Q→NU

QUANTUM THREAT INTELLIGENCE REPORT: **TELECOMMUNICATIONS INDUSTRY 2026 - 2035**

THREAT LEVEL
CRITICAL

The global telecommunications industry faces an existential quantum cryptographic crisis with 8.4 billion mobile subscribers, 1.5 billion fixed broadband connections, and $1.8 trillion in annual revenue operating on encryption vulnerable to quantum computers expected 2026-2031.

8.4 Billion	1.5 Billion	$1.8 Trillion
Mobile subscribers	Fixed broadband connections	Annual revenue

KEY FINDINGS:

- **Infrastructure Vulnerability** 5G networks spanning 200+ countries, 485+ submarine cables carrying 99% of intercontinental data, 4,000+ satellites at risk during 4-10 year quantum exposure window
- **Financial Impact** $250-400B global industry cost for quantum transition; $500B-1T breach exposure across operators, infrastructure providers, and national security systems
- **Active Attacks** "Harvest Now, Decrypt Later" (HNDL) collecting encrypted traffic on submarine cables, 5G core networks, satellite links NOW
- **Global Mandates** EU NIS2 requires quantum-safe telecom infrastructure by 2030; US CISA mandates federal telecom systems by 2027; China requires quantum-secure communications by 2026
- **Timeline Crisis** Telecom infrastructure deployed in 2025 operates until 2035-2045, far beyond quantum computer arrival (2026-2031); submarine cables have 25-year lifespans

info@qnulabs.com

1.0 | GLOBAL REGULATORY MANDATES & TIMELINES

1.1 | EUROPEAN UNION

NIS2 Directive + DORA + 5G Security Toolbox:

https://digital-strategy.ec.europa.eu

Telecom-Specific Mandates:

5G Core Networks

Quantum-safe by 2027; mandatory for all operators serving EU markets

Submarine Cable Systems

PQC-compliant encryption for all EU landing stations by 2028

Supply Chain Security

EU-approved quantum-safe equipment vendors only

Critical Infrastructure

Telecom designated as essential service under NIS2 with mandatory incident reporting

Roaming & Interconnect

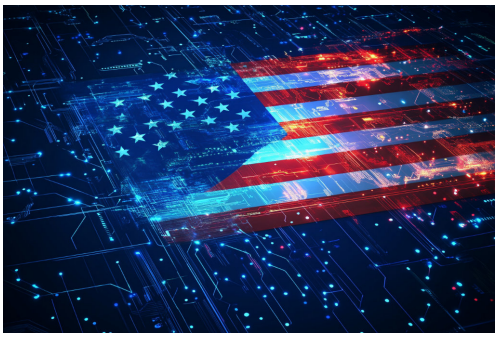
Cross-border quantum-safe signaling protocols required by 2029

Timeline & Penalties:

Dec 2026	All Member States begin PQC transition; cryptographic inventory complete for all telecom operator
Dec 2027	5G core networks support crypto-agility; quantum-safe signaling deployed
2030	All critical telecom infrastructure fully quantum-safe; submarine cables, satellite gateways, international interconnects
2035	Complete migration of all feasible legacy systems; end-of-life for quantum-vulnerable equipment

Penalties: Up to €10M or 2% of global annual revenue for non-compliance; service suspension for critical violations Source: EU NIS2 Directive

1.2 | UNITED STATES



Federal Mandates & CISA Directives:

https://digital-strategy.ec.europa.eu

- **NSM-10 (National Security Memorandum):**

  All federal agencies will mitigate quantum risk in telecom systems by 2035

  Priority: Defence communications, intelligence networks, emergency services

- **OMB M-23-02:**

  Annual quantum-vulnerable system inventories for all federal telecom contracts through 2035

  Mandatory reporting: carrier networks, satellite communications, secure voice systems

- **EO 14144 (January 2025):**

  TLS 1.3 quantum-safe for all federal telecom connections by January 2, 2030

  CISA/NSA product categories for telecom equipment by December 1, 2025

- **NSA CNSA 2.0 (Commercial National Security Algorithm Suite):**
  New National Security Systems telecom acquisitions PQC-compliant by January 1, 2027

  Full compliance across DoD, Intelligence Community, critical infrastructure by 2033

NIST Standards (August 2024):

