Why Quantum Security Needs a Global Effort

By Tooba Qasim

Building a Sustainable Ecosystem

Quantum security is often discussed as a technical challenge: new algorithms, new standards, new implementations. But when you step back and look at how the digital world actually works, one thing becomes clear very quickly:

No organisation, no country and no vendor can become quantum-safe on its own.

The internet is not owned by a single entity. Cryptography does not stop at national borders. Software supply chains cross continents. Cloud platforms serve millions of organisations at once. If quantum-safe security is going to last, it has to be built as a shared effort across industry, academia, governments and global standards communities.

This is why ecosystem collaboration is not a “nice to have” in the sustainability phase. It is the foundation that keeps quantum-safe systems viable over the long term.

Why Collaboration Matters More in the Quantum Era

Classical cryptography evolved slowly. Algorithms like RSA and elliptic curve cryptography matured over decades, with thousands of eyes reviewing implementations, breaking weak designs and refining best practices. That collective scrutiny is what made them reliable.

Post-quantum cryptography does not have that luxury of time.

PQC algorithms are new. Implementations are new. Deployment patterns are new. Even operational assumptions are new. The only way to gain confidence at scale is through **shared learning**.

When organisations collaborate by publishing research, sharing migration lessons, contributing to open-source libraries or participating in standards discussions, everyone benefits. Mistakes are discovered earlier. Weak assumptions are challenged. Interoperability improves.

Sustainability depends on this feedback loop continuing long after initial deployment.

The Role of Standards Bodies as Anchors

Global standards bodies play a unique stabilising role in the quantum transition.

Institutions such as the **National Institute of Standards and Technology (NIST)**, the **Internet Engineering Task Force (IETF)**, and **European Telecommunications Standards Institute (ETSI)** provide common reference points that vendors, governments, and organisations can align around.

These bodies do more than publish documents. They create shared language, define interoperability expectations and provide a structured way to evolve cryptography without fragmentation.

From a sustainability perspective, this matters because cryptographic change does not stop after the first migration. Algorithms will be refined, parameters will be updated and deployment guidance will evolve. Standards bodies ensure that those changes happen in a coordinated way rather than through incompatible, ad-hoc decisions.

Industry: Where Theory Meets Reality

Industry plays a different but equally critical role.

Cloud providers, operating system vendors, network equipment manufacturers and security vendors are the ones who turn standards into deployable systems. Their decisions shape what is practical, what performs well and what organisations can realistically adopt.

Sustainable quantum security depends on vendors:

- supporting hybrid cryptography properly,
- exposing cryptographic choices transparently,
- avoiding silent fallbacks to weak algorithms,
- and committing to long-term update paths.

When vendors collaborate openly through interoperability testing, shared libraries and public roadmaps they reduce risk not only for themselves but for every customer downstream.

Academia and Research: Stress-Testing the Future

Academic research remains one of the most important pillars of long-term quantum resilience.

Researchers are the ones probing assumptions, analysing attack surfaces, studying side-channel risks and questioning whether current designs will still hold under new conditions. They also explore what comes next: new cryptographic constructions, better implementations and stronger formal assurance techniques.

From a sustainability standpoint, the key value of academic involvement is **independence**. Research institutions are not tied to product cycles or procurement deadlines. They can ask uncomfortable questions early before weaknesses become operational incidents.

Maintaining strong links between academia and practitioners ensures that future innovation feeds directly into real-world security.

Government: Coordination, Guidance and Long-Term Vision

Governments play a unique role because they operate at scale and over long time horizons.

National cyber authorities provide migration timelines, sector-specific guidance and risk prioritisation that help organisations plan realistically. Governments also influence sustainability through procurement rules, compliance expectations and funding for research and skills development.

Perhaps most importantly, governments act as conveners. They bring industry, academia and regulators together around shared objectives, helping avoid fragmentation and duplicated effort.

In the quantum era, this coordination function is as important as technical leadership.

Why Neutral Forums Matter

This is where think tanks, industry clusters and neutral forums play a unique and often underappreciated role.

Unlike vendors, they are not driven by product roadmaps. Unlike regulators they are not bound by enforcement cycles. Unlike academic conferences they are not limited to narrow technical audiences.

Neutral forums translate complex technical developments into strategic language. They create spaces where security professionals, policymakers, researchers, architects and business leaders can engage with the same problem from different perspectives without commercial pressure or competitive positioning.

Most importantly, they help organisations **learn together** rather than in isolation.

The Role of the Quantum Think Tank

The Quantum Think Tank exists precisely to serve this purpose.

Its aim is not to promote a particular technology, algorithm or vendor solution but to support informed, cross-disciplinary conversation about quantum security. It brings together expertise from cybersecurity, cryptography, policy, risk management and emerging technology to help organisations make sense of a rapidly evolving landscape.

By publishing accessible analysis, convening discussions and fostering collaboration across sectors the Quantum Think Tank seeks to bridge the gap between awareness and action helping organisations move from understanding quantum risk to managing it sustainably. In a field where uncertainty is inevitable and standards continue to evolve, such neutral spaces are critical to building shared understanding and collective resilience.

Global Coordination Is Not Optional

Quantum threats are global by nature. A weakness discovered in one region affects systems everywhere. A fragmented response increases risk for everyone.

The encouraging news is that, despite geopolitical differences, there is already significant alignment on the need for quantum-safe cryptography. Countries may prioritise different tools or timelines but the underlying direction is shared. Long-term sustainability means reinforcing that alignment: sharing lessons, avoiding unnecessary divergence and keeping interoperability at the centre of decision-making.

A Sustainable Future Is a Shared One

Quantum-safe security is not a destination. It is an ongoing process that depends on collaboration long after the initial transition is complete. Organisations that view PQC purely as an internal technical project will struggle to keep pace. Those that engage with the wider

ecosystem, standards bodies, vendors, researchers, and peers will be far better positioned to adapt as cryptography continues to evolve.

Sustainability, in the end, is not about locking systems down forever. It is about building **networks of trust, knowledge and cooperation** that can evolve safely over time.