ISSN: 2993-5377

Research Article

Open Access Journal of Applied Science and Technology

Beyond the Perimeter: Toward a Quantum-Integrated SDN-Container Security Architecture for the Post-Classical Threat Environment

Troy Coienth Troublefield, DBA, Ph.D., CAIS[1-3]*

[1]*Department of Information Technology, Capella University, Minneapolis, MN, USA*

[2]*Department of Cyberpsychology, Capitol Technology University, Laurel, MD, USA*

[3]*Department of International Business, International School of Management, Paris, France.*

***Corresponding Author**
Troy Coienth Troublefield, Department of Information Technology, Capella University, Minneapolis, MN, USA and Department of Cyberpsychology, Capitol Technology University, Laurel, MD, USA and Department of International Business, International School of Management, Paris, France.

Submitted: 2026, Jun 30 **Accepted:** 2026, Jul 20; **Published:** Under Process

Citation: Troublefield, T. C. (2026). Beyond the Perimeter: Toward a Quantum-Integrated SDN-Container Security Architecture for the Post-Classical Threat Environment. *OA J Applied Sci Technol, 4*(2), 01-08.

Abstract

Contemporary cybersecurity architecture confronts a dual disruption: the escalating sophistication of classical adversarial threats in virtualized network environments and the emergent threat posed by quantum computing to the cryptographic foundations underpinning those environments. This article develops a conceptual framework, the Quantum-Integrated SDN-Container Security Architecture (QISCA), that extends practitioner-grounded findings from a prior generic qualitative inquiry on software-defined networking (SDN) and container integration into the quantum threat horizon (Troublefield, 2025). Drawing on five empirically derived themes, security enhancement strategies, implementation dynamics, operational management, threat detection, and comparative security analysis, this article argues that the centralized programmability of SDN and the micro-segmentation capabilities of container environments constitute a strategically superior foundation for post-quantum cryptographic (PQC) migration compared to traditional perimeter-based architectures. QISCA synthesizes quantum-resistant key distribution through SDN control planes, container-native post-quantum cryptographic enforcement, quantum-enhanced behavioral anomaly detection, and human-centered adoption governance grounded in the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT). The framework addresses five critical convergence challenges: cryptographic agility under quantum threat, attack surface amplification in quantum-classical hybrid environments, quantum-induced cognitive load on human operators, organizational readiness for simultaneous architecture and cryptographic transformation, and the governance of quantum key distribution (QKD) integration within dynamic container orchestration. The article concludes with a five-domain research agenda for empirical validation of QISCA across government, defense, and critical infrastructure contexts.

Keywords: Quantum Computing, Post-Quantum Cryptography, Software-Defined Networking, Container Security, Quantum Key Distribution, Cybersecurity Architecture, Cryptographic Agility, QISCA, Technology Acceptance, Quantum Threat

1. Introduction

The history of network security is a history of architectural response to paradigm-shifting threats. The transition from host-based to perimeter-based security responded to the proliferation of networked computing. The subsequent shift toward software-defined and virtualized security architectures, the subject of a prior empirical investigation in the study responded to the dissolution of meaningful network perimeters under cloud computing and distributed application architectures. The field now faces a third paradigm shift, one that operates not at the level of network topology or application deployment but at the mathematical bedrock of cryptographic security itself: the emergence of fault-tolerant quantum computing.

Quantum computers capable of executing Shor's algorithm at operationally relevant scale will render the RSA, Diffie-Hellman,

and elliptic curve cryptographic schemes that currently protect the vast majority of networked communications, including those traversing SDN control planes and container orchestration systems, computationally tractable [1]. The National Institute of Standards and Technology formalized PQC standards in August 2024, establishing CRYSTALS-Kyber for key encapsulation and CRYSTALS-Di lithium for digital signatures as the primary migration targets (NIST, 2024). However, the standardization of quantum-resistant algorithms does not by itself solve the deployment problem: cryptographic migration at enterprise scale requires an infrastructure capable of enforcing new cryptographic policies dynamically, detecting non-compliant cryptographic usage, and managing key distribution in environments characterized by rapid provisioning, ephemeral workloads, and dynamic network reconfiguration.

This is precisely the infrastructure that SDN-container integration provides. The qualitative inquiry documented, through interviews with ten cybersecurity professionals across small to medium-sized enterprises (SMEs), that SDN's centralized programmable control plane and container micro-segmentation capabilities together enable dynamic policy enforcement, granular access control, real-time threat detection, and automated security policy replication, capabilities that, this article argues, are not merely compatible with PQC migration but architecturally necessary for its sustainable execution at scale.

The contribution of this article is conceptual and synthetic: it constructs a novel framework, the QISCA, that extends the empirical findings into the quantum threat domain, integrates the current state of post-quantum cryptographic research and QKD technology, and grounds the governance of this architectural transition in established technology adoption theory. The central argument is that organizations that have implemented or are implementing SDN-container integration possess a quantum-resilience advantage over those relying on traditional architectures, but only if that advantage is systematically cultivated through deliberate PQC policy enforcement, quantum-aware threat detection, and human-centered adoption governance.

Following this introduction, the methodology is discussed, review the quantum threat landscape and its specific implications for SDN-container environments. We then present the five QISCA domains derived from the thematic findings. A framework was developed with theoretical grounding in TAM and UTAUT as applied to quantum-era adoption challenges. The governance and implementation considerations for QISCA deployment were examined. Finally, five-domain research agenda for empirical validation were proposed

2. Methodology

This article employs a conceptual-synthetic research design rather than a primary empirical one. Its purpose is theory construction: the development of an integrative conceptual framework, the QISCA, that extends an existing body of practitioner-grounded empirical findings into a problem domain those findings did not originally address. Conceptual research of this kind is appropriate when the scholarly task is not the generation of new observational data but the disciplined integration of established empirical findings, technical standards, and theoretical constructs into a coherent framework that reorganizes how a problem is understood and approached (Jaakkola, 2020; MacInnis, 2011). The contribution sought here is integrative rather than descriptive or explanatory in the empirical sense: QISCA does not report what is observed in a sample but proposes how independently developed bodies of knowledge, SDN-container security practice, post-quantum cryptographic migration, quantum key distribution, quantum-enhanced threat detection, and technology-adoption theory, cohere into a single architecture and migration pathway.

The framework is developed within a pragmatist philosophical orientation. Pragmatism privileges the practical consequences and actionability of knowledge over commitment to a single ontological or epistemological position, which is the appropriate stance for a framework whose value is measured by its capacity to guide organizational migration decisions and to generate testable propositions (Creswell & Plano Clark, 2018). Consistent with this orientation, the framework is constructed to be falsifiable: each of its central claims is articulated with sufficient precision that it can be subjected to subsequent empirical validation, and the article concludes with a five-domain research agenda specifying the measurable outcomes through which those claims may be confirmed or refuted.

2.1. Foundational Empirical Source

The empirical foundation for QISCA is the author's prior generic qualitative inquiry into how cybersecurity professionals view the integration of software-defined networking and containers to improve network security. That study employed semi-structured interviews with ten cybersecurity professionals working across small to medium-sized enterprises and analyzed the resulting data using reflexive thematic analysis, yielding five empirically derived themes: strategies for enhancing network security; implementation benefits, challenges, and adoption dynamics; operational management and expertise requirements; security monitoring, threat detection, and compliance; and the comparative analysis of traditional versus integrated security architectures [2]. These five themes constitute the practitioner-validated substrate from which the present framework is built. The current article does not re-collect or re-analyze the primary interview data; rather, it draws upon the published thematic findings, including specific participant statements reported in the original study (e.g., the characterizations offered by participants designated P2, P4, P8, P9, and P10), as the grounded departure point for conceptual extension. This constitutes a secondary, theory-extending use of qualitative findings, a recognized and methodologically legitimate practice in which validated empirical results serve as the evidentiary anchor for the development of new conceptual work in an adjacent or successor problem space.

The decision to ground QISCA in an existing qualitative study, rather than to generate the framework from the technical

literature alone, is methodologically deliberate. It ensures that the framework's architectural claims are tethered to the operational realities reported by practitioners actually responsible for SDN-container security, rather than resting solely on the theoretical affordances of the technologies. The five themes function not as illustrative material but as the structural skeleton of the framework: each QISCA domain is derived from, and traceable to, a specific theme, such that the framework's organization is dictated by the empirical findings rather than imposed upon them.

2.2. Framework Construction Procedure

QISCA was constructed through a structured, multi-stage analytic procedure designed to make the derivation of the framework transparent and reproducible. In the first stage, thematic mapping, each of the five themes were examined to identify the underlying architectural or organizational capability it represented, abstracted from its original classical-security context. Theme 1, for example, was abstracted to the capability of centralized, programmable policy enforcement; Theme 3 to the human-factors and expertise determinants of secure operation; Theme 5 to the comparative-architecture assessment of integrated versus traditional approaches. This abstraction step isolated the transferable mechanism within each theme from the specific classical application in which it was originally observed.

In the second stage, quantum-context extension, each abstracted capability was projected into the post-quantum threat environment to determine how it would bear on the distinct requirements of cryptographic migration, quantum key distribution, and quantum-era threat detection. This projection was governed by a consistent inferential logic: a capability that demonstrably improved a classical security outcome was extended to its quantum analogue only where the underlying mechanism was indifferent to the classical-versus-quantum distinction. Centralized policy enforcement, for instance, was extended to cryptographic-algorithm-policy enforcement because the enforcement mechanism, the SDN controller's capacity to apply and monitor policy across the network fabric, operates identically regardless of whether the policy concerns segmentation rules or permitted cipher suites. This stage produced the five QISCA domains, each pairing an empirical origin with a quantum security extension (presented in Table 1).

In the third stage, standards anchoring, each domain was aligned to the authoritative technical standard or guidance governing its quantum security extension, including NIST FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) for cryptographic agility, ETSI GS QKD 004 and the BB84/E91 protocols for quantum key distribution, NIST IR 8413 for quantum-enhanced detection, CISA (2024) migration guidance for operational resilience, and the NSA CNSA 2.0 suite for comparative migration strategy. This anchoring ensures that the framework's prescriptions are not free-floating but are tied to the formal standards against which organizational migration will ultimately be measured.

