QUANTUM
THINK TANK

Insight that protects. Foresight that leads

Global Post Quantum Cryptography Momentum

By Tooba Qasim
December 2025

www.cyberlondon.com | info@cyberlondon.com

How the world is actually moving (and why it’s picking different paths)

A couple of years ago, post-quantum cryptography (PQC) still sounded like a future research topic. Today it looks a lot more like a coordinated global migration programme. Governments, standards bodies, telecom groups and major vendors are aligning around a simple idea: we cannot wait for a cryptographically relevant quantum computer to appear before we start changing the cryptography that protects the internet.

What has changed since then is that the momentum is now visible in real standards, real roadmaps and real deadlines and different regions are making different bets on how to get to quantum-safe.

The big picture: Standards first, then deployment

When cryptography changes at global scale, it usually happens in layers:

1. **Standards bodies** define what “good” looks like (algorithms, parameters, safety rules).
2. **Protocol bodies** update the plumbing of the internet (TLS, VPNs, certificates, identities).
3. **Governments and regulators** set deadlines and expectations.
4. **Vendors and operators** finally roll it out across products and networks.

PQC is now progressing through all four layers at once which is why it feels like momentum rather than theory.

NIST: The global anchor for PQC algorithms

If you zoom in on one organisation driving worldwide alignment, it is the U.S. National Institute of Standards and Technology (NIST).

NIST launched its PQC standardisation project in 2016, ran multiple evaluation rounds and in August 2024 it published the first three finalised post-quantum cryptography standards: (NIST)

- **FIPS 203: ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism) for encryption/key establishment (formerly CRYSTALS-Kyber).
- **FIPS 204: ML-DSA** (Module-Lattice-Based Digital Signature Algorithm) for signatures (formerly CRYSTALS-Dilithium).
- **FIPS 205: SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm) a hash-based signature standard (based on SPHINCS+) intended as a conservative backup option.

Then, in March 2025, NIST announced **HQC** as an additional (backup) post-quantum encryption algorithm, important because it brings algorithm diversity using a different mathematical family than ML-KEM.

Why does this matter outside the U.S.? Because NIST standards tend to become the *default reference point* for global vendors, cloud platforms, libraries, security products and telecom stacks. Even countries that don't "copy and paste" NIST choices often align with them to stay interoperable.

IETF: Making PQC real inside internet protocols

NIST standardises the algorithms. But the internet runs on protocols. That is where the **Internet Engineering Task Force (IETF)** comes in.

If you care about practical deployment, the IETF is one of the most important places to watch because it is where PQC gets integrated into things organisations actually use: **TLS (for HTTPS), IPsec/VPNs, and key exchange frameworks.**

A few concrete examples already exist:

- **RFC 8784**: an IKEv2 extension that mixes preshared keys into VPN key derivation to improve resistance against "store now, decrypt later" style threats. (IETF Datatracker)
- **RFC G370**: extends IKEv2 to allow *multiple key exchanges*, supporting hybrid approaches during the transition. (RFC Editor)
- **TLS hybrid work**: the IETF has active work on hybrid key exchange in TLS 1.3 (so web traffic can move toward PQC in a controlled way), plus supporting terminology and migration framing. (IETF)

This matters because many organisations don't "swap cryptography" directly. They inherit it through TLS libraries, VPN stacks, certificate chains and vendor platforms. Protocol standardisation is how PQC moves from “approved algorithm” to “something you can actually turn on safely.”

UK: NCSC is pushing timelines, prioritisation and realism

The UK has taken a practical and strongly guidance-led approach through the **National Cyber Security Centre (NCSC)**.

The NCSC’s migration timelines are very clear: complete key discovery and planning early, pilot and prioritise next, and aim for full migration by 2035, with major milestones along the way (including 2028 and 2031 targets). (NCSC)

The important cultural signal here is that the UK is treating PQC as a programme, not a patch.

UK stance on QKD

Quantum Key Distribution (QKD) is often mentioned in the same breath as PQC, so here is a simple way to think about it:

- **PQC** is new math that runs on normal computers and makes encryption/signatures resistant to future quantum attacks.
- **QKD** is a way of distributing keys using quantum physics signals (typically photons) where eavesdropping is detectable in principle.

QKD can be valuable in certain niche environments, but the NCSC has been clear that it should **not be treated as a universal replacement** for cryptography and it highlights a key practical issue: QKD still requires robust **authentication mechanisms** and organisations should not rely on QKD alone for key generation and distribution. (NCSC)

That “authentication problem” matters because even if you distribute a key using quantum signals, you still need to authenticate endpoints and manage trust otherwise you can be fooled about *who* you are exchanging keys with.

Europe: A coordinated PQC roadmap, plus major investment in QKD infrastructure

Europe is moving on two tracks at once: **PQC migration coordination** and **quantum communications infrastructure**.

On the PQC side, the European Commission and Member States have published a Coordinated Implementation Roadmap for transition to PQC, explicitly pushing for synchronised action.

