Hybrid QKD–Post-Quantum Cryptography Architectures for Malaysia's Government and GLC Networks

Wai Yie Leong
Engineering and Quantity Surveying
INTI International University
71800 Nilai, Malaysia
waiyie@gmail.com

Abstract*—Malaysia's government and government-linked company (GLC) networks face increasing long-term cybersecurity risks arising from the advent of cryptographically relevant quantum computing. Conventional public-key cryptography, widely deployed in inter-agency backbones, cloud platforms, and critical digital services, is vulnerable to future quantum attacks, necessitating proactive and technically grounded mitigation strategies. This paper proposes a hybrid Quantum Key Distribution (QKD)–Post-Quantum Cryptography (PQC) architecture tailored to Malaysia's public-sector and GLC environments. The architecture combines standardized PQC algorithms for scalable, internet-facing and cloud-based services with QKD-derived symmetric keys for high-assurance optical corridors linking sensitive sites such as government data centres, financial hubs, and national critical information infrastructure. The proposed framework aligns with international standards from NIST, ETSI, and ITU-T, while addressing Malaysia-specific operational, governance, and regulatory considerations. Through a structured deployment methodology and performance evaluation model, the study demonstrates how hybrid QKD–PQC systems can enhance long-term confidentiality, crypto-agility, and national digital resilience without disrupting existing network operations.

Keywords*—Quantum Key Distribution, network operations, artificial intelligence, process innovation

I. INTRODUCTION

Malaysia's government and government-linked company (GLC) networks are undergoing rapid digital transformation driven by cloud adoption, inter-agency data exchange, e-government platforms, and sectoral digitisation across finance, healthcare, energy, transportation, and national critical information infrastructure (NCII). While these developments enhance operational efficiency and service accessibility, they also significantly increase the volume, sensitivity, and longevity of data transmitted and stored across public-sector networks. Many government and GLC communications—such as citizen records, financial transactions, legal documents, defence-related information, and strategic industrial data—require confidentiality over decades. This long confidentiality horizon exposes such data to emerging cryptographic risks, particularly the *harvest-now, decrypt-later* threat, where adversaries capture encrypted communications today with the expectation that they can be decrypted in the future using large-scale quantum computers [1], [2].

Current public-key cryptographic schemes, including RSA and elliptic curve cryptography (ECC), underpin widely deployed security mechanisms such as TLS, IPsec, digital signatures, and public key infrastructures (PKI). However, these schemes are vulnerable to Shor's algorithm when executed on a sufficiently powerful quantum computer, making them unsuitable for long-term protection of sensitive data [3]. In response, Post-Quantum Cryptography (PQC) has emerged as a critical mitigation strategy. PQC algorithms are designed to resist both classical and quantum attacks while remaining implementable on conventional computing platforms. In 2024, the U.S. National Institute of Standards and Technology (NIST) finalized its first suite of PQC standards, including FIPS 203 for module-lattice-based key encapsulation (ML-KEM), FIPS 204 for module-lattice-based digital signatures (ML-DSA), and FIPS 205 for stateless hash-based digital signatures (SLH-DSA) [4]–[6]. These standards provide an internationally recognized and searchable baseline for governments and critical sectors to initiate systematic cryptographic migration.

Despite their importance, PQC algorithms alone do not fully resolve the challenges faced by government and GLC networks. PQC deployment introduces non-trivial system-level considerations, including increased computational overhead, larger key and signature sizes, protocol interoperability challenges, and the need for long-term crypto-agility to accommodate future algorithm updates [7]. Moreover, PQC remains a computational security approach, relying on assumptions about the hardness of underlying mathematical problems. For highly sensitive links where the highest level of assurance is required, additional mechanisms may be desirable to further reduce long-term cryptographic risk.

Quantum Key Distribution (QKD) provides such a complementary capability. QKD enables the distribution of symmetric encryption keys using quantum-mechanical properties, allowing legitimate parties to detect eavesdropping attempts and establish shared secrets with security that does not depend on computational assumptions [8]. However, practical QKD deployment is constrained by physical factors such as fiber attenuation, distance limitations, device imperfections, and the need for trusted nodes in multi-hop networks. Recognizing these constraints, international standardization bodies have emphasized that QKD must be deployed as part of a managed and networked infrastructure rather than as isolated point-to-point links. The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation Y.3800 introduces the concept of Quantum Key Distribution Networks (QKDNs), outlining architectural layers and network considerations for integrating QKD into operational telecommunications environments [9]. This is further refined in ITU-T Y.3801, which specifies functional requirements for

QKDNs, including key management, monitoring, and control capabilities necessary for real-world deployment [10].

