

W H I T E P A P E R

---

# Virtual Private Networks in the Post-Quantum World

*Preparing Enterprise Security Infrastructure for the  
Era of Quantum-Capable Adversaries*

---

Published by BruceTyson.com  
Authors: Bruce Tyson, SecurityX

April 2026 | Classification: Public

Version 1.0

## Executive Summary

---

The cryptographic foundations underpinning today's Virtual Private Networks were designed in an era when quantum computers existed only in theoretical physics journals. That era is ending. Advances in quantum hardware — most notably, the achievement of cryptographically relevant qubit counts and error correction milestones at leading research institutions — have elevated a previously academic threat to a near-term operational risk. The implications for enterprise VPN infrastructure are profound and demand immediate strategic attention.

This whitepaper examines the specific vulnerabilities that quantum computing introduces to standard VPN protocols, including IKEv2/IPsec, TLS 1.3, WireGuard, and OpenVPN. It analyzes the timeline of quantum threat maturation, surveys the National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standardization process and its resulting algorithms, and provides a structured migration framework for organizations seeking to achieve quantum-resistant VPN postures.

Key findings include: (1) current RSA-2048 and Elliptic Curve Diffie-Hellman (ECDH) key exchange mechanisms are vulnerable to Shor's algorithm on sufficiently powerful quantum hardware; (2) adversaries are actively pursuing "harvest now, decrypt later" (HNDL) strategies, collecting encrypted VPN traffic today for future decryption; (3) NIST's finalized post-quantum standards — CRYSTALS-Kyber (now ML-KEM), CRYSTALS-Dilithium (now ML-DSA), and SPHINCS+ — provide viable, standards-backed migration targets; and (4) hybrid classical/post-quantum approaches offer a pragmatic transition path that preserves backward compatibility while adding quantum resilience.

Organizations that delay migration risk not only future confidentiality breaches but present-day data exfiltration through HNDL campaigns. The time to act is now — not when quantum supremacy over current cryptography is publicly demonstrated.

---

## Table of Contents

---

1. Introduction and Problem Statement	3
2. Background: VPN Cryptography and Quantum Computing	4
3. The Quantum Threat Landscape for VPNs	5
4. NIST Post-Quantum Cryptography Standards	7
5. Evaluating Current VPN Protocol Vulnerabilities	8

6. Post-Quantum VPN Architectures and Solutions	10
7. Migration Framework and Recommendations	12
8. Conclusion	14
9. References and Bibliography	15

---

## 1. Introduction and Problem Statement

---

For three decades, Virtual Private Networks have served as the workhorse of enterprise security — the encrypted tunnel through which remote workers connect, branch offices communicate, and sensitive data traverses untrusted public infrastructure. The cryptography securing these tunnels, primarily RSA and Elliptic Curve Cryptography (ECC) for key exchange and authentication, has proven robust against every classical computing adversary. No nation-state, no criminal organization, and no academic research team has succeeded in breaking a properly implemented 256-bit ECC key using classical hardware. This track record has bred a degree of institutional complacency that the quantum computing revolution is now beginning to erode.

The threat is not hypothetical. In 2024, IBM unveiled its Heron processor with 133 qubits and significantly improved error rates. Google's Willow chip, announced in late 2024, demonstrated quantum error correction below threshold for the first time — a milestone researchers had long identified as a prerequisite for fault-tolerant quantum computation. While no quantum computer has yet broken production cryptographic systems, the trajectory of progress is clear, and the community of cryptographers, national security agencies, and standards bodies has responded accordingly.

### **Why This Matters Now: The Harvest Now, Decrypt Later Threat**

Intelligence agencies and sophisticated threat actors do not need a quantum computer today to leverage tomorrow's quantum capability. By intercepting and storing encrypted VPN traffic now — a practice requiring only conventional network infrastructure — adversaries position themselves to decrypt that traffic retroactively once sufficiently powerful quantum hardware becomes available. Any data with long-term sensitivity (national security, intellectual property, financial transactions, health records, M&A communications) is potentially at risk from traffic collected today. The latency between data collection and decryption may be measured in years, but for high-value targets, that window is entirely within an adversary's strategic planning horizon.