In the fourth stage, literature integration, the emerging framework was systematically situated within and tested against three distinct bodies of scholarship: the SDN and container security literature, e.g., [3-6], the post-quantum cryptography and quantum key distribution literature, e.g., [7-11], and the quantum machine learning literature, e.g., [12,13]. This integration served both to corroborate the framework's technical claims and to identify the precise intersection, the dependence of migration outcomes on network architecture, that the existing literatures had left underexamined and that QISCA is positioned to address.

2.3. Theoretical Integration

The framework's analysis of adoption dynamics was grounded in two established technology-adoption theories selected for their direct continuity with the foundational study, which itself applied these lenses to SDN-container adoption. The Technology Acceptance Model supplied the constructs of perceived usefulness and perceived ease of use; the Unified Theory of Acceptance and Use of Technology supplied the constructs of facilitating conditions and social influence [14,15]. These theories were applied not as post hoc justification but as analytic instruments for diagnosing why architecturally capable organizations may nonetheless fail to migrate. This theoretical layer was further integrated with behavioral-economic constructs, prospect theory and the loss-aversion and temporal-discounting biases it describes, and the low-probability, high-consequence decision problem, to model the distinctive adoption profile of a defensive technology whose benefits are probabilistic and future-oriented [16,17]. The selection of these specific frameworks, rather than alternative adoption or diffusion theories, was dictated by methodological consistency with the underlying empirical study, preserving the analytic continuity between the validated findings and their quantum extension.

2.4. Instrument Development

Two structured analytic instruments were developed as derivatives of the framework. The Quantum Readiness Assessment (QRA) was constructed as a five-dimension, four-level maturity rubric (presented in Table 2), with dimensions, cryptographic inventory completeness, PQC migration capability, QKD infrastructure readiness, operator quantum literacy, and governance maturity, derived from the organizational readiness considerations advanced across the five QISCA domains. The phased migration roadmap was developed by translating the framework's domain prescriptions into a four-phase temporal sequence (Inventory and Assessment, Pilot PQC Deployment, Production Migration, and Operational Resilience), with phasing logic drawn from the pilot-first, incremental implementation pattern that identified as the most consistent success factor across SDN-container deployments. The comparative-complexity analysis (presented in Table 3) was constructed by evaluating SDN-container, traditional perimeter, and hybrid architectures against five migration dimensions, with the assessments derived from the architectural capabilities documented in the foundational study and the migration-timeline characteristics reported in the implementation-guidance literature.

2.5. Validity, Rigor, and Trustworthiness

Because this is conceptual rather than primary empirical work,

its rigor is assessed against the criteria appropriate to theory-building scholarship rather than against the reliability and validity standards of empirical measurement. Three criteria were applied. Logical coherence was pursued by ensuring that each framework component follows transparently from its stated empirical origin and that the inferential rule governing quantum extension, transfer only where the underlying mechanism is invariant to the classical-quantum distinction, was applied consistently across all five domains. Traceability was pursued by maintaining an explicit, auditable linkage from each QISCA domain back to a specific theme in the foundational study and forward to a governing technical standard, such that no element of the framework rests on unsupported assertion. Falsifiability was pursued by articulating the framework's central propositions as empirically testable claims and by specifying, in the accompanying research agenda, the measurable outcomes and study designs through which each could be validated or refuted across government, defense, healthcare, and critical infrastructure contexts.

3. Methodological Limitations

Several limitations constrain the conclusions that may be drawn from this work and are acknowledged as boundary conditions on the framework. First, QISCA inherits the contextual scope of its empirical foundation sample, that was comprised of ten professionals in small to medium-sized enterprises, and the architectural advantages the framework describes may manifest differently at enterprise and hyperscale tiers or in sectors not represented in the original study. Second, the framework is conceptual and therefore unvalidated; its central claim, that SDN-container environments achieve faster, more complete, and more verifiable PQC migration than traditional architectures, is a derived hypothesis rather than a demonstrated empirical result. Third, the framework's QKD and quantum-machine-learning components rest on capabilities whose operational maturity remains uncertain, such that those domains are necessarily more anticipatory than the PQC-migration domain, which is grounded in finalized standards. These limitations are not incidental; they define precisely the empirical work that the concluding research agenda is designed to motivate, and they situate QISCA as a framework offered for testing rather than as a set of validated findings.

3.1. The Quantum Threat Landscape and Its Implications for Virtualized Network Security

The advent of cryptographically relevant quantum computers poses an existential threat to the cryptographic foundations of contemporary network security, simultaneously undermining the asymmetric algorithms that secure key exchange and authentication and weakening the symmetric primitives that protect data confidentiality. This threat is rendered immediate rather than speculative by harvest-now-decrypt-later attacks (HNDL), in which adversaries collect encrypted traffic today for retroactive decryption once quantum capabilities mature, placing at risk precisely the high-value data, classified information, intellectual property, and critical infrastructure control traffic, that traverses enterprise networks and retains strategic value for decades. SDN and container architectures occupy a paradoxical position within this landscape: their centralized control planes, dynamic provisioning, and dependence on public-key-protected communications introduce distinctive quantum vulnerabilities, even as those same properties of centralized programmability, automated policy replication, and image-based software distribution offer structural advantages for systematic post-quantum migration. This section examines both dimensions of that paradox, situating the quantum threat within the operational realities of virtualized network environments and grounding the analysis in practitioner-validated findings regarding SDN-container security. It then introduces the QISCA, a five-domain conceptual framework that extends these empirical findings into the quantum security context to provide organizations a structured pathway toward quantum-resilient network security.

3.2. The Cryptographic Disruption

Quantum computing's threat to contemporary cybersecurity operates through two primary attack vectors. The first, applicable to asymmetric cryptography, derives from Shor's (1994) algorithm, which enables a fault-tolerant quantum computer to factor large integers and compute discrete logarithms in polynomial time, rendering RSA, Diffie-Hellman, and elliptic curve Diffie-Hellman (ECDH) insecure [1]. The second, applicable to symmetric cryptography and hash functions, derives from Grover's algorithm, which provides a quadratic speedup for unstructured search, effectively halving the security level of symmetric encryption and requiring key length doubling (e.g., AES-128 to AES-256) for equivalent post-quantum security [18].

The operational timeline of this threat is contested. Mosca (2018) proposed a widely cited risk calculus: if the probability that cryptographically relevant quantum computers (CRQCs) emerge within x years is greater than the sum of the time required to implement quantum-safe cryptography and the desired security shelf life of protected data, migration becomes immediately necessary [10]. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have recommended that critical infrastructure operators begin PQC migration immediately, irrespective of uncertainty about CRQC timelines, given the threat of HNDL attacks in which adversaries collect encrypted traffic today for decryption once CRQCs become available [19,20].

HNDL attacks are particularly acute for networked security environments because the data most valuable to nation-state adversaries, classified information, intellectual property, critical infrastructure control data, personally identifiable information, is precisely the data that traverses enterprise network infrastructure today and will retain strategic value for decades. An adversary conducting HNDL operations against an organization's SDN control plane communications or container orchestration API traffic is collecting material that may be decryptable within the operational lifetime of the systems those communications govern.

3.3. Quantum Vulnerabilities Specific to SDN-Container Architectures

SDN and container architectures introduce quantum-specific vulnerabilities that extend beyond the general cryptographic disruption. First, SDN's centralized control plane creates a high-value cryptographic concentration point. As the evidence suggests, the centralized control plane is simultaneously SDN's primary security advantage, enabling real-time visibility and dynamic policy enforcement, and its primary attack surface: a compromised controller yields adversarial control over the entire network fabric. Under quantum threat, the TLS sessions protecting controller-to-switch southbound communications, north-bound application programming interface (API) traffic between the controller and management applications, and east-west inter-controller communications in distributed SDN deployments all rely on public-key cryptography vulnerable to Shor's algorithm. A CRQC-equipped adversary that retroactively decrypts historical controller traffic captures not just data in transit but a historical record of network topology, policy enforcement decisions, and administrative credentials.

Second, container orchestration platforms, particularly Kubernetes, used by several participants in the study, rely extensively on TLS-protected communications between the API server, etc. (the distributed key-value store containing all cluster state), kubelet agents, and container registries. Container image signing, which the participants identified as a security best practice for ensuring container provenance, relies on digital signatures that are computationally breakable under quantum attack. An adversary capable of forging container image signatures could inject malicious workloads into orchestration pipelines without detection.

Third, the ephemeral and dynamic nature of containerized environments, their core operational advantage, creates a quantum key management challenge that static architectures do not face. Traditional enterprise environments provision cryptographic keys for relatively stable, long-lived server instances. Container environments provision, scale, and terminate workloads continuously, requiring cryptographic key issuance, rotation, and revocation at correspondingly high velocity. Post-quantum key encapsulation mechanisms (KEMs) introduce computational overhead relative to classical alternatives; the implications of this overhead for high-velocity container provisioning have not been systematically investigated.

3.4. The SDN-Container Quantum Advantage

The same architectural properties that make SDN-container integration superior to traditional security architectures for classical threats, centralized programmability, dynamic policy enforcement, micro-segmentation, and automated policy replication, also provide structural advantages for quantum-era security migration that deserve explicit recognition. The study's participants uniformly reported that SDN's centralized control plane enables consistent security policy enforcement across heterogeneous infrastructure with a precision unachievable through device-by-device configuration. This property is directly applicable to PQC migration: a centralized SDN controller can enforce cryptographic algorithm policies across the entire network fabric, detect non-PQC-compliant communications through deep packet inspection or traffic metadata analysis, and dynamically reroute or terminate connections using deprecated algorithms, functions that require manual intervention or agent-based enforcement in traditional architectures.

Container orchestration platforms similarly provide a deployment abstraction that simplifies PQC library rollout: updating the cryptographic library in a base container image propagates to all workloads derived from that image through standard container lifecycle management, enabling fleet-wide cryptographic updates without the server-by-server patching processes that characterize traditional infrastructure. P8's observation in that "through container scaling, we can implement security policy on a single container and replicate it across all deployed assets within similar containers" describes precisely the mechanism through which PQC enforcement can be systematically distributed across an organization's entire containerized application portfolio.