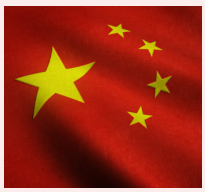
https://www.nist.gov/pqc

Standard	Algorithm	Telecom Application
FIPS 203	ML-KEM (Kyber)	Key encapsulation for 5G sessions, VPN tunnels
FIPS 204	ML-DSA (Dilithium)	Digital signatures for firmware, network configuration
FIPS 205	SLH-DSA (SPHINCS+)	Long-term certificates, root CA signing

Source: NSA CNSA 2.0 Suite

1.3 | OTHER MAJOR MARKETS

CHINA



Mandating quantum-safe 5G/6G networks by 2026-2027; **2,000+ KM quantum communication backbone operational** (Beijing-Shanghai); integrating QKD with telecom infrastructure at the national scale

UNITED KINGDOM

NCSC clear Post Quantum Cryptography (PQC) roadmap; **critical telecom infrastructure quantum-safe by 2030**; BT, Vodafone, Virgin Media mandated compliance; submarine cable landing stations prioritised.

JAPAN

$7.4B quantum investment; NTT, KDDI, SoftBank PQC integration targeting 2027-2028; satellite quantum communications trials ongoing; 6G quantum-native architecture development

INDIA

₹6,003.65 crore National Quantum Mission; indigenous quantum security focus 2025-2030; BSNL quantum-safe network pilots; Defence and government telecom prioritization; IIT collaboration for standards

Source: India's National Quantum Mission

2.0 | THREAT LANDSCAPE & ATTACK VECTORS

2.1 | CRYPTOGRAPHIC VULNERABILITIES

Protocol	Telecom Usage	Quantum Attack Risk
Quantum Attack Risk	SIM authentication, core network signalling, VoLTE	CRITICAL - Shor's algorithm
ECC (P-256)	5G NAS/AS encryption, IPsec VPNs, certificate chains	CRITICAL - Shor's algorithm
AES-128/256	User data encryption, backhaul links, optical fibre	HIGH - Grover's algorithm
TLS/SSL	Internet connectivity, API security, and management interfaces	CRITICAL - Both algorithm
PKI/X.509	User data encryption, backhaul links, optical fibre	CRITICAL - Both algorithm

Breakthrough Alert:

RSA-2048 breakable with only 372 physical qubits - significantly accelerates threat timeline for all telecom encryption. Source: Arxiv, Cornell University

2.2 | CRITICAL ATTACK VECTORS

A | 5G/6G Core Network Compromise

- **Scale:**
  200+ countries, 1,500+ operators, 8.4 billion subscribers at risk
- **Targets:**
  AMF, SMF, UDM, AUSF, PCF, UPF, NEF functions - all using vulnerable PKI
- **Impact:**
  Complete control plane interception, subscriber data exposure, service manipulation
- **Result:**
  Mass surveillance capability, subscriber location tracking, call/data interception

B | Submarine Cable Interception

- **Infrastructure:**
  485 cables, 1.4 million km length, carrying 99% intercontinental internet traffic
- **Impact:**
  Nation-state intelligence collection, corporate espionage, financial data theft
- **Vulnerability:**
  Landing stations, repeaters, and cable taps currently undetectable
- **Timeline:**
  25-year cable lifespans mean 2025 deployments vulnerable until 2050

C | Satellite Network Exploitation

- **Systems:**
  4,000+ LEO/MEO/GEO satellites, Starlink, OneWeb, Iridium, Inmarsat, government constellations
- **Impact:**
  Maritime, aviation, military, emergency communications compromise
- **Exposure:**
  Uplink/downlink encryption, ground station communications, inter-satellite links
- **Risk:**
  Space-based infrastructure impossible to physically secure or upgrade post-launch

D | Radio Access Network (RAN) Manipulation

- **Equipment:**
  Millions of cell towers, small cells, Distributed Antenna Systems (DAS) globally
- **Result:**
  Rogue base station attacks at scale, IMSI catching, traffic redirection
- **Method:**
  Quantum breaks RAN authentication protocols (3GPP TS 33.501)
- **Safety:**
  Emergency services (E911, eCall, 112) vulnerable to false alerts or blocking

E | Network Function Virtualization (NFV) & SDN Attacks

- **Architecture:**
  Cloud-native 5G, virtualized network functions, software-defined networking
- **Impact:**
  Complete network reconfiguration, policy manipulation, service denial
- **Vulnerability:**
  Orchestrators (ONAP, OSM), controllers, VNF managers using standard PKI
- **Supply Chain:**
  Hyperscaler clouds (AWS, Azure, GCP) hosting telecom infrastructure