This paper addresses three fundamental questions facing security architects, CISOs, and network engineers: What exactly makes current VPN cryptography vulnerable to quantum attacks? What standards and algorithms are available to replace vulnerable components? And how should organizations systematically migrate their VPN infrastructure toward quantum resistance without disrupting operations or introducing new attack surfaces?

## 2. Background: VPN Cryptography and Quantum Computing

---

### 2.1 How VPNs Use Cryptography

Modern VPN protocols rely on a layered cryptographic architecture. The initial handshake phase uses asymmetric cryptography — typically RSA or ECDH — to establish a shared secret between two parties who have never previously communicated. This shared secret is then used to derive symmetric session keys (AES-256 being the dominant standard) for bulk data encryption. The asymmetric phase also involves digital signatures, using algorithms like ECDSA or RSA, to authenticate the identity of each party and ensure the handshake has not been tampered with.

The security of asymmetric cryptography rests on computational hardness assumptions: that factoring large integers (the basis of RSA security) and computing discrete logarithms on elliptic curves (the basis of ECC security) are computationally infeasible for any attacker with realistic resources. These assumptions hold against all known classical algorithms. Against quantum algorithms, they do not.

### 2.2 Quantum Computing: A Primer for Security Professionals

Classical computers represent information as bits — discrete values of zero or one. Quantum computers use qubits, which exploit the quantum mechanical properties of superposition and entanglement to represent and process information in fundamentally different ways. A qubit can exist in a superposition of zero and one simultaneously until measured, and entangled qubits exhibit correlations that have no classical analog. These properties allow certain classes of problems to be solved exponentially faster on quantum hardware than on any conceivable classical machine.

Two quantum algorithms are of paramount concern to cryptographers. Shor's algorithm, published in 1994, provides an efficient quantum method for integer factorization and discrete logarithm computation — directly breaking RSA and ECC. Grover's algorithm provides a quadratic speedup for unstructured search, which effectively halves the security level of symmetric algorithms: AES-128 provides only 64-bit effective security against a quantum-equipped attacker using Grover's algorithm, while AES-256 retains approximately 128-bit effective security. The practical implication is that symmetric encryption at AES-256 remains secure in a post-quantum world; asymmetric cryptography as currently deployed does not.

### 2.3 Current State of Quantum Hardware

As of early 2026, no publicly known quantum computer can execute Shor's algorithm against production-grade RSA or ECC keys. Breaking RSA-2048 using Shor's algorithm is estimated to require millions of fault-tolerant logical qubits, far exceeding current hardware. However, progress in qubit quality, error correction, and interconnect has accelerated substantially. Industry analysts at

Gartner and academic forecasters at the Center for Security and Emerging Technology (CSET) have estimated a 50% or greater probability of cryptographically relevant quantum computers emerging within the 2030-2035 window, with some more aggressive estimates citing 2029. Planning horizons for enterprise infrastructure — including the long lifecycle of VPN hardware and the slow pace of cryptographic standard adoption — make a 2026 planning date not premature but arguably overdue.

## 3. The Quantum Threat Landscape for VPNs

### 3.1 Classifying the Quantum VPN Threat

Security practitioners should understand that quantum threats to VPN infrastructure are not uniform in timing or severity. A useful taxonomy distinguishes three threat categories based on time horizon and adversary capability:

#### **Threat Category I: Present-Day HNDL Attacks (Active Now)**

Adversaries with large-scale network interception capabilities — primarily nation-state actors — are collecting encrypted VPN traffic with the explicit intent of future decryption. NSA's BULLRUN program and related disclosures from the Snowden documents confirmed that long-term encrypted traffic archival has been a strategic intelligence priority for at least a decade. The HNDL threat requires no quantum hardware today; it merely requires storage, patience, and a future quantum capability. Any VPN traffic intercepted today that has not been protected with post-quantum key encapsulation is potentially at risk.

#### **Threat Category II: Near-Term Quantum Attacks (2028-2035 Horizon)**

Once cryptographically relevant quantum hardware becomes available — even to a limited set of nation-state actors — VPN infrastructure protected only with classical asymmetric cryptography becomes vulnerable to real-time decryption. This phase represents the transition from a strategic/intelligence threat to an operational one. First-generation quantum attacks on production cryptography are likely to be expensive, slow, and limited in scale, but targeted attacks against high-value VPN sessions (executive communications, critical infrastructure control channels, financial settlement networks) become credible.

