Quantum-Ready Malaysia

TM R&D's Path to Commercial, Standards-Aligned Quantum-Safe Networks

How post-quantum cryptography (PQC) and quantum key distribution (QKD) can work together and adapt in real time to protect Malaysia's telecommunications, government, banking and critical infrastructure networks.

Quantum-Safe Networking
TM Research & Development

1. Executive Summary

Telecommunications networks run on a form of trust that is quietly enforced by mathematics: a banking transfer, a government file transfer, a private exchange between two data centres, all rely on encryption to stay confidential. A powerful enough quantum computer would undo that guarantee, and while no such machine exists today, the danger is not purely theoretical. Encrypted traffic can be intercepted and archived right now, held in reserve until the computing power needed to break it eventually arrives. Wherever information needs to remain secret for years rather than months, that possibility already changes the calculus.

Two distinct strategies have emerged to answer this. Post-quantum cryptography (PQC) swaps out today's vulnerable mathematics for new algorithms that still run-on conventional hardware, chosen specifically because no known quantum method can break them. Quantum key distribution (QKD) works differently again: Under the protocol’s assumptions and with properly secured implementations, interception of quantum states introduces statistical disturbances that can be detected. Each has something the other lacks, yet most networks deploy them, where they are deployed at all, as isolated systems with no way to adjust automatically when circumstances change.

This paper sets out TM Research & Development's (TM R&D) work to close that gap. Through the Quantum Safe Networking (QSN) research programme, TM R&D is building a crypto-agile architecture that lets a network draw on post-quantum algorithms, quantum key distribution, or a coordinated blend of both, deciding in real time which combination best fits current network conditions. Early research under this programme a hybrid key-orchestration framework developed by TM R&D has already shown promising results in simulation, including sub-ten-millisecond key-renewal times and uninterrupted service continuity while switching between protection methods [1], [8].

This work is deliberately aligned with Malaysia's national direction on quantum-safe migration, including CyberSecurity Malaysia's MySEAL cryptographic standards programme and the recently announced national collaboration between NACSA, MCMC, and IBM on sovereign AI and quantum technology [5], [7]. It also draws on, and is validated against, a growing body of international research and field trials showing that hybrid PQC-QKD architectures are technically achievable in demanding, regulated environments such as banking [9]. The pages that follow explain the threat in plain terms, describe TM R&D's proposed architecture and roadmap, and set out where the research is headed and where industry partners, technology vendors, and government stakeholders can engage.

2. Introduction

Modern networks depend on encryption for almost everything of consequence they carry: medical records, financial transfers, and the control signalling behind national infrastructure all rely on the same underlying assumption that certain mathematical problems are too hard for a computer to solve within a practical amount of time. Quantum computing challenges that assumption directly. Two theoretical algorithms, known as Shor's algorithm and Grover's algorithm, describe how a sufficiently capable quantum machine could unpick the public-key cryptography that much of the internet, and most telecommunications traffic, currently depends on [2].

Such a machine has not been built. Forecasts for when one might exist differ widely among experts, but the timing question matters less than a more basic reality: replacing an organisation's cryptography across an entire network is a slow, multi-year undertaking, and some of the information flowing through networks today has to stay confidential for far longer than that. This is the logic behind the “harvest now, decrypt later (HNDL)” threat an adversary does not need a working quantum computer today at all; recording and storing today's encrypted traffic is enough, with decryption deferred until the technology catches up. That is why standards bodies, regulators, and telecommunications operators increasingly treat this migration as a present-day priority rather than a distant contingency [2].

Two families of technology respond to this threat, and this paper explains both. Post-quantum cryptography replaces vulnerable algorithms such as RSA and elliptic-curve cryptography with new ones standardised in the United States by the National Institute of Standards and Technology (NIST) that run on existing computing hardware but are built on mathematical problems believed to resist quantum attack [2], [3]. Quantum key distribution takes a fundamentally different approach: rather than relying on a hard mathematical problem, it uses the behaviour of individual photons to let two parties share a secret key in a way that makes eavesdropping physically detectable [4]. This paper explains why both matter, why they work better together than apart, and what TM R&D is doing aligned with Malaysia's national quantum-safe direction to bring that combination into a working, deployable capability.