3.5. The Quantum-Integrated SDN-Container Security Architecture

QISCA is a five-domain conceptual framework for achieving quantum-resilient network security through systematic integration of post-quantum cryptography, quantum key distribution, and quantum-enhanced threat detection into existing SDN-container architectures. Each domain corresponds directly to one of the five empirical themes identified in the study, extending the practitioner-grounded findings into the quantum security context. This one-to-one correspondence between empirical theme and conceptual domain ensures that the framework's architecture is dictated by practitioner-validated findings rather than imposed upon them, preserving a transparent line of derivation from observed operational reality to quantum security prescription. The result is a framework that treats post-quantum migration not as an isolated cryptographic replacement exercise but as a coordinated architectural transformation spanning policy enforcement, key distribution, threat detection, human factors, and migration strategy. Table 1 presents the QISCA domain structure.

QISCA Domain	Empirical Origin (Troublefield, 2025)	Quantum Security Extension	Primary PQC Standard
Domain 1: Cryptographic Agility & Policy Enforcement	Theme 1: Strategies for enhancing network security (micro-segmentation, dynamic policy enforcement)	SDN-enforced PQC algorithm policy; quantum-safe TLS migration; cryptographic non-compliance detection	NIST FIPS 203 (ML-KEM / Kyber); FIPS 204 (ML-DSA / Di lithium)
Domain 2: Quantum Key Distribution Integration	Theme 2: Implementation benefits, challenges, and adoption (granular access control, interoperability)	QKD-provisioned symmetric keys distributed via SDN control plane; container-native key management APIs	ETSI GS QKD 004; BB84 and E91 protocols
Domain 3: Quantum-Enhanced Threat Detection	Theme 4: Security monitoring, threat detection, and compliance (centralized control, real-time visibility)	Quantum machine learning anomaly detection; quantum-accelerated traffic analysis; harvest-now-decrypt-later detection	NIST IR 8413; quantum sensing integration
Domain 4: Operational Resilience & Human Factors	Theme 3: Operational management and expertise (skill requirements, resource investment)	Quantum-era operator training; PQC cognitive load management; quantum readiness assessment frameworks	CISA PQC Migration Guidance (2024)
Domain 5: Comparative Architecture & Migration Strategy	Theme 5: Comparative analysis of traditional vs. integrated security architectures	Quantum-classical hybrid security posture; phased PQC migration roadmap; SDN-container vs. traditional migration comparison	NSA CNSA 2.0 Suite (2022)
Note: PQC = post-quantum cryptography; QKD = quantum key distribution; ML-KEM = Module-Lattice Key Encapsulation Mechanism; ML-DSA = Module-Lattice Digital Signature Algorithm; CNSA = Commercial National Security Algorithm.			

Table 1: QISCA Framework: Five Domains, Empirical Origins, and Quantum Extensions

4. Domain 1: Cryptographic Agility and Policy Enforcement

4.1. Cryptographic Agility as an SDN Control Plane Function:

The most direct application of the empirical findings to the quantum security context is the use of SDN's centralized control plane to enforce cryptographic algorithm policies across the entire network fabric. Participants described SDN's policy automation as transformative: P2 characterized it as "a tireless enforcer that ensures every container follows the established rules," and P10 described the capability to create policies that "automatically adjust based on container behavior." Applied to cryptographic governance, this enforcement capability supports what the cryptographic community terms cryptographic agility: the ability to rapidly deploy, enforce, and update cryptographic algorithm selections across an entire infrastructure without manual device-by-device intervention.

Cryptographic agility is the organizational property most critical to successful PQC migration [7,9]. explicitly recommended that organizations design systems for cryptographic agility as the primary preparedness measure, given the possibility that currently standardized PQC algorithms may require future replacement as cryptanalytic research matures. An SDN controller configured to enforce cryptographic policy can detect TLS handshakes negotiating deprecated algorithms through traffic metadata analysis, reroute such connections to policy enforcement proxies, and log non-compliant communications for remediation, functions that require distributed agent deployment in traditional architectures but are centrally executable in SDN environments.

4.2. Container-Native Post-Quantum Cryptographic Enforcement: Container orchestration platforms provide a complementary enforcement layer at the application level. The base container image update mechanism, which participant P8 identified as enabling rapid, consistent policy replication, provides an operationally feasible path for fleet-wide PQC library deployment. Organizations can update the cryptographic libraries in their base images to NIST-standardized PQC implementations (e.g., liboqs, the Open Quantum Safe project's library), rebuild application container images from updated bases, and deploy the updated images through standard rolling update procedures, without application code modification in cases where applications use the host TLS library rather than embedded cryptographic implementations.

Kubernetes admission controllers provide a complementary enforcement mechanism at the orchestration layer: admission webhooks can reject container deployments that declare dependencies on deprecated cryptographic libraries or that fail cryptographic compliance attestation checks embedded in container image metadata. This approach operationalizes PQC enforcement within existing DevSecOps pipeline practices rather than requiring parallel cryptographic governance infrastructure.

4.3. Quantum-Safe SDN Southbound Communication: The TLS sessions protecting SDN's southbound communications, between the controller and network devices via OpenFlow or alternative protocols, represent a high-priority PQC migration target given their role in governing the entire network's security posture. A compromise of controller-to-switch communications enables adversarial network fabric manipulation at a scale that individual application-layer compromises cannot achieve. NIST's ML-KEM (FIPS 203) provides the key encapsulation mechanism appropriate for TLS 1.3 key exchange in southbound channels; ML-DSA (FIPS 204) provides the digital signature algorithm appropriate for controller authentication. Migration of SDN southbound TLS to PQC algorithms should be treated as a critical infrastructure dependency requiring priority treatment in organizational PQC migration roadmaps.

5. Domain 2: Quantum Key Distribution Integration

5.1. QKD as a Complement to Post-Quantum Cryptography: QKD provides information-theoretically secure key exchange through the physical properties of quantum mechanics: the BB84 protocol and its successors exploit the no-cloning theorem and measurement disturbance to enable two parties to establish a shared secret key with unconditional security, where any eavesdropping attempt introduces detectable disturbance [8]. QKD is distinct from PQC: PQC algorithms are classical algorithms that are computationally hard for quantum computers to break, while QKD provides security guaranteed by the laws of quantum physics rather than computational assumptions. The two approaches are complementary rather than competing: QKD addresses key exchange; PQC addresses authentication and integrity in addition to key exchange.

For SDN-container environments, QKD's most compelling application is the provisioning of symmetric session keys for the highest-sensitivity traffic channels, particularly SDN controller-to-controller communications in distributed deployments, northbound API traffic between controllers and management systems, and inter-datacenter container cluster communications. The SDN control plane's centralized architecture is well-suited to QKD integration: a QKD network interface can provision symmetric keys to the SDN controller, which distributes them to relevant network segments through the standard policy enforcement mechanism that the participants described as SDN's core security value proposition.

5.2. Container-Native Key Management for QKD-Provisioned Keys: The integration of QKD-provisioned keys into containerized application environments requires a key management architecture compatible with container lifecycle dynamics. The participants identified container ephemerality, the rapid provisioning, scaling, and termination of container instances, as both an operational advantage and a governance challenge. A QKD-native key management system for container environments must address: (a) key provisioning at container startup that does not introduce prohibitive latency in high-velocity orchestration environments; (b) key rotation synchronized with container lifecycle events; (c) key revocation for terminated containers; and (d) key inheritance policies for container replicas and blue-green deployment scenarios.

The Kubernetes Secrets management system, when configured with external secret store integration (e.g., HashiCorp Vault with a QKD provider backend), provides an architectural foundation for QKD key distribution to containerized workloads. A QKD provider plugin for the Kubernetes Key Management Service (KMS) API would enable transparent QKD key provisioning through the standard Kubernetes secrets interface, allowing application workloads to consume quantum-safe keys without modification. This approach extends the operational simplicity that the participants cited as a primary benefit of container-native security tooling to the quantum key management domain.

5.3. SDN-Mediated QKD Network Routing: The programmability of SDN control planes enables dynamic optimization of QKD network utilization, a capability not available in traditional static network architectures. QKD networks face practical constraints including distance limitations (approximately 100 km without trusted repeaters for fiber-based QKD), throughput constraints (key generation rates orders of magnitude lower than classical key exchange), and vulnerability to physical-layer attacks on the quantum channel. SDN control planes can route traffic to maximize use of QKD-provisioned keys for highest-sensitivity communications while directing lower-sensitivity traffic to PQC-protected channels, dynamically rebalancing based on real-time QKD key pool availability. This dynamic allocation capability, directly analogous to the SDN traffic engineering functions the participants described for classical security policy, transforms QKD from a point-to-point technology into a network-wide resource managed through programmable policy.

6. Domain 3: Quantum-Enhanced Threat Detection

6.1. Quantum Machine Learning for Behavioral Anomaly Detection: The study found that SDN's centralized control plane enables real-time network visibility that participants uniformly described as transformative for threat detection. P4 characterized it as "a bird's-eye view of the entire network," while P9 reported that implementation enabled threat response within minutes. This centralized visibility creates an ideal data collection substrate for quantum machine learning (QML) anomaly detection: the complete network flow data available to the SDN controller, combined with container runtime metrics from the orchestration platform, provides a comprehensive behavioral baseline from which deviations indicative of unauthorized access, lateral movement, or data exfiltration can be detected.

Quantum machine learning algorithms, including quantum support vector machines, quantum neural networks, and quantum principal component analysis, offer theoretical speedups over classical counterparts for specific tasks [12]. For network anomaly detection, quantum-enhanced clustering algorithms may enable more rapid identification of novel attack patterns in high-dimensional network flow datasets than classical machine learning achieves, particularly for the detection of sophisticated low-and-slow attacks that classical threshold-based detection systems routinely miss. The practical realization of QML advantages for network security remains an active research frontier [11,13], but the centralized data collection enabled by SDN-container architectures provides the data substrate that makes QML deployment operationally feasible as quantum processors mature.

