DIGITAL REALTY™

Quantum Ready or Quantum-Risky?

The Post-Quantum Era for Network Operators

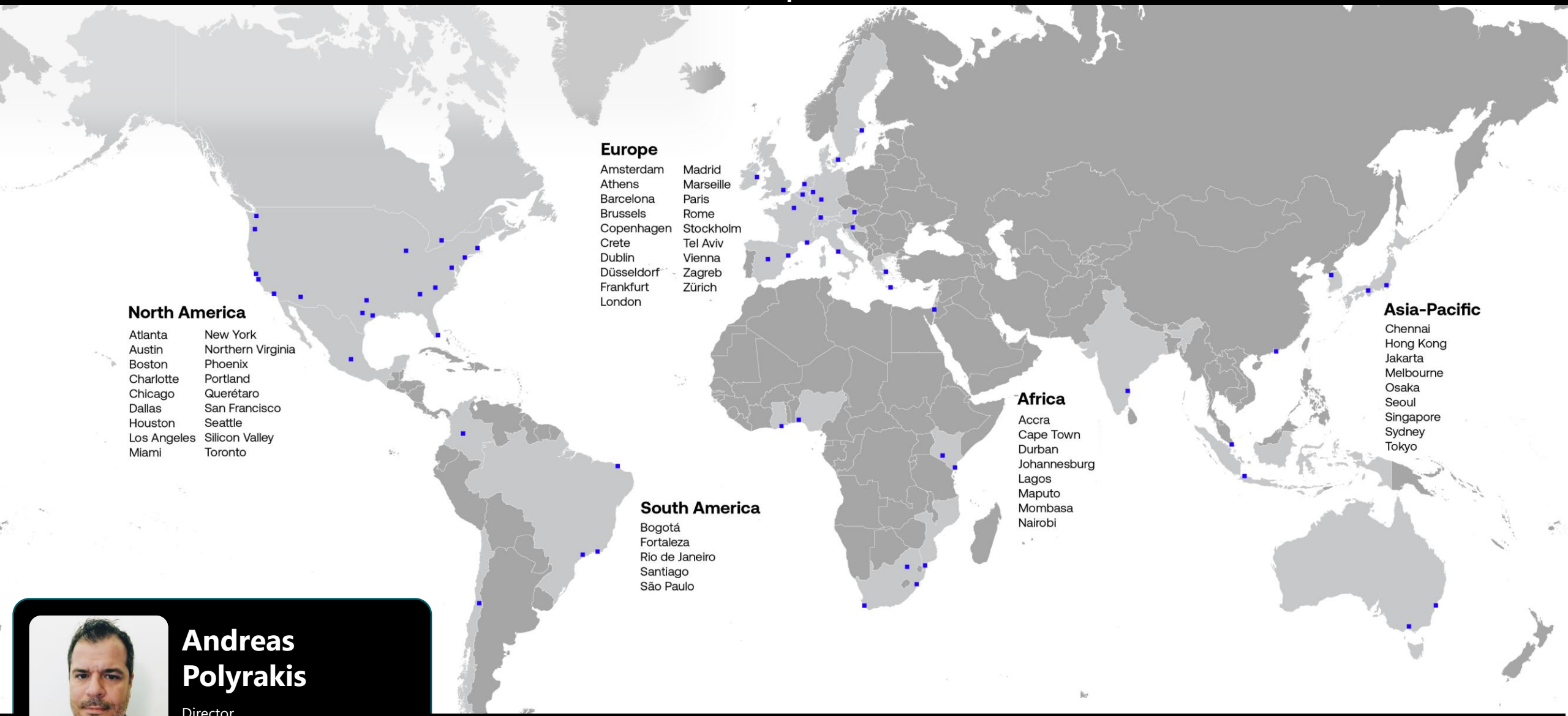
Andreas Polyrakis
Director, Strategy & Business Development,
Network Service Providers
apolyrakis@digitalrealty.com

GRNOG19 -- Dec 12th, 2025 -- Athens, Greece

DIGITAL REALTY™

A global platform with local expertise

300+ Data Centres | **25+** Countries | **50+** Metros | **6** Continents



Andreas Polyrakis

Director,
Strategy & Business Development,
Network Service Providers

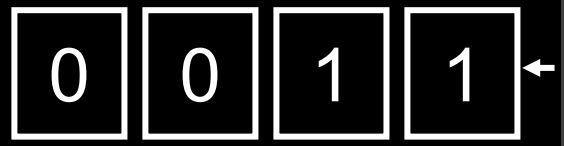
Agenda

- Quantum computers – status and maturity
- Internet cryptography basic - Symmetric vs Asymmetric - Entropy
- How future quantum computers ~~will~~ break cryptography **TODAY**
- Quantum-safe solutions: Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD); hybrid approaches
- Readiness levels and timelines
- Digital Realty in the post-quantum era

Quantum computing today

Classical vs Quantum Computers

Classical (4 bits)



Bit-based Data Representation
Classical computing uses bits that hold values of either 0 or 1 to represent data and perform calculations deterministically. Each bit has a single, specific value.