3. Why Quantum-Safe Networking Matters Now

Few organisations carry as much exposure to this shift as a national telecommunications operator. TM's footprint a nationwide fibre network, data centres and edge sites, and the submarine cable systems linking Malaysia internationally is precisely the kind of long-lived, high-value infrastructure the quantum threat is aimed at. The risk is not abstract. TM R&D's own review of the threat landscape identifies several concrete business risks that a delayed migration exposes an operator to: data harvested today and decrypted once quantum computers mature; the compromise of code-signing and digital signatures, which underpin trust in software updates; the ability to retroactively alter the apparent integrity of digitally signed records; and long-term exposure through weaknesses in key-management systems.

Malaysia has already set a national direction on this question. CyberSecurity Malaysia's Post-Quantum Cryptography Migration Framework and its accompanying sandbox give organisations a structured path to follow, and the Ministry of Digital has launched a national quantum-safe migration initiative that puts government agencies on a defined migration timeline [5]. TM R&D's own assessment reaches a similar conclusion about timing: for a telecommunications operator, this is a coordinated, urgent undertaking to begin now, not a routine algorithm upgrade that can be scheduled at leisure.

None of this requires certainty about exactly when a cryptographically relevant quantum computer will exist. What it requires is recognising that the migration itself is slow, that some data must remain confidential well beyond any plausible migration timeline, and that the organisations best positioned to respond are the ones already building the capability rather than waiting for consensus on a date.

4. Background: Quantum Computing, PQC, and QKD

To understand why two different technologies are needed, it helps to understand what each one actually does, in terms that do not require a physics or mathematics background.

- **Quantum computing, briefly:** A classical computer stores information as bits, each either a 0 or a 1. A quantum computer uses qubits, which can exist in a combination of both states at once a property called superposition. This is not simply "faster," it is a different way of exploring possibilities, and for a narrow set of problems, including the mathematics behind widely used encryption, it offers a shortcut that classical computers do not have. Two such shortcuts matter here: Shor's algorithm, which threatens the public-key cryptography used for key exchange and digital signatures, and Grover's algorithm, which weakens (though does not fully break) symmetric encryption by roughly halving its effective key strength [2].
- **Post-quantum cryptography:** PQC does not use quantum technology at all. It uses new mathematical problems, running on the same computers and networks in use today, that are believed to resist attack from both classical and quantum computers. NIST has standardised several such algorithms: ML-KEM for establishing shared keys, and ML-DSA and SLH-DSA for digital signatures, with a further algorithm, HQC, selected in March 2025 as a structurally independent backup in case weaknesses are later found in the lattice-based mathematics underlying ML-KEM [2], [3]. Because PQC needs no new hardware, it is the more immediately deployable of the two technologies, and it forms the protective floor beneath everything described in this paper.
- **Quantum key distribution:** QKD does not encrypt data directly. Instead, it lets two parties agree on a secret key by exchanging information encoded in individual photons over a dedicated quantum channel. Any attempt to intercept or measure those photons disturbs them in a detectable way, so eavesdropping reveals itself rather than passing unnoticed. This gives QKD a form of security based on physics rather than computational difficulty but it requires specialised hardware and dedicated fibre, and its range and cost are real practical constraints [4].
- **Why not choose one?** PQC provides the primary end-to-end quantum-safe cryptographic capability. QKD may provide an additional source of key material for selected high-value links where its operational constraints are justified [4], [14]. PQC is broadly deployable now and provides a resilient baseline; QKD adds a layer of physics-based assurance where the infrastructure and distance allow for it. The practical challenge and the one at the centre of TM R&D's research is coordinating the two so that a network benefits from both without requiring constant manual reconfiguration.