#### **Threat Category III: Commodity Quantum Attacks (2035+ Horizon)**

As quantum hardware matures and the cost of quantum computation declines — following a trajectory analogous to classical computing — quantum attacks on VPN cryptography may become accessible to a broader range of adversaries, including sophisticated criminal organizations and smaller nation-states. At this stage, any VPN infrastructure not running post-quantum cryptography represents a critical vulnerability.

## 3.2 Protocol-Specific Vulnerabilities

The following analysis examines the quantum vulnerability profile of the four dominant VPN protocol families:

### IPsec/IKEv2

IPsec with IKEv2 is the dominant enterprise VPN standard, supported natively on Windows, macOS, iOS, Android, and most network hardware. The IKEv2 handshake uses Diffie-Hellman key exchange (vulnerable to Shor's algorithm), RSA or ECDSA for authentication (both vulnerable), and AES-GCM for bulk encryption (quantum-resistant at 256-bit key lengths). The critical vulnerability is in the key exchange and authentication phases. RFC 8784 ("Mixing Preshared Keys in IKEv2 for Post-quantum Security") provides a partial mitigation through preshared key (PSK) injection but does not address the authentication vulnerability and introduces significant key management complexity at scale.

### TLS 1.3 (SSL VPNs)

Browser-based and SSL VPN solutions relying on TLS 1.3 face similar vulnerabilities. TLS 1.3 mandated the removal of RSA key exchange in favor of Ephemeral Diffie-Hellman (DHE) and ECDHE, which improves forward secrecy but does not address quantum vulnerability. Both DHE and ECDHE are subject to Shor's algorithm. TLS 1.3's signature algorithms — RSA-PSS and ECDSA — are likewise quantum-vulnerable. The IETF is actively developing hybrid post-quantum TLS extensions (draft-ietf-tls-hybrid-design), and several major browser vendors have deployed experimental support.

### WireGuard

WireGuard has gained significant traction for its simplicity, performance, and clean cryptographic design. However, its fixed cryptographic suite — X25519 for key exchange, ChaCha20-Poly1305 for symmetric encryption, and BLAKE2s for hashing — provides no native path to post-quantum algorithms without protocol-level modification. X25519 (an ECDH variant) is vulnerable to Shor's algorithm. The WireGuard project has acknowledged this limitation; post-quantum modifications such as PQWG (Post-Quantum WireGuard) and the integration of ML-KEM into the handshake have been proposed and demonstrated in research settings but are not yet incorporated into the reference implementation.

### OpenVPN

OpenVPN's dependence on OpenSSL provides both a vulnerability (OpenSSL's classical asymmetric stack) and an opportunity (OpenSSL 3.x's growing post-quantum support via the Open Quantum Safe liboqs integration). OpenVPN's plugin architecture and configurability make it more amenable to hybrid classical/post-quantum configurations than WireGuard's opinionated design, but this flexibility comes at the cost of complexity and the risk of misconfiguration.

## 4. NIST Post-Quantum Cryptography Standards

### 4.1 The NIST PQC Standardization Process

In 2016, recognizing the emerging quantum threat, NIST initiated a formal process to solicit, evaluate, and standardize quantum-resistant cryptographic algorithms. The process attracted 69 initial submissions from cryptographers worldwide and proceeded through four evaluation rounds characterized by public scrutiny, cryptanalysis contests, and performance benchmarking. In August 2024, NIST released the finalized Federal Information Processing Standards (FIPS) for the first set of post-quantum algorithms, marking a watershed moment for the cryptographic community.

### 4.2 Finalized NIST PQC Standards

NIST's finalized post-quantum standards fall into two functional categories: key encapsulation mechanisms (KEMs) for key exchange, and digital signature algorithms for authentication. Both are required for a complete VPN migration.