3

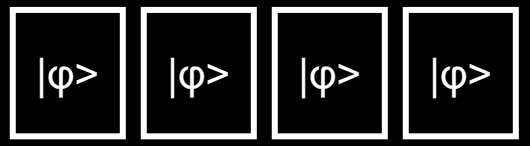
f(x)

Boolean Logic and Gates
Boolean logic and deterministic gates form the foundation of classical algorithms and circuit design. The result of a computation is deterministic:
Same input → same output

f(3)

Sequential Processing
Classical processors evaluate one input at a time sequentially, limiting scalability for large, complex problems requiring many simultaneous computations.

Quantum (4 qubits)



Qubits and Superposition
Qubits can exist in multiple states simultaneously, enabling quantum parallelism with superposition of values.

$$|\varphi, t_0\rangle = \sum_x \alpha_x |x\rangle$$

Superposition of all possible values 0000 to 1111

U_f

Quantum Algorithm Transformations
Unitary transformations operate on superpositions, allowing simultaneous function evaluation across many states.

$$|\varphi, t_1\rangle = \sum_x \alpha_x |x, f(x)\rangle$$

For every possible input x in the superposition, the function $f(x)$ is computed in parallel and stored alongside x

Quantum measurement

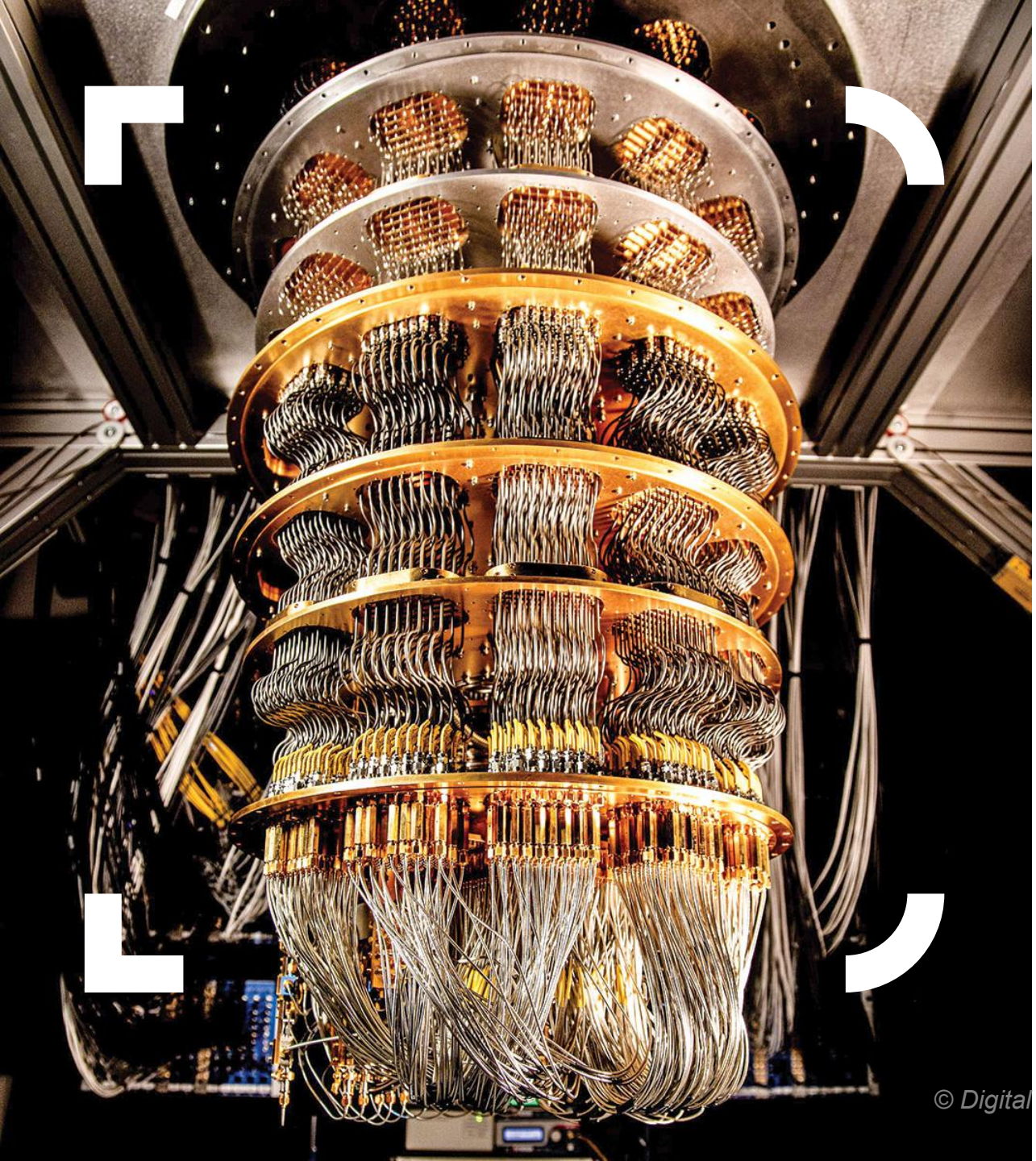
Measurement and Collapse
Measurement collapses superposition to one state based on probability amplitudes, producing a single outcome value.