Aspect	Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
Basis of security	Hardness of mathematical problems (lattice-, hash-, code-based)	Laws of quantum physics; measurement disturbs photon states
Hardware needed	Runs on existing computers and network equipment	Requires specialised quantum hardware and dedicated fibre
Eavesdropping	Not directly detectable	Detectable in real time
Standardisation	NIST FIPS 203 / 204 / 205; HQC selected 2025 [2], [3]	ETSI GS QKD interface standards (e.g., 004, 014, 015)
Resistance	Designed to resist Shor's algorithm	Not vulnerable to Shor's or Grover's algorithms (physics-based)

Table 1: Post-Quantum Cryptography and Quantum Key Distribution compared, based on [1], [2], [3], [4]

5. Malaysia's Quantum Readiness and National Direction

Malaysia's approach to the post-quantum transition is coordinated rather than ad hoc. CyberSecurity Malaysia runs MySEAL, a national programme active since 2016 that maintains two lists of trusted cryptographic algorithms: AKSA, covering algorithms already established in international standards, and AKBA, covering newer algorithms not yet incorporated into formal standards elsewhere. Products built on MySEAL-listed algorithms can pursue certification as Produk Kriptografi Terpercaya Negara, or nationally trusted cryptographic products, giving Malaysian organisations a defined, government-endorsed path to quantum-safe deployment rather than having to interpret international standards unassisted [5].

This national effort sits within a broader, internationally recognised pattern. A comparative 2025 analysis of institutional post-quantum migration strategies examining approaches taken by NIST in the United States, ANSSI in France, BSI in Germany, CRYPTREC in Japan, and ENISA across the European Union finds that national frameworks of this kind are now the norm among countries taking the quantum threat seriously, not an unusual step [6]. Malaysia's MySEAL programme, and the government-wide migration target it supports, places the country inside that same international pattern.

Malaysia's quantum ambitions also extend beyond cryptography migration alone. On 9 July 2026, the National Cyber Security Agency (NACSA) and the Malaysian Communications and Multimedia Commission (MCMC) signed a memorandum of understanding with IBM Malaysia, witnessed by the Prime Minister at the National Cybersecurity Summit 2026, to explore the establishment of a National Quantum and Artificial Intelligence Centre of Excellence. The initiative is intended to strengthen Malaysia's capabilities in AI and quantum technology across government, academia, and industry, built around ecosystem development, trusted governance and security, and talent development [7]. For an organisation such as TM R&D, already aligning its own research to MySEAL's algorithm lists, this broader national push reinforces that quantum-safe networking sits inside a larger, sustained national commitment rather than a narrow compliance exercise.

6. TM R&D's Research Capability and Strategic Role

TM R&D's work in this area is concrete and funded, not aspirational. The Quantum Safe Networking for Secured Data Centre (QSN) programme is a TM R&D academic-industry research project. The project sits within TM R&D's wider Centre of Excellence research roadmap, alongside its Advanced Cloud and Intelligent Network programmes, so quantum-safe networking is one strand of a sustained, multi-year institutional research effort rather than a standalone initiative.

The programme is built on recognised and verifiable expertise in post-quantum cryptography. TM R&D actively contributes to Malaysia's national MySEAL Focus Group, where post-quantum cryptographic algorithms are evaluated for potential inclusion in the country's trusted cryptographic algorithm list. Through this involvement, TM R&D looks forward to contributing technical expertise, research insights, and strategic guidance to the Quantum Safe Network (QSN) programme, supporting the evaluation, adoption, and implementation of post-quantum cryptographic technologies across Malaysia's digital infrastructure. This gives the research a direct line to the same national standards process described in the previous section.

The programme has already produced a peer-reviewed research output. An early analytical study developed under this collaboration a hybrid key-orchestration framework combining PQC and QKD was accepted and presented at the 2025 International Conference on Quantum Computing and Communication Technology, held in Kuala Lumpur [1], [8]. That early work, described in more technical detail in the next section, demonstrated in simulation that a software-driven decision layer can coordinate between post-quantum and quantum key sources without disrupting service, holding key-renewal delay below ten milliseconds while adapting automatically to changing network conditions [8]. This is early-stage research, not a finished product, and TM R&D is candid about that gap the next phase of work is aimed at validating the same ideas on physical hardware rather than in simulation alone.

7. Proposed Quantum-Safe Networking Architecture

The architecture TM R&D is developing adds what post-quantum cryptography and quantum key distribution have lacked on their own: a decision-making layer that sits above both and coordinates them in real time, rather than leaving each to run on its own fixed schedule. It is built from three cooperating parts: a post-quantum cryptographic layer performing key exchange with NIST-standardised algorithms such as ML-KEM; a quantum layer supplying physics-based key material through QKD, delivered via a key management system using established interfaces from the European Telecommunications Standards Institute (ETSI); and a key orchestrator that continuously monitors three live indicators how quickly the quantum channel is generating usable keys, the error rate observed on that channel, and the size of the key reserve still available to decide, in real time, which source should supply the next key [1], [8].