Algorithm	FIPS Designation	Category	Mathematical Basis
ML-KEM (CRYSTALS-Kyber)	FIPS 203	Key Encapsulation	Module Learning with Errors (MLWE)
ML-DSA (CRYSTALS-Dilithium)	FIPS 204	Digital Signatures	Module Learning with Errors (MLWE)
SLH-DSA (SPHINCS+)	FIPS 205	Digital Signatures	Hash-based (stateless)
FN-DSA (FALCON)	FIPS 206 (draft)	Digital Signatures	NTRU Lattice (compact sigs)

Table 1: NIST Finalized and Draft Post-Quantum Cryptographic Standards (as of April 2026)

### 4.3 Algorithm Selection for VPN Applications

For VPN key exchange, ML-KEM (FIPS 203) is the primary recommendation. Available in three security levels (ML-KEM-512, ML-KEM-768, and ML-KEM-1024, corresponding roughly to AES-128, AES-192, and AES-256 classical equivalents), ML-KEM-768 is widely recommended for most enterprise applications as it balances security margin, key size, and computational performance.

For digital signatures and certificate-based authentication, ML-DSA (FIPS 204) provides strong security with moderate signature and key sizes. SLH-DSA (FIPS 205) offers a hash-based alternative whose security relies on more conservative, well-understood mathematical assumptions, but with significantly larger signature sizes that may impact handshake performance in latency-sensitive applications. FN-DSA (FALCON) offers compact signatures suitable for constrained environments but presents implementation complexity challenges.

## 5. Evaluating Current VPN Protocol Vulnerabilities

---

### 5.1 Threat Modeling Framework for VPN Cryptography

Before initiating migration planning, security teams should conduct a structured threat model specific to their VPN deployment. The following dimensions are critical to assess:

- **Data Sensitivity and Longevity:** What categories of data traverse the VPN, and for how long must that data remain confidential? Personal health information with 50-year regulatory retention, national security data, and intellectual property with decade-long competitive value all have different risk profiles than transient web browsing traffic.
- **Adversary Capability and Interest:** What is the most capable adversary likely to target your organization? A regional healthcare system faces different adversaries than a defense contractor or a G7 government ministry.
- **Traffic Volume and Interception Surface:** How much VPN traffic is exposed to potential interception? Organizations with large internet-facing VPN concentrators present a larger HNDL attack surface.
- **Cryptographic Inventory:** What asymmetric algorithms, key sizes, and certificate chains are currently in use across your VPN infrastructure? Many organizations lack visibility into the full cryptographic inventory of complex, layered VPN deployments.
- **Migration Timeline and Operational Constraints:** What are the change management, compatibility, and operational availability constraints that will govern the migration timeline?

### 5.2 The Forward Secrecy Paradox

A nuance often missed in discussions of quantum VPN vulnerability is the interaction between forward secrecy and the HNDL threat. Modern VPN protocols using ephemeral key exchange (ECDHE in TLS 1.3, DHE in IKEv2) do provide classical forward secrecy: compromise of a long-term private key does not expose historical session traffic to classical adversaries. However, this protection evaporates against a quantum attacker with HNDL-collected traffic. An adversary who has recorded an ECDHE handshake and both parties' subsequent encrypted communications can use a quantum computer to derive the ephemeral session key from the intercepted handshake messages — because the quantum attack targets the ephemeral key exchange itself, not the long-term private key. Classical forward secrecy provides no protection against this attack vector.

This insight is counterintuitive but critical: organizations should not assume that their use of Perfect Forward Secrecy (PFS) provides meaningful protection against the HNDL/quantum threat. Post-quantum forward secrecy requires using a post-quantum KEM for the ephemeral key exchange — classical ECDHE with PFS is insufficient.

### 5.3 Certificate Infrastructure Vulnerabilities

Beyond the VPN protocol handshake itself, the Public Key Infrastructure (PKI) underpinning

certificate-based VPN authentication represents a second quantum attack surface. VPN gateway certificates and client certificates signed with RSA or ECDSA become forgeable by a quantum adversary capable of running Shor's algorithm. This means an attacker could potentially forge a valid certificate for any VPN gateway in a classically-secured PKI, enabling man-in-the-middle attacks even against traffic that is itself encrypted with post-quantum algorithms.

A complete quantum-resistant VPN architecture therefore requires migration of both the handshake key exchange AND the underlying PKI to post-quantum signature algorithms. This is frequently the more complex and time-consuming component of migration, given the dependencies on certificate authorities, hardware security modules (HSMs), and certificate management systems.