$|8, f(8)\rangle$

…with probability $|a_8|^2$

Measurement is probabilistic; any of the possible results may appear, each with a certain probability.

Quantum advantage:
Parallel evaluation of $f(x)$ across all states → algorithms exploit this for speedups.



Status and future

Today:

- Many restrictions (implementation-dependent), e.g.:
  - Very low operating temperatures, often near 0°K
  - Very sensitive to environment (thermal fluctuations, electromagnetic fields, vibrations, crosstalk …)
  - Low fidelity and limited coherence
  - Other technology limitations
- High error rates – 100s or 1000s of physical qubits for a single logical qubit
- Very small number of logical qubits, O(10)

Near future (2027-2030)

- Plans by different vendors for $O(10^2)$ or $O(10^3)$ logical qubits
  - Eg., IonQ just announced 40-80K logical qubits by 2030
    https://ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality

How do these affect cryptography?

Internet Cryptography today

Two types of key-based cryptography for communications:

- **Symmetric Encryption**
  - Encrypt and Decrypt using the same key.
  - Key needs to be pre-shared. Eg
    - Through an already secure comm channel
    - Through physical travelling and handing over
  - Set-up is required prior to secure communication, which makes it impractical for adhoc communications

Eg: AES algorithm

Used by IPSEC, MACSEC, OTNSEC

- **Asymmetric Encryption**
  - Encrypt and Decrypt using different keys: Encrypt through the (publicly shared) public key of the recipient; decrypt through the private key of the recipient.
  - Encryption depends on the fact that, assuming the key is large enough (eg 2048bit), it is practically impossible to calculate private key
  - Relatively easy to set up and exchange keys ad-hoc, with no advance set-up or pre-shared material required between the communicating parties. Very practical for internet use (eg https).

Eg: RSA or Diffie-Hellman (ECDH) algorithms
Used by TSL/SSL, SSH, PGP, IPSEC (handshake/session keys)

- **Asymmetric handshake, symmetric data channel**
  - Asymmetric encryption is only used during the handshake, to create a secure channel and exchange secure keys, that they will then be used to symmetrically encrypt the actual data!

Side note: How bad Entropy affects Encryption

What is Entropy?
In information theory and cryptography, **entropy is a measure of unpredictability** in a source of randomness. It is usually measured in **bits: 1 bit of entropy** = 2 equally likely outcomes (eg fair coin toss). **n bits of entropy** = 2^n equally likely possibilities.

The problem with Random Number Generators (RNGs) in deterministic computers:
• Standard computers are deterministic — "true" randomness is not natural for them.
• Hence, most RNGs are **algorithms,** seeded with some initial value, that produce sequences that *look* random but is entirely determined by the seed (**Pseudo-RNGs)**
• If the **seed is weak** (predictable or low entropy), an attacker can guess or brute-force it.
•For example, if a PRNG seed is just the current system clock, an attacker only needs to try a few thousand values to reconstruct the sequence.

True Random Number Generators (TRNGs) use physical processes (thermal noise, radioactive decay, quantum effects) to get unpredictability.

- All key-based encryption algorithms depend on good quality (=randomness) of keys.
- In most cases, keys constructed by deterministic computers are not completely random!
- This may significantly reduce the entropy of keys and has caused real-world cryptographic failures, eg Debian OpenSSL bug (2008) reduced key entropy to 15bits – keys could be brute forced in seconds!!!

