15/12/2025

IN FOCUS

The Year 2035 –Living in the Quantum Era: A Possible Future

Looking back from the year 2035, what might have occurred in the decade since the United Nations declared 2025 the International Year of Quantum? We believe that the ten years that followed this declaration will have reshaped global security, governance and trust as quantum technologies redefined the digital foundations of international cooperation. Alongside this transformation, early signals and uncertainties about quantum readiness and threat escalation time lines will have likely shaped how governments, industry leaders, and international bodies chose to act.

Mr Daniel Akinmade Emejulu
Head of Global Public Policy and Social Impact, Quside

Mr Carlos Abellán
Founder and Chief Executive Officer, Quside

Quantum technologies: the move from theory to strategy

What might analysts living in 2035 say about the state of quantum technologies in that year and their effect on the world order? Below is a possible scenario that these analysts might describe.

"In 2035, quantum technologies have become integral to national security strategies, economic competitiveness and technological governance. A decade earlier, the United Nations (UN) declaration of the International Year of Quantum in 2025 served as a pivotal moment. It coincided with a global shift from theoretical research to the practical deployment of quantum tools in government, industry, and society, even as early predictions about the attainment of quantum capability remained varied and uncertain.

"By 2025, quantum innovation had moved from university laboratories into strategic boardrooms. Companies were no longer debating if quantum-safe security was necessary, but rather how to implement it. In turn, governments recognised that quantum computing's potential to disrupt cryptography would have lasting implications for global security, stability and trust.

From niche science to a national security concern: a decade of rising awareness (2015-2025)

"Back in 2015, the idea that quantum computing could threaten global security seemed a distant concern. This was a discussion held mainly within university physics departments rather than by CEOs or in policy circles. But by the early 2020s, Intelli-gence agencies such as the US National Security Agency had begun warning that the cryptographic foundations of the current digital economy were not built to last. In essence, they were vulnerable to the new technologies that were evolving.

"Why was this a concern? To understand it, it helps to look at how mainstream 2025 encryption actually worked. Encryption of that time, the invisible guardian of secrecy, integrity and authentication across systems, relied on mathematical problems that ordinary computers in 2025 could not technically solve. By that year, encryption was ubiquitous and protected nearly everything: financial transactions, cloud services, messaging apps, national infrastructure, and emerging AI systems and agents. Once viewed as an abstract or theoretical risk, the concern that future quantum machines would be able to easily unlock 2025 encryption became both real and urgent, as cyber actors began harvesting encrypted data to store for future decryption once these quantum machines matured. This was a risk documented in several early policy reports that resulted from the condensing of earlier repetitions of the 'harvest-now-decrypt-later' concept.

"This strategy transformed cybersecurity thinking. It became a long-term survival issue and a strategic

imperative. The implications reached far beyond technology, touching the architecture of digital trust between citizens, companies and states.

Building quantum-safe architectures: the transition years (2020-2035)

"Responding to this threat required more than a simple software upgrade. The transition to quantum computing required new cryptographic standards, hardware upgrades and a fundamental rethink of how trust is engineered into systems. Quantum-safe architectures emerged, combining new mathematical algorithms with hardware foundations that ensured secure key generation and distribution.

"These advances, built on decades of research in quantum physics and cryptography, became the bedrock of modern (2035) digital security. They embodied a hybrid model combining novel mathematical algorithms with physical entropy sources derived from quantum processes. They also encouraged a growing emphasis on cryptographic agility, i.e. systems designed to replace algorithms without having to redesign entire system architectures.

Governing the quantum transition (2025-2035)

"This evolution was not merely technological: it was also policy driven, grounded in coordinated frameworks that encouraged migration towards post-quantum standards, even as governments acknowledged persistent uncertainties in the state of their respective countries' quantum readiness.

"The International Year of Quantum was declared when the emergence of the quantum world was already well under way. The declaration became a rallying point for collaboration, framing the stage on which science, policy and industry would converge. Governments worldwide published national road-maps for quantum-safe migration, providing time-bound guidance on which sectors would transition first, under what regulatory obligations and with which verification requirements.

"Chipmakers adapted architectures to support new algorithms, and quantum computing shifted from a purely scientific frontier to a source of competitive advantage.

"The UN and the Organisation for Economic Co-operation and Development facilitated policy coordination and standardisation efforts, fast-tracking cooperation across borders in policy forums focused increasingly on questions of verification, transparency, and equitable access to quantum capabilities.

"At UN General Assembly High Level Week in 2025, Amandeep Singh Gill, the UN Secretary-General's Envoy on Technology, convened the UN Digital Cooperation Day Quantum Breakfast, bringing together policymakers, technologists and industry leaders to explore the shared responsibility of building a secure quantum future.

"The interplay between public and private actors demonstrated that quantum resilience required a global effort. International partnerships emerged to support developing economies in adopting quantum-safe frameworks, preventing the rise of a new quantum divide and reinforcing the need for international bodies to coordinate verification standards across borders.

Looking back from 2035

"From the vantage point of 2035, the decade following 2025 stands as one of the most consequential in the history of digital trust. The global community learned that preparing for quantum risks was not a defensive act alone, but an opportunity to modernise and rebuild secure digital foundations for the next century.

"Looking back, therefore, the quantum era was not born from panic. It came from foresight that resulted in a collective decision to modernise security before it was too late. In this journey, national migration roadmaps, global verification standards, and intentional investment in cryptographic agility played a defining role, offering policymakers clear and actionable guidance based on the logic of the early quantum transition."

We believe that, by adopting in 2025 the perspective of 2035, it is possible to map out how important it is to build the groundwork for the resilient, verifiable, and truly global digital systems that the world depends on – and will increasingly rely on in the future.