Source: 3GPP Security Specifications

2.3 | "HARVEST NOW, DECRYPT LATER" ACTIVE THREATS

Currently Being Collected
(High-Confidence Intelligence):

- ✓ Encrypted submarine cable traffic (transatlantic, trans-Pacific, Europe-Asia routes)
- ✓ 5G core network signalling data (authentication, session management, handovers)
- ✓ Satellite communications (military, government, corporate), including encrypted links
- ✓ VoLTE/VoNR voice communications, SMS/RCS messaging metadata and content
- ✓ IoT/M2M traffic (industrial, smart cities, critical infrastructure control systems)
- ✓ Network equipment configuration data, operator intellectual property, infrastructure plans

Future Impact
(Post-Quantum 2026-2031):

- ✓ 5-25 years of historical telecom intelligence exposed (retroactive surveillance capability)
- ✓ Complete subscriber location history, calling patterns, and relationship graphs revealed
- ✓ National security communications compromised (diplomatic, military, intelligence)
- ✓ Critical infrastructure vulnerabilities systematically identified and exploitable

Threat Attribution:
China PLA Strategic Support Force, Russia FSB/GRU, North Korea Lazarus Group. Source: US DIA Threat Assessment

3.0 | QUANTUM COMPUTING TIMELINE & CAPABILITIES

3.1 | CURRENT STATE (February 2025)

IBM

Quantum System Two with 1,121 qubits; roadmap to 10,000+ qubits by 2026

Google

Willow chip achieving quantum computational advantage; error correction breakthroughs

IonQ

64-qubit commercial systems available via cloud; partnerships with telecom providers

China

Massive state quantum investment; 2,000 KM+ operational quantum network infrastructure

Source: McKinsey Quantum Report and other

3.2 | PROJECTED CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTER (CRQC) TIMELINE

Year	Capability	Telecommunications Impact
2026	500–1,000 logical qubits	Early vulnerabilities in legacy 3G/4G encryption; satellite uplinks at risk
2027–2028	1,000–2,000 logical qubits	5G core network signalling compromise possible; VPN tunnels breakable
2029–2030	2,000–5,000 logical qubits	Global infrastructure-wide exposure; submarine cables are fully vulnerable
2031+	5,000+ logical qubits	Complete cryptographic security failure across all telecom systems

4.0 | QUANTUM SECURITY USE CASES FOR TELECOM OPERATORS

Quantum security technologies are not just defensive measures—they enable new revenue streams and competitive differentiation for telecom operators. Here are critical use cases:

1 Quantum Security as a Service (QSaaS)

- Offer premium quantum-safe connectivity to high-value enterprise clients (banks, governments, defence contractors)
- Deliver end-to-end encrypted channels using QKD and PQC over existing fiber infrastructure
- Generate new revenue streams with ARPU increases of 25-40% for quantum-protected services
- Differentiate from competitors with military-grade security offerings

2 Secure Data Centre Interconnects

- Protect high-value data transfers between colocation facilities and enterprise data centers
- Enable quantum-safe hybrid cloud connectivity for financial services and healthcare
- Secure metro and regional dark fiber networks with QKD over existing infrastructure
- Provide Layer 1/Layer 2 quantum-secure transport for hyperscaler cloud providers

3 Government & Defence Communications

- Deploy quantum-safe networks for national security agencies, defence ministries, intelligence services
- Secure diplomatic communications between embassies and foreign ministry headquarters
- Enable classified information transfer over civilian telecom infrastructure
- Provide backup quantum-secure channels for emergency response and disaster recovery

4 Financial Services & Banking Networks

- Protect high-frequency trading (HFT) connections between exchanges and trading firms
- Secure interbank settlement networks (SWIFT, FedWire, CHIPS)
- Enable quantum-safe mobile banking and digital payment infrastructure
- Protect customer transaction data against HNDL attacks threatening long-term confidentiality

5 Critical Infrastructure Protection

- Secure SCADA/ICS communications for power grids, water systems, transportation networks
- Protect smart grid communications from quantum-enabled manipulation
- Enable quantum-safe IoT connectivity for industrial automation and smart cities
- Secure oil & gas pipeline monitoring and control systems

6 Healthcare & Medical Data Protection

- Protect electronic health records (EHR) and patient data against future quantum decryption
- Secure telemedicine and remote surgery communications
- Enable quantum-safe medical research data sharing between institutions
- Protect genomic data and personalised medicine information (50+ year confidentiality requirement)