Real networks rarely sit still, so instead of one fixed setting, the framework defines three operating zones that track how much quantum key capacity is available against how much the network currently needs. When the quantum channel is running fast and clean, the orchestrator leans on QKD, or a hybrid combination, since that path offers the lowest latency. When quantum capacity only partly covers demand, the hybrid mode takes over fully, blending both sources so service never interrupts. When quantum capacity is constrained or when the quantum bit error rate rises above roughly eleven per cent, the threshold beyond which the channel's output can no longer be trusted the orchestrator switches QKD off and falls back entirely onto post-quantum cryptography, with the session continuing uninterrupted [8]. In practice, this means the network is never less protected than post-quantum cryptography alone would make it, while gaining the extra physical assurance QKD provides whenever the link is capable of supporting it.

This design is not TM R&D's alone to prove. Independent field research reinforces that the underlying approach is technically sound: a 2026 field trial across a real banking network in Spain and Mexico, combining classical cryptography, QKD, and PQC under software-defined orchestration, demonstrated that hybrid architectures of this kind operate reliably in a live, regulated financial environment, with only modest and well-understood latency overhead from key-management integration [9]. Similar layered PQC-QKD network architectures, and quantum-safe designs specifically built for telecommunications infrastructure, have been described in recent research from Europe [10], [11], [12], giving TM R&D's approach a foundation in current, active international research rather than an isolated concept.

8. Hybrid PQC-QKD Testbed Roadmap

Moving from a validated model to a working capability follows a staged path. The QSN programme's roadmap runs across eight stages. It begins with the hybrid PQC/QKD architecture design and use-case identification already described in this paper, followed by technical evaluation of NIST-selected algorithms aligned to Malaysia's AKBA MySEAL 2.1 list. From there, the work moves to configuring post-quantum cryptography on site-to-site IPsec VPN tunnels, then adding crypto-agility so the system can switch algorithms on demand. The second half of the roadmap brings in the quantum channel itself: a point-to-point QKD baseline in a controlled laboratory setting, extension onto production fibre alongside live classical traffic, real-time detection of and safe reaction to attacks or faults, and finally an end-to-end demonstration combining all of the above.

9. Use Cases for Telecommunications, Government, Banking, and Critical Infrastructure

- **Telecommunications.** TM's own network nationwide fibre, data centres, edge facilities, and submarine cable systems is the first and most direct beneficiary of this work, and the reason the QSN programme exists. Recent research into quantum-secure coherent optical networking specifically addresses the kind of infrastructure TM operates, including vulnerabilities in optical network management interfaces that a quantum-safe redesign needs to account for [13].
- **Government.** Malaysia's national migration direction, described earlier in this paper, gives government agencies a defined path and timeline. A telecommunications operator that has already built quantum-safe capability is positioned to support that migration directly, rather than each agency solving the problem independently.
- **Banking.** The clearest external validation of this class of architecture comes from banking. A field trial spanning Spain and Mexico demonstrated that a hybrid QKD-PQC-classical architecture, orchestrated through software-defined networking, can secure real interbank and cloud connections without disrupting existing operations a scenario closely comparable to what TM R&D is building toward for Malaysian financial and enterprise customers [9].
- **Critical infrastructure more broadly.** Beyond banking, the same architecture applies to any sector where long-lived, sensitive data flows across networks: healthcare records, energy-sector control systems, and enterprise connections into hybrid cloud environments all face the same harvest-now-decrypt-later exposure described earlier in this paper.

Taken together, these use cases point toward a commercial product line TM R&D's research is working to eventually support, spanning quantum-safe VPN and SD-WAN offerings, secured links between enterprise customers and hybrid cloud, protected connectivity for IoT deployments, and quantum-safe archiving for data that must stay confidential long term [1].