---

## 6. Post-Quantum VPN Architectures and Solutions

---

### 6.1 The Hybrid Cryptography Approach

The cryptographic community and standards bodies broadly recommend a hybrid approach to post-quantum migration: combining a classical algorithm (ECDH or RSA) with a post-quantum algorithm (ML-KEM) in parallel, such that the combined scheme is secure if either component remains secure. This approach provides several important benefits during the transition period.

First, it preserves interoperability with legacy systems that do not yet support post-quantum algorithms. Second, it provides a security backstop: if the post-quantum algorithm is compromised by an unforeseen classical attack (a real concern given that PQC algorithms are younger than their classical counterparts and have had less cryptanalytic scrutiny), the classical component maintains the security level. Third, it satisfies both NIST's recommendations and the NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) guidance, which mandates hybrid approaches for national security systems.

#### Hybrid Key Exchange Construction

In a hybrid key exchange, the final shared secret is derived by combining the outputs of both key agreements through a secure key derivation function (KDF):  $\text{SharedSecret} = \text{KDF}(\text{ECDH\_output} \parallel \text{ML-KEM\_output} \parallel \text{context})$ . This construction ensures that the final key is secure as long as either the ECDH or the ML-KEM component is secure. Both the IETF (draft-ietf-tls-hybrid-design) and NIST SP 800-227 provide guidance on hybrid constructions for TLS and general-purpose use cases respectively.

### 6.2 Implementation Status in Major VPN Platforms

The post-quantum VPN ecosystem is maturing rapidly. The following represents the state of PQC support across major platforms as of early 2026:

- **OpenSSL 3.3+ with liboqs integration:** The Open Quantum Safe project's liboqs library provides experimental ML-KEM and ML-DSA support for OpenSSL, enabling OpenVPN and other OpenSSL-dependent applications to experiment with PQC. Production readiness varies; careful testing is required.
- **strongSwan IKEv2:** The widely deployed open-source IPsec implementation has introduced experimental support for ML-KEM in the IKEv2 key exchange, building on RFC 9370 (Multiple Key Exchanges in IKEv2) which provides the protocol-level framework for hybrid PQC/classical key exchange in IPsec.
- **Cloudflare and Google:** Both organizations have deployed hybrid X25519/ML-KEM key exchange in production TLS 1.3 environments, providing large-scale operational data on performance and compatibility. Cloudflare's 2024 transparency report indicated no meaningful latency degradation from ML-KEM-768 addition to TLS handshakes at their scale.
- **Cisco and Palo Alto Networks:** Enterprise VPN hardware vendors have begun publishing roadmaps for PQC support in their VPN concentrators and SASE platforms. Hardware support timelines typically lag software by 12-24 months due to firmware and HSM upgrade cycles.
- **Microsoft Azure and AWS VPN Gateways:** Cloud VPN gateways from major providers have published PQC roadmaps but as of Q1 2026 have not yet deployed production-grade post-quantum key exchange for customer VPN connections.

### 6.3 Crypto Agility as an Architectural Principle

One of the most important lessons from the transition to TLS 1.3 and the deprecation of MD5 and SHA-1 is the extraordinary operational cost of cryptographic migrations in systems not designed for algorithm agility. Crypto agility — the architectural property of being able to swap cryptographic algorithms without fundamental redesign — should be a first-class architectural requirement for any new VPN system and a criterion for evaluating existing platforms.

VPN implementations that hard-code cryptographic suites (WireGuard being the canonical example) impose migration costs proportional to the depth of the reimplementation required. In contrast, policy-based VPN systems that externalize algorithm selection to configurable cipher suites (IKEv2 with configurable proposal lists, TLS 1.3 with configurable cipher suites) allow algorithm migration through configuration changes rather than code changes — though the availability of PQC options still depends on the underlying cryptographic library.