How Quantum Computing breaks current internet encryption

- Large-scale quantum computers could **break** today's widely used **asymmetric encryption algorithms** like RSA and ECC (Shor's Algorithm, 1994).
  - Today, such quantum computers do not exist, but we will need ~2300 logical qubits to break 256-bit ECC (most common today) and ~4000 qubits to break RSA/DSA-2048.
  - **Once scalable quantum computers become available, the existing asymmetric algorithms will be at stake**

- **Symmetric encryption algorithms** are partially impacted
  - Grover's Algorithm (1996) reduces brute-force complexity $2^n \rightarrow 2^{n/2}$
    - AES-128 (typical for TLS, WPA2/3, IPSEC, OpenVPN etc) is significantly weakened but not trivial to break
    - Today's "high-security" AES-256, still require "astronomically large" operations – safe for post-quantum era.
  - **Symmetric encryption with longer keys is considered Quantum-Safe**

- **Entropy** - brute-force on poorly constructed keys is much easier with quantum computers.

NISTIR 8105

Report on Post-Quantum Cryptography

April 2016

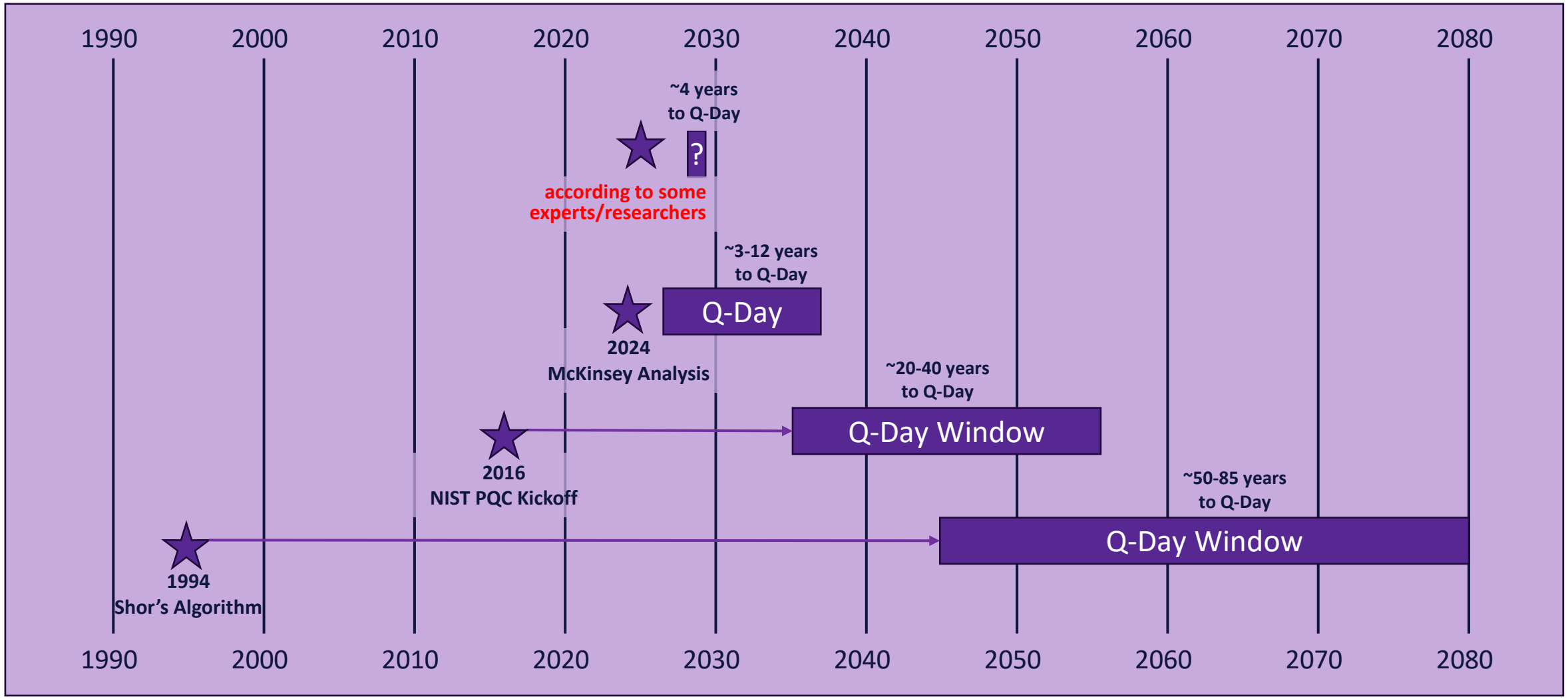
Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Ok. So, how much time do we have?

Q-Day Timeline

(credits :Quantropi)



Bad News: We need to act!