6.2. Harvest-Now-Decrypt-Later Detection: A specifically quantum-era threat detection requirement that SDN-container architectures are positioned to address is the identification of HNDL operations: systematic collection of encrypted traffic for future decryption once CRQCs become available. HNDL attacks manifest as anomalous large-scale traffic capture operations, potentially indistinguishable from legitimate network monitoring without behavioral baseline analysis. SDN's centralized flow

visibility enables detection of exfiltration patterns consistent with bulk encrypted traffic harvesting: unusually large outbound data transfers, systematic copying of encrypted communications across network segments, or anomalous access to SDN controller logs that would reveal network topology for future exploitation.

Container-level network monitoring, enabled by SDN micro-segmentation and container network interface (CNI) plugin telemetry, provides a more granular detection surface than network-level monitoring alone, enabling identification of container workloads engaged in unusual data access patterns consistent with HNDL operations. The combination of SDN flow analysis and container runtime security monitoring creates a multi-layer HNDL detection capability that neither technology provides independently.

6.3. Cryptographic Inventory and Vulnerability Assessment:

A prerequisite for PQC migration is comprehensive cryptographic inventory: identification of all cryptographic algorithm usages across the network environment, including embedded cryptographic implementations in application code, operating system TLS libraries, hardware security modules, and protocol-layer cryptography. SDN-container environments facilitate cryptographic inventory through: (a) SDN deep packet inspection to identify cryptographic protocol usage in network traffic; (b) container image analysis to identify cryptographic library dependencies before deployment; and (c) runtime container network monitoring to detect cryptographic negotiation patterns in active workloads. This combination of static and dynamic cryptographic analysis, centrally orchestrated through the SDN control plane and container admission control, enables organizations to maintain current cryptographic inventories at the scale and dynamism that container environments demand, a capability unavailable in traditional architectures that require agent-based scanning of individual servers.

7. Domain 4: Operational Resilience and Human Factors in Quantum-Era Security

7.1. Quantum-Era Cognitive Load and Operator Challenges:

Findings in the study identified training deficits and skill gaps as the primary proximate drivers of misconfiguration risk in SDN-container environments, a finding the study connected to the broader literature attributing 89% of breaches in these environments to administrative error [21,22]. The quantum security transition amplifies these human factors challenges in two respects. First, PQC migration introduces a new domain of technical complexity, cryptographic algorithm selection, parameter tuning, hybrid classical-PQC deployment strategies, and QKD infrastructure management, that requires expertise currently scarce in cybersecurity professional communities. Second, the coexistence of classical, PQC, and QKD-provisioned cryptographic systems during the transition period creates an environment of exceptional complexity in which operator errors are correspondingly more consequential.

The cognitive load implications of quantum-era security management extend the pattern found for SDN-container integration: complexity that exceeds operator training produces misconfiguration, and misconfiguration produces the security vulnerabilities the technology was deployed to prevent. For quantum security, the consequence of misconfiguration is potentially more severe: a misconfigured PQC deployment that silently falls back to classical cryptography provides false assurance of quantum resistance while remaining vulnerable to HNDL attack.

7.2. TAM and UTAUT Applied to Quantum Security Adoption:

The Technology Acceptance Model and UTAUT frameworks that) applied to SDN-container adoption provide directly applicable lenses for analyzing quantum security adoption dynamics [14,15]. TAM predicts that perceived usefulness and perceived ease of use are the primary determinants of adoption intentions. For quantum security adoption, the perceived usefulness challenge is significant: unlike SDN-container integration, where participants could point to concrete, immediately measurable security improvements (data leaks eliminated, security check time reduced 88%), PQC migration's benefits are primarily defensive against a threat that has not yet materialized for most organizations. Loss aversion and temporal discounting biases predict that organizations will systematically underinvest in protection against probabilistic future threats relative to their objective expected loss, particularly when the protective investment requires significant immediate cost [16].

UTAUT's facilitating conditions construct is equally relevant: quantum security adoption requires organizational capabilities, cryptographic expertise, quantum-aware security tooling, QKD-compatible network infrastructure, that most organizations do not currently possess. Findings in the study show that facilitating conditions were the primary differentiator between organizations that achieved sophisticated SDN-container implementations and those that achieved only basic deployment; the same dynamic will govern quantum security adoption, with organizations possessing mature security programs, dedicated cryptographic expertise, and executive-level security investment achieving substantive PQC migration while resource-constrained organizations remain exposed.

7.3. Quantum Readiness Assessment Framework:

Drawing on the organizational readiness assessment approach advocated for SDN-container implementation, QISCA proposes a QRA framework structured around five dimensions: (a) cryptographic inventory completeness, the degree to which the organization has catalogued all cryptographic algorithm usages across its environment; (b) PQC migration capability, the availability of technical expertise, tooling, and development capacity to execute cryptographic library updates and protocol migrations; (c) QKD infrastructure readiness, the assessment of network infrastructure proximity to QKD network access points and the feasibility of QKD integration for highest-priority communications; (d) operator quantum literacy, the degree to which security operations staff possess sufficient understanding of quantum cryptographic

concepts to make informed operational decisions; and (e) governance maturity, the existence of organizational policies, executive accountability, and budget allocation for quantum security transition. Table 2 presents the QRA scoring rubric.

QRA Dimension	Level 1 (Unaware)	Level 2 (Aware)	Level 3 (Prepared)	Level 4 (Resilient)
1. Cryptographic Inventory	No systematic inventory exists	Ad hoc inventory in high-priority systems only	Automated scanning in SDN/container environments; partial coverage	Complete real-time inventory via SDN and container CI/CD integration
2. PQC Migration Capability	No PQC awareness or tooling	Awareness only; no migration activity	Pilot PQC deployment in non-production environments	Active PQC migration with defined completion timeline
3. QKD Infrastructure Readiness	No assessment conducted	Feasibility assessment completed	QKD integration plan developed	QKD-provisioned keys active in highest-priority channels
4. Operator Quantum Literacy	No quantum security training	Executive awareness briefings only	Technical staff trained in PQC fundamentals	Dedicated quantum security competency within security team
5. Governance Maturity	No quantum security policy	Quantum security referenced in risk register	Quantum security policy drafted; budget allocated	Executive accountability assigned; migration milestones tracked
Note. Organizations targeting Level 3 across all dimensions before 2027 are positioned to complete substantive PQC migration within CISA's recommended timeline (CISA, 2024).				

Table 2: Quantum Readiness Assessment Framework Scoring Rubric

8. Domain 5: Comparative Architecture and Migration Strategy

8.1. SDN-Container vs. Traditional Architecture Migration Comparison: Theme 5 showed that cybersecurity professionals consistently assessed SDN-container integration as superior to traditional security architectures in agility, control granularity, and threat containment capability. This comparative advantage extends directly to PQC migration: the architectural properties that make SDN-container environments superior for classical security, centralized policy enforcement, automated policy replication, container image-based software distribution, also make them faster, more consistent, and more verifiable migration targets for PQC deployment.

Table 3 presents a structured comparison of PQC migration complexity across SDN-container, traditional perimeter, and hybrid architectures across five critical migration dimensions.

Migration Dimension	SDN-Container Architecture	Traditional Perimeter Architecture	Hybrid Architecture
Cryptographic Policy Enforcement	Centralized via SDN controller; container admission control enables pre-deployment enforcement	Device-by-device configuration; agent-based enforcement required	Partial centralization; enforcement gaps at perimeter edges
Cryptographic Inventory Coverage	Automated via SDN DPI and container image analysis; near-complete in containerized workloads	Manual scanning; agent deployment required; high coverage gaps	Automated for SDN/container components; manual for legacy systems
PQC Library Distribution	Container image rebuild and rolling update; fleet-wide in hours	Server-by-server patching; fleet-wide in weeks to months	Mixed; fast for containerized components, slow for legacy
Compliance Verification	Real-time via SDN flow analysis; non-compliant traffic detected immediately	Periodic scanning; detection latency measured in days	Real-time for SDN/container segments; periodic for legacy
HNDL Exposure Reduction	High: SDN enables rapid protocol migration; container micro-segmentation limits blast radius of continued classical cryptography	Low: protocol migration requires manual intervention; broad exposure until completion	Medium: SDN/container components protected; legacy exposure continues
Note: DPI = deep packet inspection; HNDL = harvest-now-decrypt-later. Migration timeline estimates based on NIST (2024) implementation guidance and comparative infrastructure change management literature.			

Table 3: Post-Quantum Cryptographic Migration Complexity by Architecture Type

8.2. Phased QISCA Migration Roadmap: Drawing on the empirical finding that phased, pilot-first implementation was the most consistent success factor across SDN-container deployments, with P10 recommending "starting with small pilot projects, focusing on specific use cases, and gradually expanding deployment", QISCA proposes a four-phase migration roadmap for organizations implementing the framework. Phase 1 (Inventory and Assessment, 0–6 months) encompasses cryptographic inventory

through SDN deep packet inspection and container image analysis, completion of the QRA, identification of HNDL priority data and the cryptographic channels through which it transits, and establishment of the executive governance structure for quantum security transition. Phase 2 (Pilot PQC Deployment, 6–18 months) encompasses PQC library integration in base container images for non-production workloads, hybrid TLS 1.3 with PQC key encapsulation for SDN control plane communications in test environments, establishment of cryptographic compliance monitoring through SDN flow analysis, and operator training for quantum security fundamentals across the security operations team. Phase 3 (Production Migration, 18–36 months) encompasses production rollout of PQC-enabled container images through rolling updates, migration of SDN southbound communications to PQC-protected protocols, activation of quantum-enhanced anomaly detection in the security operations center, and QKD integration for highest-priority communications channels where infrastructure is available. Phase 4 (Operational Resilience, 36+ months) encompasses continuous cryptographic monitoring and agility maintenance, quantum literacy development across the broader IT and security organization, participation in industry quantum security information-sharing programs, and preparation for potential second-generation PQC algorithm transitions as cryptanalytic research matures.