10. Migration Strategy and Crypto-Agility Framework

A successful migration does not start with choosing algorithms; it starts with knowing what cryptography is already in use. TM R&D's approach follows this inventory-first logic: identifying which cryptographic algorithms, certificates, and keys are active across the network and where, before classifying that inventory by risk and prioritising what needs to change first. From there, the work proceeds through architecture and planning, development and engineering, phased implementation, and ongoing evaluation a five-stage progression that mirrors both TM R&D's own project phases and the structured approach recommended in the broader post-quantum migration literature [1], [6].

Crypto-agility is the property that makes this sustainable rather than a one-time project. Rather than migrating once and hoping the chosen algorithms remain secure indefinitely, a crypto-agile network can switch between classical, post-quantum, and hybrid protection as threats, compliance requirements, or link conditions change, without re-engineering the system each time. This is precisely the behaviour TM R&D's orchestration layer is designed to provide, and it echoes an approach increasingly documented elsewhere: recent research on crypto-agile gateways combining classical, PQC, and QKD key sources in real optical networks describes the same underlying philosophy treat cryptographic protection as something the network adjusts continuously, not something fixed at deployment [14]. Related work on hybrid, group-based quantum-secure communication similarly demonstrates that combining PQC key exchange with QKD protocols can be made to work flexibly across different communication patterns, not just simple point-to-point links [15].

11. Implementation Challenges and Risk Management

TM R&D's own risk assessment for the QSN programme identifies two primary challenges. The first is the cost and availability of QKD hardware: unlike PQC, which runs on conventional computing equipment, QKD requires specialised optical hardware that is not yet widely available from local vendors, and the programme's mitigation is to pursue partnerships rather than in-house acquisition. The second is the depth of local expertise in this still-specialised field, which the programme addresses through its capacity-building focus for local talent.

Independent field research adds further, quantified consideration. The Spain-Mexico banking field trial found that integrating a key-management system into an existing IPsec/IKEv2 setup increased session-establishment latency by a factor of roughly three to fifteen, depending on distance a meaningful overhead, but one that remained comfortably within normal tolerances for wide-area network operations under real-world conditions [9]. This is a useful, externally sourced data point: it confirms that hybrid quantum-safe architectures carry a measurable but manageable performance cost, rather than an unquantified one.

TM R&D's own early research is similarly candid about its current limits. It is worth being clear about what the figures cited earlier in this paper represent: they come from software modelling and analytical calculation, not from measurements taken on physical quantum hardware, and TM R&D has been explicit that the next phase of research is aimed squarely at closing that gap through the physical testbed described in the roadmap above.

12. Commercialization and Industry Partnership Opportunities

TM R&D's quantum-safe networking research is being built collaboratively, and the partnerships already in motion illustrate the direction of travel. TM R&D and other Malaysian organisations have signalled intent to form a consortium to pursue quantum communication capability jointly, reducing the cost and risk of any single organisation acquiring QKD infrastructure alone. Singapore's National Quantum-Safe Network has expressed interest in cross-border quantum key distribution between Malaysian and Singaporean data centres, pointing toward regional, not merely national, quantum-safe infrastructure.

Beyond protecting TM's own infrastructure, this capability is a foundation TM R&D intends to build customer-facing offerings on top of, rather than an end in itself. Meeting Malaysia's national migration framework comes first; the commercial return is what follows once that foundation is in place. Organisations beginning their own quantum-safe planning, and technology partners working in post-quantum cryptography or quantum communication, are invited to engage with TM Research & Development whether to explore the underlying research, contribute to the testbed, or align migration roadmaps with Malaysia's national direction.

13. Conclusion

None of this is a distant, hypothetical concern. Because encrypted traffic can be captured and stored now for decryption later, the exposure is immediate for any organisation whose information must remain confidential for years, and it is a matter of national consequence for an operator whose network carries the communications of banks, hospitals, and government bodies. Post-quantum cryptography and quantum key distribution each solve part of this puzzle on their own, but treated as separate systems and configured by hand, they fall short of the resilience a coordinated approach could deliver.

