaders in the next era of digital trust.

Endnotes

1. Roger A. Grimes, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto, 2019

GLOBAL CYBERSECURITY FORUM

stc