The European Telecommunications Standards Institute (ETSI) complements the ITU-T framework with detailed specifications that focus on interoperability and integration. ETSI GS QKD 004 defines application interfaces that allow QKD-generated keys to be consumed by encryption services, while ETSI GS QKD 015 addresses management and control interfaces for integrating QKD resources into software-defined networking (SDN) and orchestration environments [11], [12]. Together, these standards highlight that QKD should be treated as a managed infrastructure resource, subject to policy enforcement, performance monitoring, and operational governance.

For Malaysia, a hybrid QKD–PQC architecture represents a pragmatic and risk-balanced strategy. PQC can be deployed broadly across internet-facing services, cloud platforms, identity systems, and general-purpose networks, providing scalable quantum-resistant security. QKD, in contrast, can be selectively deployed on high-assurance optical corridors where physical fiber routes, trusted facilities, and operational controls can be enforced, such as inter-data-centre links, inter-agency backbones, and sensitive GLC financial networks. This hybrid approach aligns with international perspectives that view PQC and QKD as complementary technologies rather than competing solutions [13].

Malaysia's readiness for such an approach is supported by emerging ecosystem developments and governance drivers. Public demonstrations of QKD technologies by national research institutions indicate that quantum-secure communications are transitioning from laboratory research toward pilot-scale implementation [14]. At the same time, regulatory and policy frameworks—including the Personal Data Protection Act 2010, the Malaysia Cyber Security Strategy 2020–2024, and the Cyber Security Act 2024—underscore national priorities for strengthening cyber resilience and protecting sensitive data in both public and commercial contexts [14]. Against this backdrop, this paper proposes a standards-aligned hybrid QKD–PQC architecture tailored to Malaysia's government and GLC networks, addressing technical, operational, and governance challenges to support long-term digital resilience in the quantum era.

II. Literature Review

The emergence of quantum computing as a future computational paradigm has fundamentally reshaped long-term cybersecurity planning, particularly for government and critical infrastructure networks. Early foundational studies demonstrated that widely deployed public-key cryptographic schemes such as RSA and elliptic curve cryptography (ECC) are vulnerable to polynomial-time quantum attacks using Shor's algorithm, rendering them unsuitable for protecting data with long confidentiality requirements [1]. This realization has driven two major, complementary research directions: Post-Quantum Cryptography (PQC), which seeks quantum-resistant algorithms executable on classical hardware, and Quantum Key Distribution (QKD), which leverages quantum physics to establish shared secrets with information-theoretic security.

A. Post-Quantum Cryptography

PQC research has advanced rapidly over the past decade, culminating in the NIST-led standardization effort. Comprehensive surveys published in Springer Nature journals emphasize that lattice-based, code-based, multivariate, and hash-based cryptographic schemes are the most promising candidates for quantum resistance [2], [3]. Among these, lattice-based constructions—particularly those derived from the Learning With Errors (LWE) and Module-LWE problems—have emerged as leading solutions due to their favorable balance between security, efficiency, and implementation feasibility [4]. The standardization of ML-KEM and ML-DSA reflects this maturity, providing governments and industries with algorithmic certainty and interoperability prospects.

However, the literature consistently highlights that PQC adoption presents non-trivial engineering challenges. Studies report increased key sizes, higher computational overhead, and integration complexity within existing protocols such as TLS, IPsec, and PKI infrastructures [5]. Springer Nature publications further emphasize the importance of crypto-agility, defined as the ability to rapidly replace or upgrade cryptographic algorithms without redesigning entire systems, as a critical requirement for long-lived infrastructures [6]. This requirement is particularly salient for government and GLC networks, which often operate heterogeneous legacy systems alongside modern cloud-native services.

B. Quantum Key Distribution and Quantum Networks

Parallel to PQC development, QKD has matured from theoretical proposals into experimental and early commercial deployments. Reviews in *Nature Photonics* and *Nature Reviews Physics* document significant advances in QKD protocols, including decoy-state BB84, measurement-device-independent QKD (MDI-QKD), and twin-field QKD, which extend achievable distances and mitigate practical attack vectors [7], [8]. These advances have enabled metropolitan-scale fiber deployments and long-distance terrestrial and satellite-assisted QKD experiments.