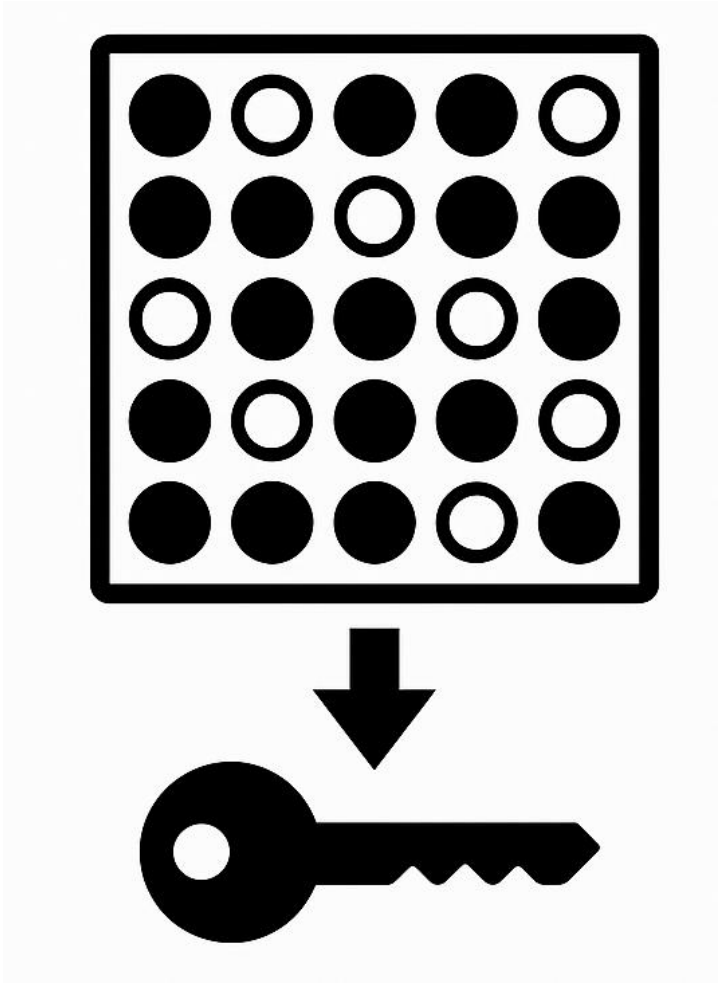
Good News: We still have some time to prepare! -Do we?

More Bad News: Today's data is vulnerable to harvesting (a.k.a store-now-decrypt-later) attacks

Solutions

Start with Entropy

- Update your cryptographic libraries
- Consider hardware entropy sources
- Monitor RNG quality
- **Ensure that your RNG's are suitable for the level of security that you require!**



Upgrade Asymmetric Encryption to use PQC

Asymmetric encryption

- Asymmetric encryption is widely used, esp to encrypt ah-hoc connections, eg HTTPS
- All digital certificates, TLS handshakes, SSH logins, PGP, cryptocurrencies → must move to PQC.
- This is an urgent migration target.

Problem

- **Asymmetric (public-key)** crypto = **broken by Shor's algorithm** (RSA, ECC, DH, DSA).

Solution

- **Post-quantum cryptography (PQC)** = cryptographic algorithms designed to be secure against **both classical and quantum computers.**
- They run on classical hardware (CPUs, GPUs, FPGAs) or special chips/cards.

Cryptographic Protocols need to be modified to replace old, broken algorithms with PQC algorithms

Status of PQC (2025)

NIST PQC Standardization (U.S.)

2016: Launched PQC competition (69 submissions).
2022: Announced winners (Round 3).
2024: Draft standards published. For Encryption / Key Encapsulation: **CRYSTALS-Kyber** (lattice-based, efficient, main KEM). HQC (Hamming Quasi-Cyclic) in progress

EU / ETSI and **ISO** → aligning with NIST, pilots underway.

Industry: TLS 1.3 "hybrid" key exchanges (X25519 + Kyber) already being tested by Google, Cloudflare, AWS, Microsoft,…

Symmetric Encryption: Secure your Key Distribution with QKD (…)

Symmetric encryption

- Symmetric crypto algorithms are **not broken** by Quantum computers – **but brute force** is significantly easier, hence smaller key sizes could be unsafe
- Solution: upgrade to a larger keys, eg AES-512

The problem lies on the key exchange

- Symmetric cryptography requires the keys to be **securely** exchanged – this can be a **real challenge**!