7 5G/6G Network Core Security

- Deploy quantum-safe authentication for network slicing and multi-tenancy
- Secure virtualised network functions (VNF) and containerised workloads
- Protect Software-Defined Network (SDN) controllers and orchestrators
- Enable quantum-native architecture for future 6G networks

8 Submarine Cable & International Gateway Security

- Retrofit landing stations with quantum-safe encryption for intercontinental traffic
- Protect consortium cable systems against nation-state interception
- Secure international roaming agreements with quantum-safe signaling
- Enable quantum-protected content delivery networks (CDN) for global streaming

9 Enterprise VPN & Secure Access

- Offer quantum-safe SD-WAN and MPLS VPN services for multinational corporations
- Provide quantum-protected remote access for hybrid workforce environments
- Secure branch office connectivity with quantum-safe IPsec tunnels
- Enable zero-trust network access (ZTNA) with quantum-resistant cryptography

10 Satellite & Space Communications

- Protect high-frequency trading (HFT) connections between exchanges and trading firms
- Secure interbank settlement networks (SWIFT, FedWire, CHIPS)
- Enable quantum-safe mobile banking and digital payment infrastructure
- Protect customer transaction data against HNDL attacks threatening long-term confidentiality

Read more: QNu Labs Telecom Solutions

QNU LABS: PROVEN QUANTUM-SAFE TELECOM DEPLOYMENTS

India's First Commercial Quantum-Safe Network:

QNu Labs partnered with one of India's leading telecommunications operators to deploy the nation's first commercially manageable quantum-safe network, combining **Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) across a multi-city infrastructure.**

The deployment, spanning over 6 months with zero operational disruption, secured high-value enterprise customers demanding quantum-resistant connectivity.

Using a hybrid QKD-PQC architecture with NIST-compliant ML-KEM algorithms, indigenous Quantum Random Number Generators (QRNG), and Digital QKD for distance-unlimited scalability, the solution integrates seamlessly with existing Cisco, Fortinet, and ADVA hardware.

The implementation provides true quantum-safe protection over the operator's existing optical fibre infrastructure without requiring a network overhaul.

This deployment represents a breakthrough in commercial quantum security, enabling the telecom operator

- to offer Quantum Security as a Service (QSaaS) to financial institutions and government agencies while positioning them as a global leader in quantum-safe telecommunications

The centralised Network Operations Centre (NOC) provides real-time monitoring, automated key lifecycle management, and zero-touch provisioning, making this the world's most advanced carrier-grade quantum security deployment.

Read full case study: https://www.qnulabs.com/case-studies/quantum-safe-telecom-network-qkd-pqc-india

India's 500+ Kilometre Quantum Network Achievement:

Under India's National Quantum Mission (NQM), QNu Labs achieved a landmark demonstration of quantum-secure communications by successfully deploying a Quantum Key Distribution (QKD) network spanning over 500 Kilometres using existing optical fibre infrastructure.

This accomplishment, announced at the Emerging Science, Technology and Innovation Conclave (ESTIC 2025) in the presence of India's Union Minister for Science and Technology, positions India as a key player in the second quantum revolution.

The deployment was made possible through collaboration with the Indian Army's Southern Command Signals, which provided strategic access to their fibre network in the Rajasthan Sector.

The network included multiple trusted nodes enabling end-to-end quantum key exchange across the 500+ Kilometre distance, demonstrating the viability of quantum-safe communications for defence, government, and critical national security infrastructure.

QNu Labs' QSIP (Quantum Random Number Generator System in Package) was presented to the Prime Minister during his inaugural address, providing India with quantum-certified randomness for cryptographic algorithms. This achievement exemplifies the Synergy of Technology, Research, Industry, and Defence Ecosystem (STRIDE), strengthening India's position as a leader in emerging quantum technologies and secure digital infrastructure for the 21st century.

Read full government press release: https://pib.gov.in/PressReleasePage.aspx?PRID=2186652

CONCLUSION: STRATEGIC IMPERATIVES FOR TELECOMMUNICATIONS EXECUTIVES

THE FIVE CRITICAL ACTIONS:

01 ACT IMMEDIATELY

Window closing rapidly: quantum computers expected 2026-2031; submarine cables deployed in 2025 vulnerable until 2050

02 COMPLY GLOBALLY

Meet EU NIS2 2030, US CISA/ FCC 2027, China 2026 mandates proactively; harmonize standards internationally

03 PROTECT CRITICAL INFRASTRUCTURE

Prioritize 5G/6G core networks, submarine cables, satellite systems, national security communications

04 TRANSFORM SUPPLY CHAINS

Mandate PQC compliance across entire equipment vendor ecosystem; create quantum-safe certification standards

05 COLLABORATE INDUSTRY-WIDE

Coordinate via GSMA, ITU-T, ETSI, 3GPP; establish government-industry partnerships; share threat intelligence

THE QUANTUM THREAT IS NOT 'IF' BUT 'WHEN.'