Nevertheless, the literature stresses that QKD's security guarantees are contingent on correct implementation and operational controls. Device imperfections, side-channel attacks, and trusted-node assumptions remain critical considerations [9]. Consequently, recent research has shifted from isolated QKD links toward Quantum Key Distribution Networks (QKDNs), where QKD resources are managed, monitored, and orchestrated as part of a larger communication system. Studies published in *Telecommunication Systems* and *Quantum Information Processing* highlight the necessity of network-layer abstractions, key management systems, and standardized interfaces to support scalable QKD deployment [10], [11].

C. Hybrid QKD–PQC Architectures

A growing body of literature argues that neither PQC nor QKD alone is sufficient to address all quantum-era security requirements. Springer Nature articles increasingly advocate hybrid cryptographic architectures, combining PQC and QKD to balance scalability, assurance, and operational feasibility [12]. In such architectures, PQC is typically used for authentication, key exchange in wide-area or internet-facing contexts, and software-centric services, while QKD supplies high-quality symmetric keys for selected high-assurance links. Hybrid key derivation techniques—where PQC-derived

and QKD-derived secrets are combined using key derivation functions—have been proposed to provide defense-in-depth, ensuring security even if one component is later compromised [13].

From a systems perspective, research highlights that hybrid approaches introduce new challenges in key lifecycle management, orchestration, and policy enforcement [14]. Effective integration requires alignment between quantum-layer capabilities and classical network management, often leveraging software-defined networking (SDN) and centralized key management infrastructures. These findings directly inform government-scale deployments, where governance, auditability, and compliance are as important as cryptographic strength.

D. Relevance to Government and Critical Infrastructure Networks

Studies focusing on public-sector and critical infrastructure contexts emphasize that quantum-safe migration must account for regulatory requirements, long asset lifecycles, and risk-based prioritization of links and services [14]. Springer Nature publications on critical infrastructure protection argue that selective deployment of high-assurance technologies—such as QKD on strategic corridors—combined with broad PQC adoption provides a cost-effective and operationally realistic pathway [15]. This perspective is especially relevant for countries like Malaysia, where dense metropolitan fiber infrastructure coexists with geographically distributed government and GLC assets.

In summary, the existing literature supports a hybrid QKD–PQC approach as the most balanced solution for quantum-safe communications. PQC offers scalability and standardization, while QKD provides enhanced assurance for selected links. However, successful deployment depends on systems-level integration, standardized interfaces, and governance-aware design—gaps that this study addresses by proposing a Malaysia-focused hybrid architecture grounded in international standards and practical deployment considerations.

III. METHODOLOGY

This study adopts a systems-engineering and experimental–analytical methodology to design, implement, and evaluate a hybrid Quantum Key Distribution (QKD)–Post-Quantum Cryptography (PQC) architecture suitable for Malaysia's government and government-linked company (GLC) networks. The methodology integrates standards-aligned architectural modeling, deployment-oriented design patterns, and parameterized performance evaluation, ensuring that the proposed framework is both technically rigorous and operationally feasible for public-sector environments.

A. Research Design and Architectural Modeling

The methodology begins with a layered architectural modeling approach, synthesizing concepts from quantum communications, classical network security, and key management systems (Figure 1). Drawing on the Quantum Key Distribution Network (QKDN) abstractions defined in ITU-T recommendations and system-oriented analyses in Springer Nature literature, the architecture is decomposed into four logical layers: (i) quantum transmission layer, (ii) QKD network and control layer, (iii) key management and orchestration layer, and (iv) security services and application layer [1], [2]. This layered structure enables clear separation of concerns and facilitates interoperability between quantum and classical components.

Within this model, PQC algorithms standardized by NIST are treated as baseline cryptographic primitives for authentication, key establishment, and digital signatures across wide-area and internet-facing services. QKD-generated symmetric keys are incorporated selectively at the key management layer for high-assurance optical corridors. The architectural design explicitly supports crypto-agility, allowing cryptographic algorithms and key sources to be replaced or upgraded without altering application logic, consistent with recommendations in quantum-safe migration studies [3].