In June 2025, the Commission's messaging was concrete: start transitioning by end of **2026** and move critical infrastructure as soon as possible (with a target no later than **2030** in that communication).

On the quantum communications side, Europe is heavily invested in EuroQCI (European Quantum Communication Infrastructure), which includes QKD as an additional layer of protection for certain use cases.

So, in simplified terms:

- Europe is coordinating PQC adoption as a baseline, while also building QKD-based infrastructure where it makes sense.
- The UK, by contrast, is generally more cautious about relying on QKD as a broad solution and strongly emphasises PQC for mainstream adoption.

China: Strong QKD deployment, plus its own crypto standardisation direction

China's progress is often most visible in quantum communications, particularly QKD networks and space-to-ground links.

China's Beijing–Shanghai quantum communication backbone was an early high-profile example (**over 2,000 km**) and more recent published work describes the China Quantum Communication Network spanning **over 10,000 km**, with extensive backbone nodes and metro networks.

On PQC standardisation, China is also pursuing its own direction and national priorities (and, like other major powers, it has strong incentives around sovereignty and control of cryptographic supply chains). Public reporting indicates a push toward China-led quantum-resistant standards alongside (or independent from) U.S.-led efforts. (The Quantum Insider)

In plain terms: China appears to be investing heavily in quantum communications (QKD) as a strategic capability, while also building out post-quantum cryptography pathways aligned to its own ecosystem.

Japan: Structured PQC guidance, plus active QKD RsD

Japan's approach is a mix of careful cryptographic governance and strong industry activity.

On PQC guidance, Japan's national cryptography evaluation body **CRYPTREC** publishes PQC guidance documents, including a **Post-Quantum Cryptography guideline (2024 edition)**. (cryptrec.go.jp)

On QKD, Japanese organisations (including NEC, Toshiba, and NICT) continue to publish and demonstrate progress in quantum networking and QKD technologies, including recent announcements on QKD network technologies and integration approaches. (NEC Global)

So Japan, like Europe and China, is active in quantum communications while also building structured PQC guidance through a national evaluation framework.

A quick "by-continent" snapshot with examples

To keep this global, here are examples across regions showing that PQC migration is not only a US/UK/EU conversation:

- **North America (Canada):** Canada's national cyber centre has published a roadmap for migrating government systems to PQC. (Canadian Centre for Cyber Security)
- **Europe:** EU-wide coordinated PQC roadmap and EuroQCI initiative. (Digital Strategy)
- **Asia:** Japan's CRYPTREC PQC guidance and active QKD RCD; China's large-scale QKD networks and broader crypto direction. (cryptrec.go.jp)
- **Oceania (Australia):** Australia's ASD/ACSC has published "Planning for post-quantum cryptography" guidance. (cyber.gov.au)
- **Africa (South Africa example):** Research collaboration and demonstrated quantum satellite communication links have been reported between South Africa and China, showing quantum comms activity expanding beyond the usual centres. (su.ac.za)
- **Southeast Asia (Singapore):** Singapore's Cyber Security Agency released a Quantum-Safe Handbook and Quantum Readiness Index. (Cyber Security Agency of Singapore)

So what should an organisation take from all this?

If you strip away the acronyms and geopolitics, the message is surprisingly consistent:

- **PQC is the mainstream path** because it works on normal systems and can be deployed widely.
- **Standards now exist** (and more are coming) so this is no longer hypothetical.
- **Protocols are being updated** so PQC can be adopted without breaking the internet. (IETF Datatracker)
- **QKD is real but specialized**, useful in some contexts but not a universal replacement and it comes with practical constraints (especially around authentication and deployment complexity).
- **Different countries will emphasise different tools**, but almost all are now treating "quantum-safe" as a long-term national resilience issue.

Useful Links

- NIST PQC project: https://csrc.nist.gov/projects/post-quantum-cryptography (NIST)
- FIPS 203 (ML-KEM): https://csrc.nist.gov/pubs/fips/203/final (NIST Computer Security Resource Center)
- NCSC PQC migration timelines (UK): https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (NCSC)
- NCSC quantum networking technologies (QKD discussion): https://www.ncsc.gov.uk/whitepaper/quantum-networking-technologies (NCSC)
- EU PQC roadmap: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (Digital Strategy)
- EuroQCI: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (Digital Strategy)
- IETF RFC 8784 (PQC resilience for IKEv2 via PPK): https://datatracker.ietf.org/doc/html/rfc8784 (IETF Datatracker)
- IETF RFC 9370 (multiple key exchanges in IKEv2): https://www.rfc-editor.org/rfc/rfc9370.html (RFC Editor)

About the author: Tooba Qasim is a PhD researcher in cybersecurity at City St George's, University of London. Her research includes authentication challenges in Quantum Key Distribution (QKD), analysis of post-quantum cryptography (PQC) algorithms in security protocols and exploring the security and performance of PQC on hardware and resource-constrained devices.