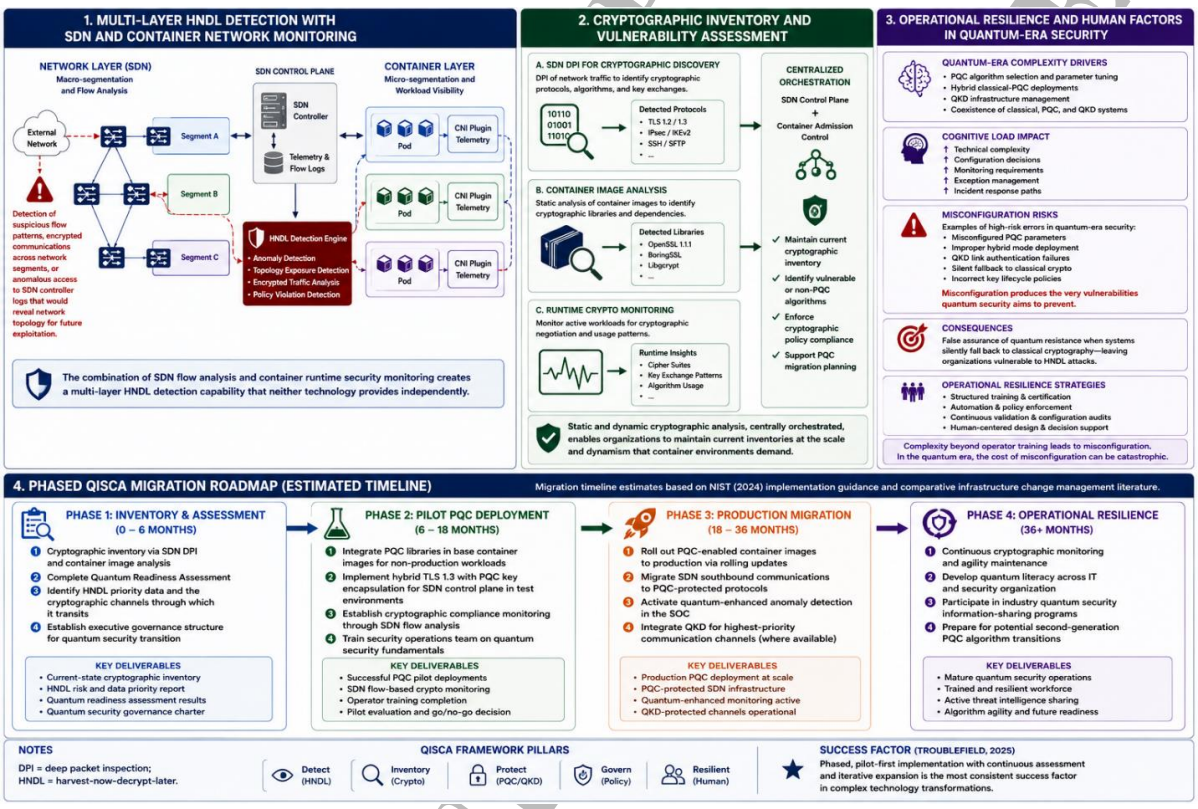

Figure 1: Quantum-Integrated SDN-Container Security Architecture Framework

Figure 1 presents the QISCA, a comprehensive framework designed to help organizations secure SDN and containerized environments against emerging quantum-computing threats. The framework integrates four complementary domains: multi-layer HNDL detection, cryptographic inventory and vulnerability assessment, operational resilience and human factors, and a phased migration roadmap for PQC adoption. Together, these domains provide a structured approach for identifying quantum-era risks, managing cryptographic transition, and sustaining long-term organizational resilience.

- **Domain 1:** Multi-Layer HNDL Detection with SDN and Container Network Monitoring, the first section illustrates how organizations can detect Harvest-Now-Decrypt-Later (HNDL) activities through the combined use of SDN flow monitoring and container-level telemetry. HNDL attacks occur when adversaries collect encrypted data today with the intention of decrypting it later using future quantum computing capabilities. Traditional network monitoring often lacks the visibility needed to identify these activities because the encrypted content itself remains unreadable.

- The framework addresses this challenge through two complementary monitoring layers. At the network layer, SDN flow analysis identifies unusual communication patterns, anomalous access to SDN controller logs, encrypted traffic anomalies, and suspicious east-west communications across network segments. At the container layer, micro-segmentation

and Container Network Interface (CNI) telemetry provide visibility into individual workloads, enabling detection of unusual data access behavior and cryptographic communication patterns. By combining SDN telemetry with container runtime monitoring, the framework creates a multi-layer detection capability that is significantly more effective than either technology operating independently.

- **Domain 2:** Cryptographic Inventory and Vulnerability Assessment, the second section focuses on maintaining comprehensive visibility into cryptographic assets throughout the enterprise. A fundamental requirement of quantum-security readiness is understanding where cryptography is used, which algorithms are deployed, and which systems remain vulnerable to future quantum attacks.

- The framework employs three complementary discovery mechanisms. First, Deep Packet Inspection (DPI) identifies cryptographic protocols and key-exchange mechanisms actively operating within network traffic. Second, container image analysis examines deployed workloads to identify embedded cryptographic libraries and dependencies before they enter production. Third, runtime cryptographic monitoring continuously evaluates active workloads to detect cryptographic negotiation patterns, cipher suite selection, certificate validation activity, and PQC implementation status.

- These capabilities are coordinated through centralized SDN control-plane orchestration and container admission controls, allowing organizations to maintain continuously updated cryptographic inventories at the scale and speed required by modern cloud-native environments. This capability is particularly important because traditional agent-based scanning approaches often fail to keep pace with the dynamic nature of containerized infrastructures.

- **Domain 3:** Operational Resilience and Human Factors in Quantum-Era Security, the third section highlights the human dimensions of quantum-security adoption. While technological solutions are essential, research consistently demonstrates that operator error and configuration mistakes remain among the most significant sources of cybersecurity risk.

- The figure identifies several complexity drivers introduced by the quantum transition, including PQC algorithm selection, parameter tuning, hybrid classical-PQC deployments, QKD management, and coexistence of classical and quantum-resistant cryptographic systems. These factors increase cognitive workload for administrators and security practitioners, elevating the risk of misconfiguration.

- The framework illustrates how cognitive overload can result in implementation errors such as incorrect PQC parameter selection, improper hybrid deployment strategies, QKD authentication failures, cryptographic fallback to vulnerable classical algorithms, and flawed key lifecycle management. Such errors may create a false sense of security while leaving organizations vulnerable to HNDL attacks. To address these challenges, the framework recommends structured training programs, automation, continuous validation, policy enforcement, and human-centered system design principles.

- **Domain 4:** Phased QISCA Migration Roadmap, the fourth section presents a practical four-phase roadmap for transitioning toward quantum-resistant security architectures. The roadmap follows a phased implementation approach derived from successful SDN-container deployment practices and quantum-security migration guidance.

- **Phase 1:** Inventory and Assessment (0–6 Months), this phase focuses on establishing organizational awareness and governance. Activities include cryptographic inventory development through DPI and container image analysis, completion of a QRA, identification of HNDL-priority data assets, and creation of executive governance structures to oversee quantum-security initiatives. The primary outcome is a clear understanding of the organization's cryptographic exposure and readiness posture.

- **Phase 2:** Pilot PQC Deployment (6–18 Months), the second phase introduces PQC technologies in controlled environments. Organizations begin integrating PQC libraries into non-production container images, implementing hybrid TLS 1.3 with PQC key encapsulation for SDN control-plane communications, establishing cryptographic compliance monitoring, and conducting workforce training. This phase reduces implementation risk while allowing operational teams to gain experience with quantum-resistant technologies.

- **Phase 3:** Production Migration (18–36 Months), the third phase expands quantum-resistant capabilities into production environments. Activities include rolling deployment of PQC-enabled container images, migration of SDN communications to PQC-protected protocols, activation of quantum-enhanced anomaly detection capabilities within Security Operations Centers (SOCs), and implementation of QKD for the highest-priority communications channels where infrastructure permits.

- **Phase 4:** Operational Resilience (36+ Months), the final phase focuses on long-term sustainability and cryptographic agility. Organizations maintain continuous cryptographic monitoring, expand quantum literacy across IT and security teams, participate in quantum-security information-sharing communities, and prepare for future PQC algorithm transitions as cryptographic research evolves. The objective is to establish a resilient security posture capable of adapting to future advances in quantum computing and cryptanalysis.

Notes and Framework Significance

The figure notes that:

- **DPI = Deep Packet Inspection**
- **HNDL = Harvest-Now-Decrypt-Later**

Migration timeline estimates are based on NIST (2024) post-quantum implementation guidance and comparative infrastructure change-management research.

Overall, the QISCA framework demonstrates that successful quantum-era security requires more than simply replacing cryptographic algorithms. Effective protection emerges from the integration of advanced threat detection, continuous cryptographic visibility, organizational governance, workforce readiness, and phased operational transformation. The framework, therefore, provides a comprehensive blueprint for organizations seeking to transition from classical cybersecurity architectures to resilient quantum-ready environments.

8.3. Theoretical Grounding: TAM and UTAUT in the Quantum Security Transition

Davis's (1989) Technology Acceptance Model and Venkatesh et al.'s (2003) Unified Theory of Acceptance and Use of Technology, which was applied to explain SDN-container adoption dynamics, provide directly transferable analytical lenses for understanding the structurally distinct challenges of quantum security adoption. The quantum security transition, however, inverts several of the conditions that drove SDN-container adoption: where the latter offered immediately verifiable benefits, the former demands investment against a threat whose consequences are delayed, probabilistic, and unobservable until it is too late to act. This section applies three core constructs, perceived usefulness, facilitating conditions, and social influence, to explain why conventional adoption logic systematically undervalues post-quantum migration, why the expertise gap constitutes a structural rather than incidental barrier, and how regulatory mandates function to reframe adoption from optional investment to institutional expectation. Together, these theoretical lenses illuminate both the barriers to quantum security adoption and the interventions, reframed value propositions, ecosystem-level facilitating conditions, and regulatory social influence, through which those barriers may be overcome.