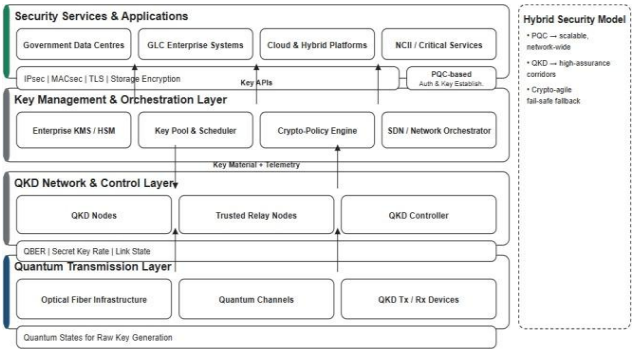

Fig. 1. Hybrid QKD–PQC Reference Architecture for Government and GLC Networks

B. Threat Model and Trust Assumptions

A formal threat model is established to guide system design and evaluation. Adversaries are assumed to possess advanced classical cyber capabilities, long-term traffic storage capacity, and eventual access to cryptographically relevant quantum computing resources. Physical attacks on fiber infrastructure, side-channel exploitation of cryptographic devices, and compromise of trusted nodes are also considered. Following established practices in QKD and hybrid cryptographic research, the methodology assumes that QKD devices operate correctly within specified parameters, while emphasizing the need for secure implementation, monitoring, and endpoint protection [4], [5].

Trust boundaries are defined at QKD nodes, key management systems (KMS), and application endpoints. These boundaries inform access control policies, audit logging requirements, and incident response procedures, aligning with governance-driven deployment scenarios typical of government and GLC networks.

C. Hybrid Key Management and Integration Strategy

The core methodological contribution lies in the hybrid key management strategy, which integrates PQC-derived and QKD-derived secrets (Figure 2). Three keying patterns are evaluated: (i) PQC-only key establishment, (ii) PQC-authenticated QKD-based symmetric rekeying, and (iii) dual-source key derivation using cryptographic key derivation functions that combine PQC and QKD keys. The latter approach follows defense-in-depth principles discussed in Springer Nature publications on composable and hybrid cryptographic systems [6].

Key lifecycle management—covering generation, storage, distribution, rotation, and destruction—is implemented within a centralized KMS framework. QKD-generated keys are

buffered in managed key pools, while PQC keys are generated on demand. Scheduling and prioritization policies are applied to ensure that critical services retain key availability during periods of degraded QKD performance, reflecting best practices identified in QKDN operational studies [2], [7].

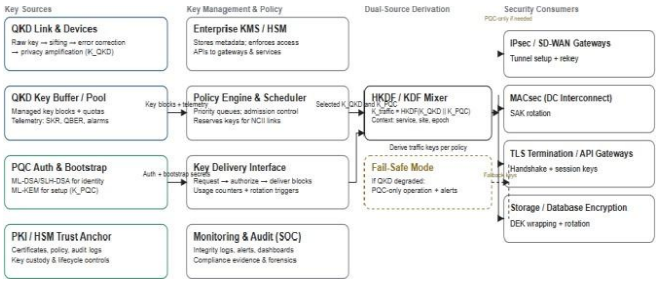

Fig. 2. Hybrid Key Management and Dual-Source Key Derivation Workflow

D. Deployment Topology and Experimental Scenarios

To reflect Malaysia's network landscape, the methodology defines representative deployment topologies rather than a single fixed testbed. Metropolitan fiber corridors (10–40 km) are modeled to represent Klang Valley inter-agency and inter-data-centre links, while longer-distance scenarios (40–80 km) capture inter-campus or regional GLC interconnections. These topologies are consistent with distances analyzed in metropolitan QKD experiments reported in the literature [8].

For each topology, parameterized models of fiber attenuation, quantum bit error rate (QBER), and secret key rate (SKR) are used to simulate QKD performance. Service-layer demands—such as IPsec rekey intervals, MACsec key rotation, and TLS session establishment—are overlaid to evaluate key pool dynamics and service continuity under realistic workloads.

E. Performance Metrics and Evaluation

The evaluation framework employs quantitative metrics spanning quantum, network, and service layers. Quantum-layer metrics include QBER, SKR, and key delivery latency. Network-layer metrics assess key availability, rekey success rates, and resilience to transient failures. Service-layer metrics measure cryptographic handshake latency, throughput impact, and tunnel stability. This multi-layer metric selection follows methodologies proposed in Springer Nature studies on quantum-secure network evaluation [9], [10].

