DR SHARLENE THIAGARAJAH
TM Research & Development CEO

Quantum tech for secure communications

- While quantum technology is still developing, global interest is growing rapidly
- Groundwork needs to begin well before quantum threats become practical

IMAGINE locking an important document in a safe today, confident that nobody has the key. Years later, however, someone invents a tool powerful enough to open that safe.

The document has not changed. The lock has.

That is one way to understand the cybersecurity challenge emerging alongside quantum computing.

Unlike today's computers, quantum computers use principles of quantum mechanics to approach certain complex problems differently. While the technology is still developing, global interest is growing rapidly.

McKinsey's Quantum Technology Monitor 2025 reported that investment in quantum technology start-ups grew by about 50% in 2024 to nearly US$2bil.

In some ways, the journey may feel familiar. Artificial intelligence (AI) spent years largely associated with research laboratories before becoming part of everyday business.

Quantum technology is still at an earlier stage, but it is attracting similar attention as organisations consider its future possibilities and risks.

The concern is not that quantum computers will suddenly make our digital systems unsafe tomorrow.

The more important issue is whether we are preparing early enough for a future in which some of today's encryption methods may no longer be enough.

Harvest now, decrypt later

Today, encryption protects banking transactions, healthcare records, business communications and government information.

However, quantum computers can easily break some of the public-key cryptography security algorithms widely used today.

The risk may begin before quantum computers arrive. Imagine an attacker stealing an encrypted file today.

They may not be able to read it now, but they could store it and attempt to decrypt it years later when quantum technology becomes available.

It is like stealing a locked time capsule because you believe a master key will eventually be discovered.

The National Institute of Standards and Technology (NIST) highlights health records, financial data, intellectual property and national-security information as examples of data that must remain confidential for years or decades.

The World Economic Forum has similarly identified "harvest now, decrypt later" as an immediate quantum-era security concern.

This matters especially for telecommunications networks, which act like the highways of the digital economy, carrying business communications, financial services and digital transactions.

The GSMA says the telecom industry needs to prepare for post-quantum cryptography (PQC) across networks, devices and systems because the transition affects operators, vendors, regulators and technology partners.

Quantum security is therefore increasingly a business resilience and trust issue, not simply another IT upgrade.

What is a quantum-safe network?

A quantum-safe network (QSN) is designed to keep communications secure against future quantum-enabled threats.

One important technology is PQC, which uses cryptographic methods designed to withstand attacks from both conventional and quantum computers, while remaining compatible with existing systems and networks.

Think of PQC as upgrading the lock before a more sophisticated lock-picking machine arrives.

NIST finalised its first three PQC standards in 2024, marking an important step towards future quantum-resistant security.

Another technology being explored is quantum key distribution (QKD), which applies quantum principles to the exchange of encryption keys that ensures the transmitted data cannot be stolen.

In practical terms, PQC can provide the broad foundation for quantum-safe security at the application layer, while QKD adds another layer of protection at the network (connectivity) layer.

Banks, governments and telecommunications providers are already evaluating how these technologies could fit into future security architectures.

Why crypto-agility matters

Security standards will continue to evolve. That is why crypto-agility matters: systems need to be designed so cryptographic technologies can be updated as standards and threats change.

Rather than rebuilding an entire system whenever security requirements evolve, organisations should be able to change the "lock" while keeping the broader infrastructure intact.

This helps digital infrastructure remain adaptable and resilient over the long term.

Where should organisations begin?

Organisations do not need to replace everything immediately.

A practical first step is to understand where cryptography is already used across systems, applications, hardware and services.

It is similar to conducting a fire-safety inspection. Before replacing equipment, you first need to know where the risks are.

NIST recommends building and maintaining a cryptographic inventory, identifying sensitive and long-lived data, and developing migration roadmaps to prioritise systems that need protection.

The approach can therefore be straightforward: identify, prioritise, test, migrate and continuously improve.

Why Malaysia should prepare now

Malaysia's expanding digital economy makes trusted cybersecurity increasingly important.

As services such as 5G, digital banking, healthcare and e-government become increasingly connected, protecting the systems and information behind them becomes more critical.

The Malaysia Digital Economy Blueprint identifies a trusted, secure and ethical digital environment as essential to enabling businesses and society to benefit from digital services while protecting data, privacy and security.

More recently, NACSA's MyKriptografi Action Plan 2026-2030 explicitly identifies preparation for emerging cybersecurity challenges, including the quantum-computing era.

The plan covers government, national critical information infrastructure, industry and academia, and focuses on cryptographic governance, national expertise, trusted technologies, research and innovation.

Preparing for the quantum era will therefore require collaboration between government, industry, academia and research institutions to strengthen standards, talent, research capability and trusted quantum-safe technologies.

Advanced research on QSN

Against this backdrop, TM Research and Development is exploring how future telecommunications infrastructure can be better prepared for the quantum era.

Our advanced research on quantum technology includes adaptive quantum-safe networking architectures, examining how PQC can be combined with selected QKD capabilities to strengthen network threat detection and risks.

We are building a robust collaboration ecosystem with several universities and technology partners within the region to further explore secure communications across different geographies and countries.

Led by two of our leading research centres, the COE of Advanced Cloud and COE of Intelligent Networks, our work also explores crypto-agility through simulation, laboratory testing and interoperability testing. Watch this space!

Preparing before the risk arrives

Preparing for quantum security is much like buying insurance. You prepare before the risk becomes a reality, not afterwards.

Migrating cryptographic systems can take years, so the groundwork needs to begin well before quantum threats become practical.

The quantum era does not need to arrive tomorrow for preparation to make sense today.

By starting early, we are confident Malaysia can build a digital future that is not only more connected, but also trusted and secure.