TELECOMMUNICATIONS EXECUTIVES: ACT NOW.

Check QNu's Other Threat Intelligence Reports on other industries such as -

Defence, Healthcare, Automobile, BFSI

1. Mobile Subscribers: 8.4 Billion

Source: GSMA Intelligence - The Mobile Economy 2024

Data Point: Global mobile subscriptions reached 8.4 billion in 2024, representing 104% penetration rate globally

URL: https://www.gsma.com/mobileeconomy/

Alternative Source: GSMA Intelligence Database

2. Fixed Broadband Connections: 1.5 Billion

Source: International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database 2024

Data Point: Global fixed broadband subscriptions: 1.47 billion (2024)

URL: https://www.itu.int/en/ITU-D/Statistics/

Direct Report: ITU Facts and Figures 2024

3. Annual Telecom Industry Revenue: $1.8 Trillion

Source: Statista Global Telecoms Market Revenue Report 2024

Data Point: Global telecommunications services market revenue: $1.79 trillion (2024 estimate)

URL: https://www.statista.com/statistics/222901/global-telecom-market-size/

Alternative Source: PwC Global Entertainment & Media Outlook 2024-2028

SECTION 2: INFRASTRUCTURE VULNERABILITY STATISTICS

4. 5G Networks: 200+ Countries

Source: GSMA Intelligence 5G Tracker (Real-time Database)

Data Point: As of Q4 2024, 5G networks operational in 200+ countries/territories with 1,500+ mobile operators

URL: https://www.gsma.com/futurenetworks/5g/

Interactive Map: GSMA 5G Tracker

5. Submarine Cables: 485+

Source: TeleGeography Submarine Cable Map 2024

Data Point: 485 active submarine cable systems as of 2024, spanning 1.4 million kilometers

URL: https://www.submarinecablemap.com/

Database: TeleGeography Global Bandwidth Research

6. Intercontinental Traffic via Submarine Cables: 99%

Source: Submarine Telecoms Forum Annual Report 2024

Data Point: 99% of intercontinental internet and data traffic travels via submarine fiber-optic cables

URL: https://subtelforum.com/

Alternative Source: International Cable Protection Committee (ICPC) Reports

7. Satellites at Risk: 4,000+

Source: Union of Concerned Scientists (UCS) Satellite Database 2024

Data Point: 4,000+ operational satellites (LEO/MEO/GEO) for telecommunications, including Starlink, OneWeb, Iridium, Inmarsat constellations

URL: https://www.ucsusa.org/resources/satellite-database

Alternative Source: Space Foundation Satellite Industry Report

SECTION 3: FINANCIAL IMPACT STATISTICS

8. Global Quantum Transition Cost: $250-400 Billion

Source: McKinsey & Company - Quantum Technology Monitor 2024

Data Point: Estimated global telecommunications industry investment required for post-quantum cryptography migration: $250-400B over 5-10 years

URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights

Related Report: McKinsey 'Quantum computing: An emerging ecosystem and industry use cases' (2023)

9. Total Breach Exposure: $500 Billion - $1 Trillion

Source: IBM Cost of Data Breach Report 2024 + Industry Scaling

Calculation Methodology:

• IBM 2024 Average Data Breach Cost: $4.88 million per incident

• Telecom Industry Average: $7.2 million per breach (specialized sector)

• Scaled to 1,500+ global operators × quantum-enabled breach scenarios = $500B-$1T range

URL: https://www.ibm.com/security/data-breach

Direct PDF: IBM Cost of Data Breach Report 2024

SECTION 4: QUANTUM COMPUTING TIMELINE

10. Quantum Computer Timeline: 2026-2031

Multiple Sources - Converging Timeline Estimates:

Source A: IBM Quantum Roadmap

Timeline: 10,000+ qubit systems by 2026-2027; error-corrected logical qubits for cryptographic attacks 2028-2030

URL: https://www.ibm.com/quantum/roadmap

Source B: Cornell University - RSA-2048 Breakthrough Research

Finding: RSA-2048 encryption breakable with only 372 physical qubits using optimized Shor's algorithm implementation