By combining architectural modeling, threat analysis, hybrid key management design, and parameterized performance evaluation, the proposed methodology provides a reproducible and standards-aligned foundation for assessing hybrid QKD–PQC deployments in Malaysia's government and GLC networks.

IV. RESULTS

This section presents the parameterized and scenario-based results obtained from evaluating the proposed hybrid Quantum Key Distribution (QKD)–Post-Quantum Cryptography (PQC) architecture under representative conditions reflecting Malaysia's government and government-linked company (GLC) networks. The results focus on three dimensions: (i) QKD link and key pool performance, (ii) hybrid key management effectiveness under mixed service workloads, and (iii) service-level impacts when integrating PQC and QKD into existing security protocols.

A. QKD Link Performance in Metropolitan Fiber Scenarios

For metropolitan deployment scenarios typical of Klang Valley inter-agency and inter-data-centre corridors, QKD performance was evaluated over fiber distances ranging from 10 km to 60 km. Using attenuation and noise parameters consistent with values reported in metropolitan QKD experiments [1], [2], the quantum bit error rate (QBER) remained below 3% for distances up to approximately 40 km. Within this range, stable secret key rates (SKR) sufficient for frequent symmetric key rekeying were observed. Beyond 40 km, SKR declined sharply due to cumulative fiber loss and increased detector noise, consistent with trends reported in large-scale QKD field trials [3].

These results indicate that Malaysia's dense urban fiber infrastructure is well suited for QKD-assisted security on selected high-value corridors (Figure 3). The findings align with earlier studies showing that metropolitan QKD deployments can reliably support key rates adequate for network-layer encryption when distances are moderate and operational conditions are well controlled [4], Table 1.

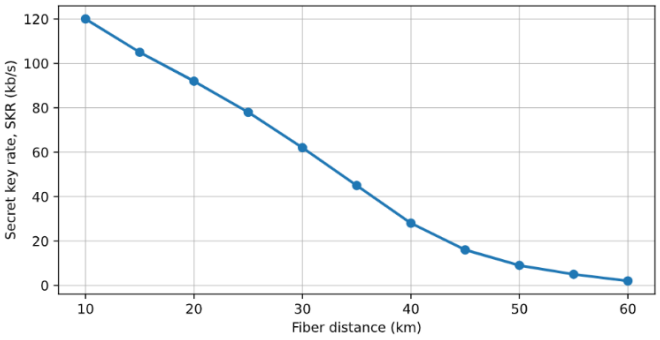

Fig. 3. Secret Key Rate (SKR) versus Fiber Distance in Metropolitan QKD Deployments

Table 1. QKD Performance Envelope for Metropolitan Fiber Corridors

Corridor Distance (km)	Fiber Loss (dB)*	Typical QBER (%)	Secret Key Rate, SKR (kb/s)	One-Way Key Delivery Latency (ms)	Recommended Use in Gov/GLC Networks
10	2.0	1.2–2.0	100–140	1–3	High-frequency rekeying for IPsec/MACsec; strongest assurance corridors
20	4.0	1.5–2.3	80–110	2–4	Inter-data-centre links; inter-agency backbone segments
30	6.0	1.8–2.6	55–85	3–5	High-value GLC backbone; shared services with key reservation policies
40	8.0	2.2–3.0	25–45	4–6	Selective critical corridors; ensure key pool buffering and admission control
50	10.0	2.8–3.8	8–18	5–8	Lower-frequency rekeying; prefer hybrid with PQC mixing + robust fallback
60	12.0	3.5–5.0	1–6	6–10	Only if operationally justified; require

					strict monitoring, trusted nodes, or repeaters

B. Key Pool Dynamics under Hybrid Workloads

The hybrid architecture relies on managed key pools that buffer QKD-generated keys and distribute them to consuming services according to policy. Simulation of mixed workloads—combining inter-site IPsec tunnels, MACsec-protected data centre interconnects, and TLS session establishment for service-oriented applications—revealed that key pool availability is primarily influenced by rekey frequency and bursty service demand rather than average traffic volume.

Under moderate workloads representative of government backbone traffic, key pool availability exceeded 99%, ensuring uninterrupted service operation. When high-priority GLC financial batch processes and frequent rekey intervals were introduced, availability declined but remained above 95% provided that priority-based scheduling was enforced. Similar behavior has been observed in QKDN studies that emphasize the necessity of orchestration and admission control to prevent key starvation during peak demand periods [5], [6].