8.4. Perceived Usefulness and the Quantum Threat Credibility Gap

Davis's (1989) TAM identifies perceived usefulness as the primary driver of technology adoption intentions. Findings in the study show that perceived usefulness in SDN-container adoption was driven by immediately verifiable, concrete security improvements, elimination of data leaks, reduction of security administration time, and penetration testing validation of containment effectiveness. These proximate, observable benefits created strong adoption motivation aligned with TAM predictions. Quantum security presents a fundamentally different perceived usefulness structure: its benefits are protection against a threat that has not yet materialized for the adopting organization, with benefits that cannot be observed or measured in the absence of the quantum threat itself.

This structure maps onto what Kunreuther and Michel-Kerjan (2010) termed the low probability, high consequence decision problem: individuals and organizations systematically underinvest in protection against rare but catastrophic events, particularly when the protective investment is immediate and certain while the protected-against consequence is delayed and probabilistic. For quantum security adoption, this implies that traditional ROI-based decision frameworks will systematically undervalue PQC migration, favoring observable near-term security improvements over probabilistic future-threat protection. TAM-based adoption interventions for quantum security must therefore reframe perceived usefulness in terms that overcome temporal discounting: the operational cost of post-quantum migration increases exponentially as CRQC availability approaches (due to the growing archive of vulnerable-ciphertext traffic available for decryption), the HNDL threat is active now even though the decryption threat is future, and regulatory and contracting requirements for PQC compliance are emerging that create immediate business consequences for non-migration.

8.5. Facilitating Conditions and the Quantum Expertise Gap

UTAUT's facilitating conditions construct, the perceived availability of organizational and technical resources supporting adoption, is directly explanatory of the primary structural barrier to quantum security adoption in SME environments. Findings in the study show that facilitating conditions were the primary differentiator between sophisticated and basic SDN-container implementations: organizations with dedicated security expertise, senior leadership commitment, and adequate training resources achieved materially better outcomes than those without. For quantum security, the facilitating conditions gap is more severe: quantum cryptographic expertise is not merely scarce among SME cybersecurity teams, it is scarce in the broader cybersecurity workforce globally.

The CISA (2024) PQC migration guidance acknowledges this expertise gap, recommending that organizations without internal quantum cryptographic expertise engage with managed security service providers and NIST-certified cryptographic product vendors rather than attempting independent migration. Venkatesh et al.'s (2003) UTAUT prediction that organizational support structures co-determine adoption outcomes alongside individual motivation has direct implications for quantum security policy: government and industry bodies that provide accessible cryptographic migration tooling, certified vendor ecosystems, and workforce development programs are not merely providing convenience, they are constituting the facilitating conditions without which adoption is structurally infeasible for a substantial segment of the economy.

8.6. Social Influence and Regulatory Drivers

UTAUT's social influence construct, the degree to which individuals perceive that institutional referents and peer organizations believe they should use a focal technology, provides a framework for understanding the role of regulatory mandates in quantum security adoption. NSA's (2022) Commercial National Security Algorithm

Suite 2.0 (CNSA 2.0) establishes PQC algorithm requirements for national security systems with defined transition timelines; CISA's (2024) guidance extends similar expectations to critical infrastructure operators; the Office of Management and Budget (OMB) has issued guidance directing federal agencies to begin PQC migration inventories. These regulatory signals function as social influence mechanisms that convert quantum security adoption from an optional investment to an institutional expectation, a dynamic that UTAUT predicts will accelerate adoption among organizations whose decision-making is sensitive to institutional norms, including federal contractors, regulated industries, and defense industrial base participants.

The participant sample included healthcare organizations driven by HIPAA compliance requirements and DoD contractors driven by CMMC standards, populations in which regulatory social influence was directly observable as an adoption accelerant. The same regulatory dynamics will govern quantum security adoption in these sectors, with the additional urgency created by the NSA's explicit notification that national security systems relying on classical public-key cryptography must complete CNSA 2.0 transitions by 2030.

8.7. Governance and Implementation Considerations for QISCA

Translating QISCA from a conceptual framework into operational practice requires deliberate attention to the organizational, supply chain, and interoperability dimensions through which quantum security migration succeeds or fails. The empirical evidence demonstrates that SDN-container integration, technical capability alone is insufficient without sustained executive commitment, vendor partnership, and the operational accommodation of transitional complexity, conditions that apply with greater force to a multi-year post-quantum cryptographic migration spanning the full software, hardware, and managed-service supply chain. This section addresses three interdependent implementation considerations: the governance structures needed to sustain accountability across the migration timeline, the vendor and supply chain dependencies that extend migration beyond organizational boundaries, and the hybrid classical-PQC operation that interoperability with non-migrated endpoints makes operationally inevitable, before setting out a five-domain research agenda for the empirical validation QISCA's claims require. Because QISCA is derived from qualitative findings and the current quantum security literature rather than from validated deployment outcomes, the concluding research agenda identifies the most consequential empirical questions, spanning migration performance, operator cognitive load, QKD integration feasibility, adoption dynamics, and sector-specific implementation, whose investigation would advance the framework from proposed architecture to evidence-based practice.

8.8. Organizational Governance Structure

QISCA implementation requires governance structures that integrate quantum security decision-making into existing cybersecurity program frameworks. The findings show that leadership commitment was a critical success factor for SDN-container implementation, with one participant noting that an executive seeking an exception from verification requirements on the first day of implementation effectively undermined the entire program. For quantum security, the governance stakes are higher: PQC migration requires sustained multi-year investment, cross-functional coordination between security, IT, development, and procurement organizations, and executive accountability for migration timeline adherence.

The QISCA governance model proposes three organizational components. First, a Quantum Security Steering Committee at the executive level, chaired by the CISO or equivalent, with membership from IT, legal, procurement, and business unit leadership, responsible for migration roadmap approval, resource allocation, and quarterly progress review. Second, a Quantum Security Technical Working Group composed of cryptographic and network security specialists is responsible for technical migration planning, vendor evaluation, tooling selection, and operator training program design. Third, a Cryptographic Compliance Monitoring function embedded within the security operations center, responsible for continuous cryptographic inventory maintenance through SDN and container analytics, non-compliance detection, and remediation coordination.

8.9. Vendor and Supply Chain Considerations

Post-quantum cryptographic migration extends beyond organizational network infrastructure to encompass the full supply chain of software, hardware, and managed services. Container images sourced from third-party registries may include cryptographic dependencies using classical algorithms; network devices in the SDN data plane may implement TLS using classical libraries that require firmware updates for PQC compatibility; cloud service providers offering container orchestration services must provide PQC-compatible control plane APIs before container workloads running on those platforms can achieve end-to-end PQC protection. The participants described vendor engagement as a necessary component of SDN-container integration, P3 resolved compatibility challenges "through software updates, configuration refinements, and continuous testing" in close collaboration with vendors, and the same vendor partnership dynamic applies at greater scale to PQC migration.

The Open Quantum Safe project (oqs-project.org) provides a practical starting point for container-native PQC deployment, offering liboqs, an open-source C library implementing NIST-standardized PQC algorithms, and OQS-OpenSSL, a fork of OpenSSL supporting PQC algorithms in TLS. Organizations building container base images from OQS-OpenSSL enable PQC-compatible TLS across all containerized workloads that use the OpenSSL library for network communications, with minimal application-level modification. The Kubernetes SIG-Security community has documented PQC migration considerations for "distributed /etc directory," or etcd, the Kubernetes API server, and kubelet communications, providing a roadmap for container orchestration platform PQC migration that organizations can adapt

to their specific deployment contexts.

8.10. Interoperability and Hybrid Operation

The transition to post-quantum cryptography cannot occur instantaneously across an entire enterprise infrastructure; a period of hybrid classical-PQC operation is operationally inevitable. During this period, SDN-container environments must maintain interoperability with both PQC-capable and classical-only endpoints, including legacy on-premises systems, partner organization networks, and internet endpoints that have not yet completed PQC migration. The evidence show that interoperability challenges were among the most technically demanding aspects of SDN-container integration, with P9 specifically citing compatibility challenges between cloud platforms as a persistent operational complication.

For quantum security, hybrid TLS 1.3 key exchange, in which both a classical ECDH key exchange and a PQC KEM are performed, with the session key derived from both, provides interoperability with classical-only endpoints while protecting against HNDL attacks on traffic to PQC-capable endpoints. IETF RFC 8784 and subsequent drafts establish the hybrid key exchange framework for TLS. SDN policy enforcement can direct traffic to PQC-capable paths when available and to hybrid paths for traffic to classical-only destinations, with logging of all classical-only connections for remediation prioritization. This SDN-mediated traffic steering capability enables organizations to maximize quantum security coverage across their communication fabric while maintaining operational continuity with non-PQC endpoints, a direct application of the dynamic traffic management capabilities that the participants described as SDN's core operational advantage.

8.11. Research Agenda for Empirical Validation of QISCA

QISCA is a conceptual framework developed from qualitative empirical findings and the current quantum security literature; its claims require empirical validation across diverse organizational contexts. The following five-domain research agenda identifies the most consequential empirical questions for advancing quantum-integrated SDN-container security from framework to validated practice. Each domain is framed around falsifiable propositions with specified measurable outcomes, so that the framework's central claims can be tested rather than assumed and confirmed or refuted on the basis of evidence. Collectively, these research domains chart a pathway from conceptual architecture to validated practice, prioritizing the questions whose answers would most directly determine whether QISCA's architectural and behavioral claims hold across the government, defense, healthcare, and critical infrastructure contexts in which quantum migration is most urgent.

8.12. Research Domain 1: PQC Migration Performance in SDN-Container Environments

The primary empirical question is whether SDN-container environments achieve measurably faster, more complete, and more verifiable PQC migration than traditional architectures. Comparative studies pairing organizations undergoing PQC migration with and without SDN-container infrastructure would provide the strongest evidence for QISCA's central claim. Specific measurable outcomes include time to complete cryptographic inventory, proportion of network traffic protected by PQC algorithms at defined migration milestones, rate of non-PQC-compliant connection detection and remediation, and incidence of cryptographic misconfiguration relative to architecture type. Longitudinal designs spanning the 2025–2030 CNSA 2.0 transition window would capture the full migration trajectory. Defense industrial base organizations, which face the most explicit regulatory PQC migration requirements, represent a particularly valuable study population given their organizational scale, regulatory accountability, and existing security program maturity.