Solution: Quantum key distribution (QKD)

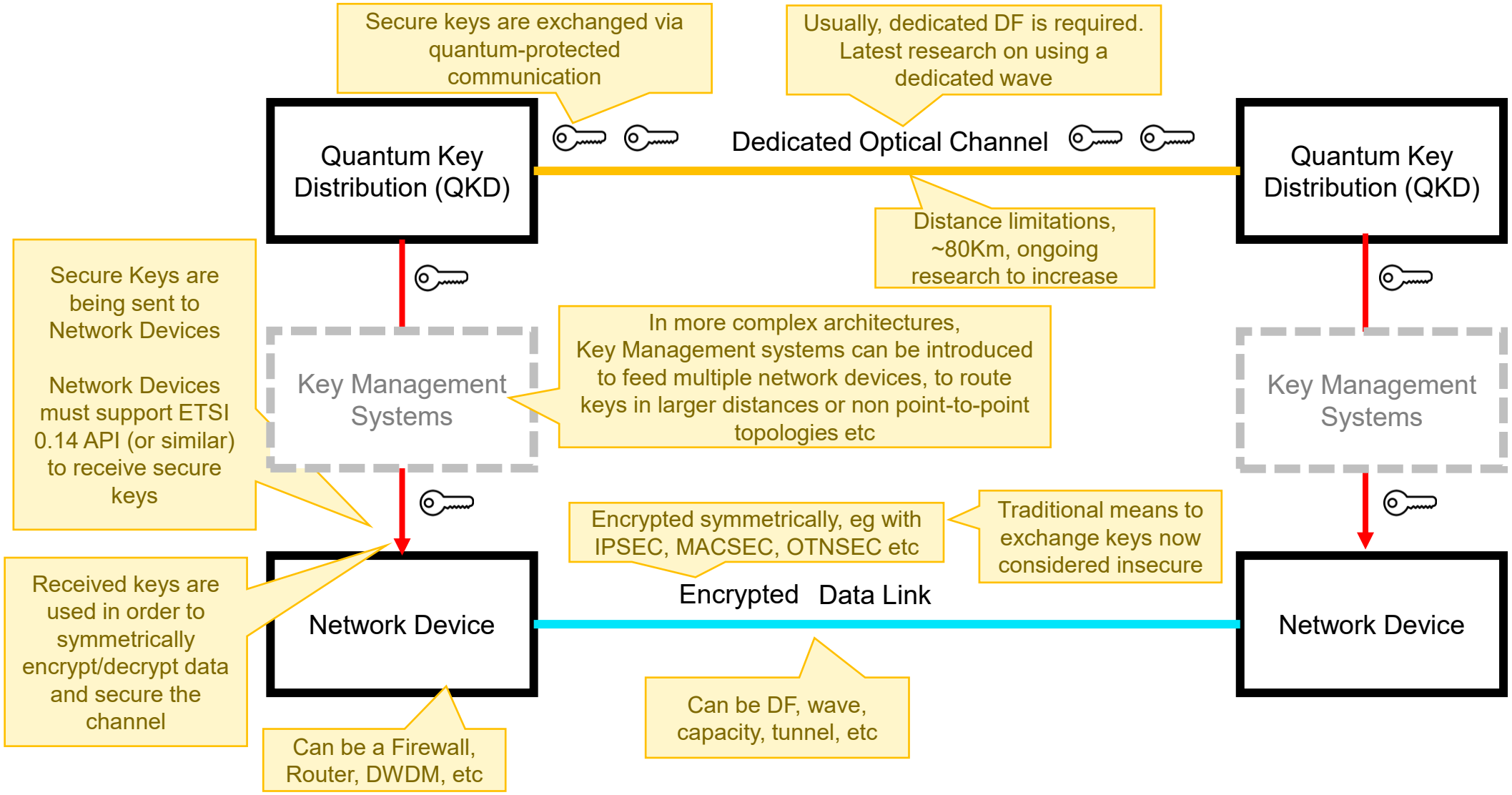
- **QKD** - a method to securely distribute symmetric encryption keys using the principles of quantum mechanics.
- **Data channel:** Then traditional Symmetric Encryption is used, eg IPSEC, MACSEC, OTNSEC etc
- **Limitations:** Expensive QKD hardware, distance limitations (~100Km), usually a dedicated DF is required just for the key exchange
- **Advantages:** Secure by the laws of physics, not human algorithms and hard-to-solve math!

Non-Quantum key distribution solutions also exist!

QKD principle:

- Photons are used to share secret keys.
- If a photon is intercepted and measured, its quantum state collapses, and this disturbance is immediately detectable.
- When such interference is detected, the key exchange is aborted.
- If no disturbance is found, the keys have been exchanged securely.

Quantum Key Distribution – High Level Diagram



Summarizing the solutions

QKD

- QKD is very secure, but very complicated and expensive, with significant distance limitations.
- Requires new hardware and dedicated comm links and it cannot secure ad-hoc communications.
- Expected to be used primarily to secure lower network layers (0-3) of channels that carry very sensitive data, eg defence, governmental, finance backbone links

QKD alternatives

- To overcome the limitations of QKD, other means of secure exchange of keys have been proposed, including digital QKD, key proxys and other solutions.