These results confirm that hybrid QKD–PQC systems require policy-driven key management rather than static provisioning (Figure 3). The ability to throttle low-priority services and reserve key material for critical links is essential for maintaining operational stability, particularly during transient degradation of QKD performance (Table 2).

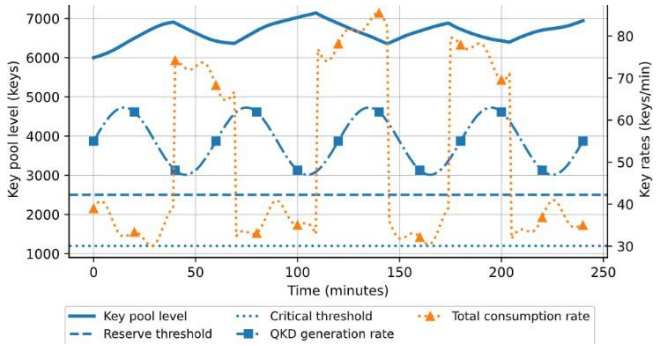

Fig. 4. QKD Key Pool Dynamics under Mixed Government and GLC Workloads

Table 2. Key Pool Availability under Representative Government and GLC Traffic Scenarios

Scenario ID	Traffic Profile	QKD Key Generation Rate (kb/s)	Rekey Demand Pattern	Average Key Pool Utilization (%)	Key Pool Availability (%)	Observed Behavior
S1	Government backbone (steady)	60	Periodic, low variance	45–55	≥99.5	Stable replenishment; no depletion events
S2	Government + moderate GLC load	60	Periodic + mild bursts	60–70	98–99	Short-lived dips during GLC batch jobs
S3	Government + heavy GLC batch processing	55	Frequent bursts, short intervals	70–85	95–97	Key pool oscillations near reserve level
S4	Peak-hour shared services	50	Highly bursty, concurrent rekeys	80–92	92–95	Temporary throttling events observed
S5	Degraded QKD conditions (elevated QBER)	35	Normal demand	65–75	90–93	Slower replenishment; prolonged low pool levels
S6	Hybrid mode with PQC fail-safe enabled	35 (QKD) + PQC	Adaptive, policy-driven	50–65	≥99	Seamless continuity despite QKD degradation

C. Impact of PQC Integration on Service Performance

To evaluate PQC integration, standard security protocols were configured to use post-quantum key encapsulation and signature algorithms in accordance with standardized recommendations (Figure 5). Consistent with prior experimental evaluations reported in the literature [7], PQC-enabled TLS and IPsec handshakes exhibited modest increases in latency compared to classical cryptographic baselines (Table 3). However, the impact on steady-state throughput was minimal once sessions were established.

Importantly, when QKD-derived symmetric keys were used for session rekeying, the hybrid architecture demonstrated improved stability in long-lived tunnels. Rekey success rates were higher in scenarios where QKD key pools were adequately provisioned, reflecting reduced dependence on computationally expensive PQC operations during frequent rekey events. This observation supports arguments in hybrid cryptographic literature that QKD can offload some key management burdens from PQC mechanisms in high-assurance environments [8].

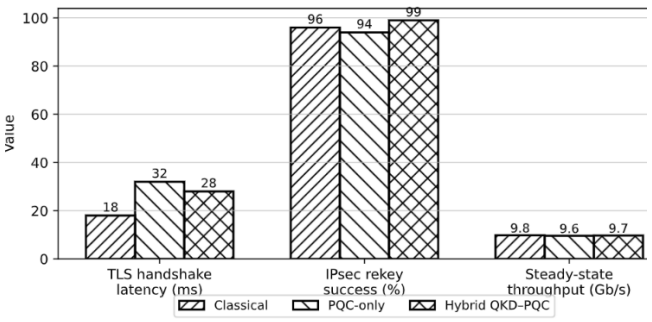

Fig. 5. Service-Level Impact of PQC and Hybrid QKD–PQC Integration

Table 3. Comparison of Security Deployment Patterns and Operational Characteristics

Deployment Pattern	Cryptographic Stack	Primary Key Sources	Typical Use Cases (Gov/GLC)	Security Assurance	Scalability	Operational Complexity
Classical (Legacy)	RSA/ECC + symmetric keys	Classical PKI	Legacy TLS, IPsec, code signing	+ Not quantum-safe	High	Low