8.13. Research Domain 2: Quantum-Era Cognitive Load and Operator Performance

Building directly the finding that training deficits and cognitive overload are the primary human factors drivers of misconfiguration risk, this research domain investigates the cognitive load implications of simultaneous SDN-container and PQC governance for security operations personnel. Research questions include: What cognitive load profiles do security operators exhibit when managing hybrid classical-PQC cryptographic environments? Do PQC alert fatigue and cryptographic misconfiguration rates differ significantly between organizations with dedicated quantum security training programs and those without? What interface design and decision support tool features most effectively reduce PQC-related cognitive load without reducing operator engagement with cryptographic compliance? Experimental and quasi-experimental designs using validated cognitive load measurement instruments in simulated and operational security operations center environments would provide the most rigorous evidence for intervention design [23-25].

8.14. Research Domain 3: QKD Integration Feasibility in Container Orchestration Environments

The feasibility of QKD key provisioning for high-velocity containerized workloads, where key generation, distribution, and rotation must occur at the timescale of container lifecycle events, has not been empirically investigated in production-scale environments. Research questions include: What key provisioning latency is introduced by QKD-backed Kubernetes KMS integration relative to classical key management? Does QKD key pool depletion create availability risks in high-container-turnover environments? What QKD key generation rate requirements are implied by realistic enterprise container orchestration workloads at different organizational scales? Laboratory and pilot deployment studies in partnership with QKD network operators, including European Quantum Communication Infrastructure (EuroQCI) participants, would enable empirical characterization of QKD-container integration feasibility across realistic deployment scenarios [26].

8.15. Research Domain 4: TAM and UTAUT Validation for Quantum Security Adoption

The application of TAM and UTAUT to quantum security adoption proposed in this article extends established frameworks to a novel

adoption context that may exhibit different dynamics than classical technology adoption. Empirical validation questions include: Do perceived usefulness and ease of use predict quantum security adoption intentions in the same pattern as classical technology adoption, or does the probabilistic, future-oriented nature of the quantum threat alter the relationship? Do HNDL threat awareness and regulatory mandate exposure moderate the perceived usefulness, adoption intention relationship? Does quantum security facilitating conditions availability explain variance in PQC migration progress beyond that explained by individual-level TAM constructs? Survey research with cybersecurity leadership populations across sectors, supplemented by interview-based investigation of adoption decision-making processes, would provide the evidence base for TAM-UTAUT refinement specific to quantum security adoption.

8.16. Research Domain 5: Sector-Specific QISCA Implementation Studies

QISCA is proposed as a general framework; its applicability across diverse organizational sectors, defense, healthcare, financial services, and critical infrastructure requires sector-specific empirical examination, given the variation in regulatory requirements, infrastructure characteristics, and resource availability across sectors. Case study research examining QISCA implementation in each sector would characterize how Domain 1–5 requirements manifest differently across contexts, identify sector-specific implementation challenges and success factors, and develop sector-tailored implementation guidance that complements the general QISCA framework. Government and defense sector implementations merit priority investigation given NSA's CNSA 2.0 timelines and the national security implications of quantum-vulnerable cryptographic infrastructure in these sectors [27-29].

9. Discussion

This article advanced a single, falsifiable proposition: that organizations operating SDN-container architectures hold a structural advantage in post-quantum cryptographic migration, and that this advantage is realizable only through deliberate cultivation rather than passive inheritance. The Discussion that follows interprets what that proposition means for theory and practice, situates QISCA against the existing quantum-security and network-security literatures, examines the boundary conditions and counterarguments that constrain the framework's claims, and clarifies what QISCA does and does not establish in its present conceptual form.

The central interpretive contribution of QISCA is its reframing of post-quantum migration from a cryptographic replacement problem into an architectural governance problem. The prevailing treatment of PQC migration in the standards literature is algorithm-centric: it specifies which primitives to adopt, ML-KEM for key encapsulation and ML-DSA for signatures, and establishes transition timelines, but it largely abstracts away the infrastructure through which those primitives must be enforced, monitored, and sustained at enterprise scale. QISCA's argument is that the infrastructure is not incidental to migration but determinative of it. The same five capabilities that the participants identified as the operational core of SDN-container value, centralized policy enforcement, granular access control, real-time visibility, automated policy replication, and superior threat containment, map with notable precision onto the five capabilities that distinguish a tractable PQC migration from an intractable one. This correspondence is the empirical spine of the framework: each QISCA domain is not a theoretical postulate but an extension of a practitioner-validated finding into the quantum context. The interpretive weight of the framework therefore rests on whether that extension is sound, that is, on whether the architectural properties that demonstrably improved classical security outcomes transfer to cryptographic migration. The article's position is that they do transfer, because the underlying mechanism, centralized programmability applied to distributed enforcement, is indifferent to whether the policy being enforced concerns micro-segmentation rules or cryptographic algorithm selection.

This interpretation carries a consequential implication that distinguishes QISCA from the dominant framing of the quantum threat as a uniform, organization-agnostic risk. If architecture determines migration tractability, then quantum resilience is not distributed evenly across organizations of comparable size or sector; it is stratified by the maturity of an organization's existing network architecture. An organization that has already invested in SDN-container integration possesses, in the controller and the container image pipeline, the two enforcement points through which fleet-wide cryptographic transition becomes operationally feasible in hours rather than months. An organization reliant on traditional perimeter architecture faces device-by-device reconfiguration and agent-based scanning, processes whose latency the article characterizes as measured in weeks to months and whose coverage gaps are structural rather than incidental. The practical consequence is that the harvest-now-decrypt-later exposure window, the period during which an organization's encrypted traffic remains collectible for future decryption, is itself a function of architectural choice. This is a meaningful reframing: it converts a prior, seemingly unrelated infrastructure decision into a determinant of quantum risk posture, and it suggests that the return on SDN-container investment includes a quantum-resilience dividend that has not previously been recognized in the literature [30].

The framework's theoretical grounding in TAM and UTAUT addresses what is arguably the more difficult half of the migration problem. The technical argument for SDN-container superiority, even if fully accepted, does not explain why organizations would act on it, and the behavioral analysis in this article suggests strong reasons they may not [14,15]. The quantum threat presents an adoption profile that inverts the conditions under which the participants embraced SDN-container integration. Where those participants could point to concrete, immediately measurable improvements, eliminated data leaks, an 88% reduction in security check time, penetration-test-validated containment, PQC migration offers benefits that are by their nature unobservable in the absence of the threat itself. Through the lens of Kunreuther

and Michel-Kerjan's (2010) low-probability, high-consequence decision problem, and the loss-aversion and temporal-discounting biases identified by Kahneman and Tversky (1979), the article predicts systematic organizational underinvestment in protection against a probabilistic future event when the protective cost is immediate and certain [16]. This is not a peripheral observation; it is a structural prediction that the most architecturally capable organizations may nonetheless fail to migrate, because conventional ROI-based decision frameworks will undervalue the investment. The framework's response, reframing perceived usefulness around the active and present nature of the HNDL threat, the exponentially rising cost of deferred migration, and the emergence of regulatory and contractual compliance requirements that create immediate business consequences, is an attempt to engineer the perceived-usefulness conditions under which rational adoption becomes likely. The introduction of regulatory mandates as a social-influence mechanism (NSA CNSA 2.0, CISA guidance, OMB directives) is particularly important, because it identifies the lever through which adoption can be accelerated in precisely the sectors, defense, healthcare, critical infrastructure, where observed regulatory drivers functioning as adoption accelerants for classical security.

QISCA's contribution should be read alongside, and in distinction from, the existing literatures it draws upon. The SDN and container security literatures have thoroughly characterized the classical attack surfaces of these architectures, including the controller as a single point of failure and the security implications of Kubernetes networking, but they predate or do not engage the quantum threat [3-6]. The quantum-security and PQC-migration literatures have rigorously analyzed cryptographic agility and migration strategy but treat the network architecture as an undifferentiated substrate [7,9,10]. QISCA's distinctive position is at the intersection: it is, to the framework's knowledge, the first synthesis to argue that the architectural choices analyzed in the former literature directly govern the migration outcomes analyzed in the latter. The framework similarly extends the QKD literature by proposing the SDN control plane as the mediating layer that transforms QKD from a point-to-point technology into a network-wide, policy-managed resource, an integration pathway that addresses the practical constraints, distance limitation, throughput, and physical-layer vulnerability, that have confined QKD to niche deployment [8,11]. In each case, QISCA's value is not the generation of new cryptographic or networking knowledge but the structural integration of established knowledge across domains that have developed in isolation.

Several boundary conditions and counterarguments warrant explicit acknowledgment, as they define the limits of the framework's claims. First, the empirical foundation on which QISCA rests, the generic qualitative inquiry, comprised ten cybersecurity professionals across small to medium-sized enterprises. This sample is appropriate for the theory-generating purpose it served, but it constrains the generalizability of the findings extended here; the architectural advantages QISCA describes may manifest differently at enterprise and hyperscale tiers, and the SME context may understate the coordination complexity of migration in large, heterogeneous environments. Second, and most importantly, QISCA is a conceptual framework, not a validated one. Its central claim, that SDN-container environments achieve measurably faster, more complete, and more verifiable PQC migration than traditional architectures, is a hypothesis derived from the logical extension of qualitative findings, not a demonstrated empirical result. The article is explicit on this point, and the five-domain research agenda is the appropriate response: the framework's propositions are framed to be falsifiable, with specified measurable outcomes (time to cryptographic inventory completion, proportion of PQC-protected traffic at milestones, misconfiguration incidence by architecture type) precisely so that they can be tested rather than assumed. Third, the framework's QKD and quantum-machine-learning domains rest on capabilities whose operational maturity remains uncertain. The practical realization of QML anomaly-detection advantages remains an active research, and QKD integration with high-velocity container orchestration has not been empirically characterized at production scale. QISCA's treatment of these domains is therefore appropriately forward-looking rather than immediately prescriptive; it specifies the architecture into which these capabilities would integrate as they mature, while acknowledging that PQC migration, by contrast, is an immediate and standards-grounded imperative frontier [13].