PQC

- PQC can be implemented on hardware or software, much easier to deploy. Upgrade of existing systems might be possible.
- However, we are not certain that the new PQC algorithms are not breakable with classical or quantum computers.
- Expected to be used widely on adhoc communications and layer-7 encryption

Depending on security requirements, technical feasibility and cost, a combination of the aforementioned solutions is expected.

Eg a bank may decide to secure some key links, eg datacenters and headquarters, with QKD (IPSEC/MACSEC), and use PQC to harden communications with remote branches or application-level security (TLS/SSL)

Current State & Deployments

Current state and deployments

Region / Country	Mandates & Policies	Timeline / Deadlines
United States	NSM-10 (2022), OMB Memo M-23-02, Quantum Cybersecurity Preparedness Act. NIST PQC standards (FIPS 203/204/205 in 2024). CNSA 2.0 requires PQC for national security systems.	Inventories ongoing now. New NSS acquisitions quantum-resistant by **2027**. 112-bit algorithms deprecated after **2030**, fully removed by **2035**.
Canada	Cyber Centre “Roadmap for Migration to PQC” (2025). Departments must inventory and migrate.	Plans by **2026**, high-priority systems PQC by **2031**, full migration by **2035**.
UK	NCSC PQC migration roadmap.	Planning phase by **2028**, critical migrations by **2031**, full migration by **2035**.
European Union	EC Recommendation (2024) for coordinated roadmap. PQC in Cyber Resilience Act product rules.	Critical infrastructure secured by **2030**, medium/low risk by **2035**.
Japan	National strategy (NICT, MIC) and PQC pilots in Tokyo QKD network. Participation in NIST/ISO standardization.	Migration planning underway; no fixed national deadlines yet, but PQC required in critical national infrastructure by **early 2030s**.
South Korea	National strategy combining PQC + QKD. Government networks (48 ministries) already on QKD backbone; PQC migration roadmap in parallel.	PQC transition starting now; target completion aligned with 2030–2035 international window.
International / Standards	**NIST (US):** FIPS 203–205 finalized. **ISO/IEC JTC 1 SC27:** PQC work in progress. **ETSI ISG QSC:** ongoing PQC + QKD profiles.	Global adoption of NIST algorithms expected 2024–2026; ISO standards later this decade.
NATO	Recognized PQC as essential to future cyber defense (2022). Guidance to member states: inventory and prepare migration. Coordinated approach aligned with NIST PQC standards.	PQC adoption for NATO communications and defense systems by **early 2030s**, aligned with member states’ 2030–2035 timelines.

National QKD Projects

- **EU: EuroQCI**
  Pan-EU terrestrrial + space quantum-secure comms initiative
- **UK: London metro**
  QKD service trial (BT + Toshiba, EY as firsc first customer)
- **Germany: 254 km**
  QKD over commmeriarcial fibre (Toshiba Europe)
- **Japan: Tokyo QKD**
  Network (NICT)
- **China**
  Baijing–Shanghai QKD backbone & national integration
- **Singapore**
  NQSN / NQSN+(national quantum-safe network)
- **Spain**
  REDIMadrid quantum-secure transport (with Ciena)
- **France**
  ParisQCI / Orange Quantum Defender
- **Switzerland**
  SwissQuantum / Geneva elections
- **Italy**
  QUID– Quantum Italy Deployment (EuroQCI-IT)
- **DOE/ESnet quantum**
  DOE/ESnet quantum netwk testbeds
- **India**
  C-DOT national QKD efforts
- **UAE QuantumConnect (TII)**

Carrier pilots and deployments (indicative*)