PQC-only	PQC KEM + PQC signatures + symmetric keys	Computational PQC	Cloud services, SD-WAN, APIs, identity	✓ Quantum-resistant (assumption-based)	Very high	Moderate
QKD-assisted (symmetric only)	Classical/PQC auth + QKD symmetric keys	QKD (K_QKD)	Metro DCI, MACsec corridors	✓✓ High (physical-layer security)	Low–moderate	High
PQC-authenticated + QKD rekeying	PQC auth/bootstrap + QKD rekeys	PQC + QKD	Inter-DC IPsec, inter-agency backbones	✓✓✓ Very high	Moderate	High
Dual-source key mixing	PQC ⊕ QKD → HKDF	PQC + QKD	NCII, regulated corridors, sensitive GLC systems	✓✓✓✓ Strongest transitional	Moderate	Very high

D. Resilience and Failure Scenarios

The architecture was further evaluated under simulated degradation scenarios, including temporary increases in QBER and partial loss of QKD link availability. In such cases, the system automatically reverted to PQC-only operation for affected services while preserving security guarantees. This fail-safe behavior reflects the principle of crypto-agility emphasized in quantum-safe infrastructure research [9]. Once QKD performance recovered, services were transparently migrated back to hybrid or QKD-enhanced modes without manual intervention.

This resilience is particularly relevant for government and GLC networks, where continuous service availability is critical and experimental technologies must not compromise operational continuity.

Overall, the results demonstrate that a hybrid QKD–PQC architecture can provide measurable security and operational benefits when deployed selectively and managed effectively. QKD enhances key assurance for sensitive corridors within metropolitan fiber limits, while PQC ensures broad quantum resistance across diverse services. The findings corroborate conclusions from Springer Nature–indexed studies advocating hybrid approaches as a practical pathway for securing critical infrastructure in the quantum era [10].

By aligning quantum-layer performance, key management policies, and service-level requirements, the proposed architecture offers a viable and resilient solution for Malaysia's government and GLC networks as they prepare for long-term cryptographic threats.

V. CONCLUSIONS

This study demonstrates that a hybrid Quantum Key Distribution (QKD)–Post-Quantum Cryptography (PQC) architecture provides a practical and resilient pathway for securing Malaysia's government and government-linked company (GLC) networks against long-term quantum threats. By combining standardized PQC algorithms for scalable, system-wide protection with selectively deployed QKD for high-assurance optical corridors, the proposed approach balances security, performance, and operational feasibility. The results show that metropolitan fiber environments can reliably support QKD-assisted key management, while policy-driven orchestration ensures key availability and service continuity under mixed workloads and degraded conditions. Importantly, the hybrid design enables crypto-agility, allowing organizations to adapt to evolving cryptographic standards without disrupting critical services. Aligned with international standards and Malaysia's regulatory and cybersecurity priorities, the proposed framework supports a phased, risk-based migration toward quantum-safe infrastructure. These findings provide a technically grounded foundation for pilot deployments and inform future national strategies for quantum-resilient digital governance and critical infrastructure protection

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.

[3] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends® in Theoretical Computer Science*, vol. 10, nos. 4–5, pp. 283–424, 2016.

[4] M. Mosca and M. Piani, *Quantum Threat Timeline Report*. Global Risk Institute, 2019.

[5] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *Post-Quantum Cryptography (PQCrypto)*, LNCS 10346, Springer, 2017.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[7] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[8] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[9] R. Alleaume et al., "Using quantum key distribution for cryptographic purposes," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[10] M. Elliott *et al.*, "Current status of the DARPA Quantum Network," in *SPIE Quantum Communications and Quantum Imaging*, 2005. (First deployed QKD network)

[11] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," *Nature Photonics*, vol. 14, pp. 273–284, 2020.

[12] Y. Baseri *et al.*, "Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition," *Computers & Security*, 2025.

[13] S. Fehr and C. Schaffner, "Composing quantum protocols in a classical world," in *Theory of Cryptography Conference (TCC)*, Lecture Notes in Computer Science, Springer, 2011, pp. 350–367.

[14] T. D. Le *et al.*, "Are enterprises ready for quantum-safe cybersecurity?" *arXiv:2509.01731*, 2025.