TM R&D's contribution, grounded in Malaysia's national quantum-safe direction, is to unify the two under a single, real-time decision layer: post-quantum cryptography always active as a protective baseline, quantum key distribution layered on top whenever the link supports it, and the system shifting between the two on its own as conditions evolve. Early results are encouraging, they line up with independent field validation from elsewhere in the industry, and they sit within a funded, staged roadmap toward physical testbed validation. This is research, not yet a finished product, and TM R&D says so plainly. Even so, it gives Malaysian industry, government, and telecommunications stakeholders a credible, standards-aligned starting point for a shift that will happen on quantum computing's timeline, not anyone else's.

14. References and Sources

[1] A. Sanz, E. Salegi, A. Atutxa, D. Franco, J. Astorga, and E. Jacob, “QuLore: An Adaptive Security Framework to Extend Quantum-Safe Communications to Real-World Networks,” arXiv:2511.22416 [cs.CR], Feb. 2026, doi: 10.48550/arXiv.2511.22416.

[2] National Institute of Standards and Technology, “Post-Quantum Cryptography,” Computer Security Resource Center. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[3] National Institute of Standards and Technology, “NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption,” Mar. 2025. [Online]. Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[4] E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and M. Mehic, “Quantum Key Distribution Networks – Key Management: A Survey,” ACM Computing Surveys, vol. 57, no. 10, art. 257, May 2025, doi: 10.1145/3730575.

[5] CyberSecurity Malaysia, “Post-Quantum Cryptography Migration Framework / MySEAL.” [Online]. Available: https://www.cybersecurity.my/portal-main/services/post-quantum-overview

[6] M. El Bizri, A. M. El-Hajj, L. Sliman, and A. M. Haidar, “Institutional Approaches to Post-Quantum Cryptography: A Comparative Analysis of Migration Frameworks,” IEEE Access, vol. 14, pp. 3259–3283, 2026, doi: 10.1109/ACCESS.2025.3650465.

[7] National Cyber Security Agency (NACSA) and Malaysian Communications and Multimedia Commission (MCMC), “NACSA, MCMC and IBM Forge Strategic Partnership to Advance Malaysia’s Sovereign AI and Quantum Future,” press release, Cyberjaya, Malaysia, Jul. 9, 2026.

[8] O. Abuajwa, A. B. Mahmud, R. Mohamad, and S. M. B. M. Hassan, “Hybrid Key Orchestration of PQC and QKD for Adaptive Quantum-Safe Networks,” presented at the Int. Conf. Quantum Computing and Communication Technology (ICQCT), Kuala Lumpur, Malaysia, 2025.

[9] R. J. Vicente et al., “Quantum-safe IPsec in the banking industry,” arXiv:2604.12985v1 [quant-ph], Apr. 2026.

[10] P. Spooren, A. Neuhold, S. Ramacher, and T. Hühn, “PQC-Enhanced QKD Networks: A Layered Approach,” in Proc. IEEE Int. Conf. Quantum Communications, Networking, and Computing (QCNC), Kobe, Japan, Apr. 2026.

[11] A. Fernández-Vilas et al., “QURSA: architecture for quantum-safe 5G,” in Proc. SPIE 13635, Quantum Technologies for Defence and Security II, Madrid, Spain, Oct. 2025, doi: 10.1117/12.3071778.

[12] R. B. Mendez, J. S. Buruaga, J. P. Brito, A. Pastor, D. R. Lopez, and V. Martin, “Quantum resistant software Defined-Networking IPsec, enabling ITS communication over IP networks on real telco infrastructures,” Computer Networks, vol. 280, art. 112171, May 2026, doi: 10.1016/j.comnet.2026.112171.

[13] O. Joseph and I. Aviv, “Quantum-Secure Coherent Optical Networking for Advanced Infrastructures in Industry 4.0,” Information, vol. 16, no. 7, art. 609, Jul. 2025, doi: 10.3390/info16070609.

[14] A. Comin, “Hybrid Quantum Security: Integrating QKD and PQC in Brownfield Optical Networks,” Quantum Information Technologies Journal, 2025, doi: 10.13052/qi2795-0492.116.

[15] J. Sepúlveda, D. Marchsreiter, and F. M. Cardano, “Hybrid Quantum-secure Group-based Communication with PQC and QKD,” in Proc. 28th Euromicro Conf. Digital System Design (DSD), 2025, doi: 10.1109/DSD67783.2025.00077.