Carrier	Country/Region	What they did	Status
BT (with Toshiba)	UK	London-metro **QKD service**; first customer **EY** connecting two London sites	Commercial pilot / early service. (global.toshiba)
Verizon	USA	**QKD trial** sending encrypted video between D.C./Virginia sites over production fiber	Trial completed. (techblog.comsoc.org)
Orange Business	France	**Orange Quantum Defender**: QKD + PQC hybrid service over Orange's Paris fiber	Commercial service launched. (Newsroom Groupe Orange)
Deutsche Telekom (T-Labs)	Germany	Long-duration **entangled-photon transmission** over deployed fiber; quantum networking record	Lab/field milestone toward carrier QKD. (telekom.com)
Telefónica	Spain	**QKD field trials** on commercial optical network (Madrid); healthcare data protection demo	Trials / pilots. (Telefónica)
Colt Technology Services	UK/EU	**QKD/quantum-safe trials** across Colt optical network; also **LEO satellite QKD** trial with Nokia & Honeywell	Trials completed / ongoing. (Colt Technology Services)
KT (Korea Telecom)	South Korea	Partnership to **deploy QKD** for carrier infrastructure (with HEQA Security)	Deployment program announced. (Quantum Computing Report)
SK Broadband	South Korea	Nation-wide **quantum-safe/QKD network** connecting **48 government departments** (~800 km)	In operation (phase 1 complete). (ID Quantique)
China Telecom	China	**Hybrid QKD+PQC** system; 1,000 km quantum-encrypted call; rollout across 16 cities; part of Beijing–Shanghai backbone ecosystem	Rollout / national backbone participation. (The Quantum Insider)
Singtel / SPTel (with SpeQtral, Toshiba)	Singapore	**QKD trials** and enterprise education under NQSN/NQSN+ national program	Trials / early services. (sptel.com)
NTT Group	Japan	**Quantum-safe transport** platform with crypto-agility; Japan carrier R&D on QKD-ready networks (with NICT/NEC/Toshiba)	R&D / field demos. (NTT)
KDDI / KDDI Research	Japan	**QKD multiplexing** with **33.4 Tbps** co-propagating data over 80 km; broader national quantum initiatives	Lab/field demo results. (kddi-research.jp)
Vodafone	Europe / Global	Announced quantum-safe networking strategy; trials of PQC integration into VPN and mobile core; exploring QKD partnerships under EU quantum initiatives	Early trials / roadmap announced (Vodafone Group News)

* Compiled with AI – some inaccuracies may exist

Big Tech Post Quantum Migration News

Connectivity-related:

- **Clouds & CDNs (AWS, Azure, Google Cloud, Cloudflare)** → enabling PQC for customer APIs, VPNs, and storage.
- **Enterprise security (Palo Alto, Zoom, Cisco upcoming)** → hybrid PQC for VPNs, conferencing, identity.

Other (application level):

- **Browsers (Chrome, Edge, Safari)** → adopting PQC first, since TLS handshakes are the front line.
- **Messaging (Apple iMessage, WhatsApp planned)** → embedding PQC into end-to-end encrypted messaging.

Big Tech PQC Initiatives

- **Microsoft**
  - Added PQC support in **Edge browser** (Kyber key exchange in TLS).
  - Testing PQC in **Windows** and **Azure services**.
  - Involved in NIST PQC standardization process.
- **Google**
  - Ran large-scale Chrome PQC trials (Kyber + X25519 hybrid).
  - Announced Chrome will transition to PQC in production for HTTPS/TLS.
  - Google Cloud also piloting PQC in APIs and KMS.
- **Apple**
  - iMessage updated to include a PQC key exchange protocol (“PQ3”), using Kyber plus classical ECC.
  - First mass-market messaging platform to roll out PQC at scale.
- **Meta (Facebook, WhatsApp, Instagram)**
  - Began PQC migration in backend infrastructure.
  - Exploring PQC for WhatsApp end-to-end encryption in future releases.
- **Cloudflare**
  - Enabled PQC in TLS connections for millions of websites it fronts.
  - Ran one of the first Internet-wide PQC experiments.
  - PQC support in Cloudflare Tunnel, CDN, and Zero Trust products.
- **Palo Alto Networks**
  - Added hybrid PQC key exchange for VPN/firewall solutions.
  - Targeted at enterprise customers with high-security needs.
- **Amazon (AWS)**
  - AWS Key Management Service (KMS) added PQC support.
  - PQC also tested in AWS TLS endpoints and customer SDKs.
- **Zoom**
  - Rolled out end-to-end PQC encryption in video calls.
  - Among first conferencing platforms to do so.

The role of Digital Realty in the post-quantum era

Digital Realty in the post-quantum era

- Neutral, open datacenters are crucial to the development of the internet
- While technology keeps evolving and modes of connectivity and transport keep changing, Data Centers will remain the home of the future ecosystems
- Digital Realty is the meeting place for Enterprises and Service Providers
- Maintaining a vibrant, relevant ecosystem is of key importance for us

Our Quantum agenda

- Host Quantum Computers and Quantum ecosystem
- Host third parties' Quantum-Safe solutions
- Harden our own communication products (eg metro-connect) and internal communications
- Attract provides of quantum-safe related services (eg secure transport, secure-keys-as-a-service, entropy-as-a-service etc) to participate into our ServiceFabric platform and make their services available to our clientele worldwide

Just announced:
British Startup Installs New York City's First Quantum Computer

Key takeaways:

It is not too early to start working on Quantum-Safe!

- If you haven’t done it already, please start!
- If you are already working on it, please reach us

Questions?
Thank you!

Andreas Polyrakis
Director, Strategy & Business Development,
Network Service Providers
apolyrakis@digitalrealty.com

DIGITAL REALTY