A further tension internal to the framework deserves attention, because it is the point at which the technical and human-factors analyses meet and partly conflict. The same centralized programmability that makes SDN-container architectures superior migration targets also concentrates cryptographic authority and operational complexity at the control plane, and the article's own human-factors analysis warns that complexity exceeding operator training produces misconfiguration, the proximate cause to which the underlying literature attributes 89% of breaches in these environments [21,22]. The quantum transition compounds this: a misconfigured PQC deployment that silently falls back to classical cryptography furnishes false assurance of quantum resistance while preserving full HNDL vulnerability, a failure mode arguably more dangerous than no migration at all, because it removes the perception of risk without removing the risk. This is not a flaw to be argued away but a genuine constraint on the framework's promise. It is the reason the human-factors and governance domains are positioned as co-equal with the technical domains rather than subordinate to them, and the reason the QRA includes operator quantum literacy and governance maturity as scored dimensions alongside technical capability. The architectural advantage QISCA describes is real but conditional; it is realized only by organizations that pair programmable enforcement with the training, executive commitment, and facilitating conditions that UTAUT identifies as the differentiators between sophisticated and merely nominal implementation [31].

The practical implications for organizations follow directly from these interpretations. For organizations that have already implemented SDN-container integration, the actionable conclusion is that quantum-resilience does not require a separate, separately

justified security program; it is achievable as a deliberate extension of the programmable security architecture already in place, beginning with the cryptographic inventory and readiness assessment that constitute Phase 1 of the migration roadmap and prioritizing the southbound control-plane TLS sessions whose compromise would yield network-fabric-scale adversarial control. For organizations reliant on traditional architectures, the implication is more sobering: the migration latency and coverage gaps inherent to device-by-device administration extend the HNDL exposure window in a manner that architectural modernization could materially reduce, which reframes SDN-container adoption not merely as a classical-security improvement but as a quantum-preparedness measure. For policymakers and standards bodies, the analysis suggests that facilitating conditions, accessible migration tooling, certified vendor ecosystems, and workforce development, are not conveniences but structural prerequisites for adoption across the substantial segment of the economy that lacks internal quantum cryptographic expertise, a gap that CISA's (2024) own guidance acknowledges when it directs expertise-constrained organizations toward managed providers.

Taken together, these interpretations position QISCA as a framework whose significance lies less in any single technical mechanism than in its integrative reframing of the quantum-migration problem. It argues that the cryptographic transition the field now faces is governed by architectural and organizational variables that the algorithm-centric standards literature has left underexamined, that those variables can be deliberately managed through the programmable enforcement capabilities of SDN-container environments, and that the human and governance dimensions of the transition are co-determinative of its success. These are claims that the field can and should test. The framework's value, pending that empirical validation, is to specify the architecture, the readiness criteria, and the phased pathway through which organizations can convert investments they have already made into systematic quantum resilience, and to identify, with sufficient precision to guide both practice and research, the conditions under which that conversion will succeed or fail.

10. Conclusion

The convergence of quantum computing and the widespread adoption of SDN-container architectures creates both the most consequential cybersecurity challenge of the coming decade and the most promising architectural foundation for addressing it. This article has developed QISCA, the Quantum-Integrated SDN-Container Security Architecture, as a conceptual framework that extends practitioner-grounded empirical findings on SDN-container security into the quantum threat domain, integrating NIST-standardized post-quantum cryptography, quantum key distribution, and quantum-enhanced threat detection across five domains corresponding to the five primary themes of the underlying empirical research.

The article's central argument is that SDN-container integration is not merely compatible with post-quantum cryptographic migration, it is architecturally superior for that migration compared to traditional perimeter-based security approaches. The centralized programmability of SDN control planes enables cryptographic policy enforcement and compliance monitoring at a scale and consistency that traditional device-by-device administration cannot achieve. The container image distribution mechanism provides a fleet-wide cryptographic library update pathway that server-based patching approaches require weeks to months to execute. The micro-segmentation capabilities that the participants described as transformative for classical threat containment are equally effective for limiting the blast radius of any residual classical cryptographic exposure during the hybrid transition period [32,33].

However, the technical advantages of SDN-container architecture for PQC migration are not self-executing. As stated in the findings and the TAM-UTAUT analysis of quantum adoption dynamics confirms, human factors, operator training, executive commitment, organizational facilitating conditions, and governance maturity, are co-equal determinants of security outcomes alongside technical architecture decisions. The organizations that achieve genuine quantum resilience will be those that cultivate quantum cryptographic expertise systematically, govern PQC migration with the same discipline they apply to other critical infrastructure programs, and leverage SDN-container programmability deliberately for cryptographic enforcement rather than passively inheriting whatever cryptographic posture their existing technology stack provides.

The harvest-now-decrypt-later threat is not a future problem; it is a present operation conducted against today's encrypted traffic by adversaries positioned to decrypt it when CRQCs become available. The organizational decision to defer quantum security investment is a decision to accept that exposure. QISCA provides a framework for converting the architectural investments organizations have already made in SDN-container integration into a systematic foundation for quantum resilience, not as a separate security program requiring separate justification, but as the logical extension of the same programmable, centrally governed security architecture that has already demonstrated measurable improvements in classical threat protection.

The future of network security is not a choice between classical excellence and quantum readiness, it is the disciplined, human-centered integration of both into a unified architecture capable of protecting organizational assets across the full threat horizon.

References

1. Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.
2. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.
3. Hussein, A., Chadad, L., Adalian, N., Chehab, A., Elhajj, I. H., & Kayssi, A. (2020). Software-Defined Networking (SDN): the security review. *Journal of Cyber Security Technology, 4*(1), 1-66.

4. Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14-76.
5. Minna, F., Blaise, A., Rebecchi, F., Chandrasekaran, B., & Massacci, F. (2021). Understanding the security implications of kubernetes networking. *IEEE Security & Privacy, 19*(5), 46-56.
6. Sultan, S., Ahmad, I., & Dimitriou, T. (2019). Container security: Issues, challenges, and the road ahead. *IEEE access, 7*, 52976-52996.
7. Barker, E., Chen, L., & Davis, R. (2018). Recommendation for key-derivation methods in key-establishment schemes. *NIST Special Publication, 800*, 56C. National Institute of Standards and Technology.
8. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of International Conference on Computers, Systems and Signal Processing*, 175–179.
9. Chen, L., Chen, M., Coretti, S., Duric, A., Fischlin, M., Gagliardoni, T., Gjøsteen, K., Hülsing, A., Kampanakis, P., & Maram, V. (2022). PQC migration: Challenges, approaches, and recommendations. *Cryptology ePrint Archive*.
10. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy, 16*(5), 38-41.
11. Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters, 85*(2), 441.
12. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature, 549*(7671), 195-202.
13. Wittek, P. (2014). Quantum machine learning: what quantum computing means to data mining. *Academic Press*.
14. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly, 13*(3), 319-340.
15. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view1. *MIS quarterly, 27*(3), 425-478.
16. Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291.
17. Kunreuther, H., & Michel-Kerjan, E. (2010). Market and government failure in insuring and mitigating natural catastrophes: How long-term contracts can help. In Private markets and public insurance programs (pp. 175–202). *American Enterprise Institute Press*.
18. Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).
19. CISA (Cybersecurity and Infrastructure Security Agency). (2024). *Post-quantum cryptography initiative*. U.S. Department of Homeland Security.
20. NSA (National Security Agency). (2022). *Commercial national security algorithm suite 2.0* (CNSA 2.0) cybersecurity advisory.
21. Demirci, S., & Sagiroglu, S. (2019). Optimal placement of virtual network functions in software defined networks: A survey. *Journal of Network and Computer Applications, 147*, 102424.
22. Yurekten, O., & Demirci, M. (2021). SDN-based cyber defense: A survey. *Future Generation Computer Systems, 115*, 126-149. 235–259.
23. Paas, F., Tuovinen, J. E., Tabbers, H., & van Gerven, P. W. M. (2003). Cognitive load measurement as a means to advance cognitive load theory. *Educational Psychologist, 38*(1), 63–71.
24. Casalicchio, E., & Iannucci, S. (2020). The state-of-the-art in container technologies: Application, orchestration and security. *Concurrency and Computation: Practice and Experience, 32*(17), e5668.
25. Cox, J. H., Chung, J., Donovan, S., Ivey, J., Clark, R. J., Riley, G., & Owen, H. L. (2017). Advancing software-defined networks: A survey. *Ieee Access, 5*, 25487-25526.
26. Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243-256.
27. ETSI (European Telecommunications Standards Institute). (2020). *Quantum key distribution (QKD): Interface and protocol stack* (*ETSI GS QKD 004 V2.1.1*).
28. Haji, S. H., Zeebaree, S. R., Saeed, R. H., Ameen, S. Y., Shukur, H. M., Omar, N., ... & Yasin, H. M. (2021). Comparison of software defined networking with traditional networking. *Asian Journal of Research in Computer Science, 9*(2), 1-18.
29. National Institute of Standards and Technology. (2024). *Post-quantum cryptographic standards: Federal information processing standards FIPS 203, FIPS 204, FIPS 205.* U.S. Department of Commerce.
30. Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2020). Software-defined network (SDN) data plane security: issues, solutions, and future directions. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 341-387.
31. Statista. (2023). *Average cost of a data breach in the United States from 2006 to 2023*.
32. Troublefield, T. C. (2025). *How Cybersecurity Professionals View the Integration of Software-Defined Networks and Containers to Improve Network Security: A Generic Qualitative Inquiry* (Doctoral dissertation, Capella University).
33. Wong, J., Salim, M., Chua, F. F., & Tham, C. K. (2023). Container security survey: Taxonomy of attacks on container-based applications. *Journal of Network and Computer Applications, 216*, 103659.