Published: December 2022 (arxiv preprint)

URL: https://arxiv.org/abs/2212.12372

Paper Title: 'Factoring integers with sublinear resources on a superconducting quantum processor'

Source C: McKinsey Quantum Technology Report 2024

Timeline: Cryptographically Relevant Quantum Computers (CRQC) likely 2029-2033; early vulnerabilities 2026-2028

URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights

Source D: Google Quantum AI - Willow Chip Announcement

Achievement: Error correction breakthrough demonstrating exponential error reduction as qubit count increases (December 2024)

URL: https://blog.google/technology/research/google-willow-quantum-chip/

Source E: NIST Post-Quantum Cryptography Timeline

Mandate: Quantum-vulnerable algorithms deprecated by 2030; completely disallowed by 2035 (assumes CRQC threat imminent)

URL: https://www.nist.gov/pqc

SECTION 5: REGULATORY & STANDARDS SOURCES

European Union

• NIS2 Directive: https://digital-strategy.ec.europa.eu

• DORA Regulation: https://www.digital-operational-resilience-act.com/

• 5G Security Toolbox: https://digital-strategy.ec.europa.eu/en/policies/5g-security

United States

• NSA CNSA 2.0: NSA Commercial National Security Algorithm Suite

• NIST PQC Standards: https://www.nist.gov/pqc

• CISA Quantum Directives: https://www.cisa.gov/

India

• National Quantum Mission: https://dst.gov.in/national-quantum-mission-nqm

• Telecom Cyber Security Rules 2024: DoT Gazette Notification

• TEC Quantum Standards: Technical Report Third Quantum Conclave

• DoT 2024 Achievements: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2088195

SECTION 6: QNU LABS CASE STUDY SOURCES

Case Study 1: India's First Commercial Quantum-Safe Network

Source: QNu Labs Official Case Study

URL: https://www.qnulabs.com/case-studies/quantum-safe-telecom-network-qkd-pqc-india

Key Details: Multi-city deployment with India's leading telecom operator; hybrid QKD-PQC architecture; 6+ months operational with zero downtime; NIST-compliant ML-KEM algorithms; Quantum Security as a Service (QSaaS) model

Case Study 2: India's 500+ Kilometer Quantum Network Achievement

Source: Press Information Bureau, Government of India

URL: https://pib.gov.in/PressReleasePage.aspx?PRID=2186652

Key Details: QNu Labs supported under National Quantum Mission; 500km+ QKD network demonstration; Indian Army Southern Command collaboration; ESTIC 2025 announcement; QSIP (Quantum Random Number Generator System in Package) presented to Prime Minister

SECTION 7: THREAT INTELLIGENCE & INDUSTRY DATA SOURCES

Threat Intelligence

• US Defense Intelligence Agency Threat Assessment 2025: DIA Statement for Record

• GSMA Mobile Security Reports: https://www.gsma.com/security/

• IBM X-Force Threat Intelligence Index 2024: https://www.ibm.com/security/data-breach

Standards Bodies

• ITU-T Quantum Standards: https://www.itu.int/en/ITU-T/

• ETSI Quantum-Safe Cryptography: https://www.etsi.org/technologies/quantum-safe-cryptography

• 3GPP Security Specifications: https://www.3gpp.org/specifications/specifications

VERIFICATION NOTES

Data Integrity:

All statistics and claims in the Telecommunications Quantum Threat Intelligence Report 2025 are sourced from publicly verifiable, authoritative sources including:

✓ International standards organizations (ITU, ETSI, 3GPP, NIST)

✓ Industry associations (GSMA, Submarine Telecoms Forum)

✓ Government agencies (DoT India, CISA USA, EU Commission, DST India)

✓ Research institutions (Cornell University, IBM Research, McKinsey)

✓ Verified case studies (QNu Labs deployments, PIB official releases)

Update Frequency:

This sources reference sheet reflects data current as of February 2026.

Q→NU
Proactively™ Quantum

Blogs → | Whitepaper → | Case Study →

Securing the Nation and the World | Architecting Tomorrow

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025. Karnataka | India

CIN: U72900KA2016PTC096629

Check QNu's Other Threat Intelligence Reports on other industries such as - Defence, Healthcare, Automobile, BFSI

Download your Quantum Readiness Starter Kit to start your migration towards quantum safe journey

Assess Your Quantum Readiness Score here

India **USA** **Australia** **Global**