---

## 7. Migration Framework and Recommendations

---

### 7.1 Phase 0: Inventory and Risk Assessment (Immediate)

Before any migration activity begins, organizations must develop a comprehensive cryptographic inventory. This is frequently the most labor-intensive phase and the one most often underestimated. The inventory should capture:

- All VPN endpoints, concentrators, and gateways, including cloud-based and SD-WAN components
- The specific VPN protocols, cryptographic algorithms, and key sizes in use at each component
- Certificate chains, including issuing CAs, certificate validity periods, and key algorithm used for each certificate in the chain
- Hardware Security Modules (HSMs) and their PQC algorithm support status
- Third-party and partner VPN connections and their cryptographic capabilities
- Any regulatory or compliance requirements that may constrain algorithm choices or mandate specific standards

Automated cryptographic discovery tools — including network scanning tools that perform TLS/IKE handshake analysis, certificate transparency log analysis, and SIEM-based detection of cipher suite negotiation — can accelerate this inventory process substantially. Several commercial vendors offer dedicated cryptographic bill-of-materials (CBOM) tooling that provides ongoing visibility into deployed cryptographic assets.

### 7.2 Phase 1: Hybrid PQC Deployment (12-18 Months)

Following inventory completion and risk prioritization, organizations should begin deploying hybrid classical/post-quantum key exchange on high-priority VPN connections. The recommended sequence:

- Deploy hybrid ML-KEM-768 + X25519 key exchange on internet-facing VPN concentrators handling the most sensitive traffic categories
- Update certificate management infrastructure to issue and validate ML-DSA certificates alongside existing ECDSA certificates, using a hybrid certificate approach where available
- Enable PQC cipher suites in negotiation frameworks (IKEv2 SA proposals, TLS 1.3 cipher suite configuration) in audit mode first to identify compatibility issues before enforcement
- Remediate any client endpoints, network devices, or partner connections that fail PQC handshake negotiation
- Update PKI hierarchy to include PQC root and intermediate certificates, maintaining dual RSA/ECDSA + PQC certificate chains during the transition period

Organizations subject to CNSA 2.0 requirements (US national security systems and their prime

contractors) should be aware that the NSA has established a 2030 target date for post-quantum transition of network encryption systems. Meeting this timeline requires initiating Phase 1 activities no later than 2026-2027.

### 7.3 Phase 2: Post-Quantum Primary (18-36 Months)

Once hybrid deployment is stable and compatibility issues are resolved, organizations should transition to treating the PQC component as primary, with the classical algorithm as the fallback for legacy compatibility. This phase involves:

- Migrating PKI roots to PQC signature algorithms (ML-DSA or SLH-DSA for root CAs, given their long validity periods and the importance of conservative algorithm choice)
- Removing support for classical-only key exchange in VPN policy, enforcing that all connections negotiate at minimum a hybrid classical+PQC key exchange
- Updating VPN client software across managed device fleets to versions with native PQC support
- Engaging VPN hardware vendors on firmware upgrade timelines for PQC support in concentrators and edge devices

### 7.4 Phase 3: Classical Deprecation (36-60+ Months)

The final phase — deprecating classical asymmetric cryptography entirely from VPN infrastructure — should not be rushed. Premature deprecation creates operational risk (broken connections with unmitigated legacy endpoints) without providing meaningful additional security benefit over well-implemented hybrid cryptography. Phase 3 activities should be driven by the completion of ecosystem-wide PQC adoption rather than by a fixed timeline. Key milestones that indicate readiness for Phase 3 include:

- Greater than 99% of VPN client connections successfully negotiating PQC or hybrid key exchange
- Completion of PKI migration to PQC-signed certificate chains
- Confirmation from all third-party and partner VPN endpoints that they support PQC key exchange
- Regulatory guidance confirming that the deprecation of specific classical algorithms is compliant with applicable standards (NIST, CNSA 2.0, FIPS)

Phase	Timeline	Key Activities	Success Metrics
Phase 0	Immediate (0-6 mo)	Cryptographic inventory, risk assessment, vendor engagement	CBOM complete; risk tiers assigned
Phase 1	12-18 months	Hybrid PQC deployment on priority connections; PKI dual-stack	High-priority VPNs: hybrid PQC active

Phase 2	18-36 months	PQC-primary policy; PKI root migration; client fleet updates	>90% connections using PQC/hybrid
Phase 3	36-60+ months	Classical deprecation; full PQC-only infrastructure	100% PQC; classical removed

Table 2: Post-Quantum VPN Migration Framework Summary

## 8. Conclusion

The migration of VPN infrastructure to post-quantum cryptography is not a future consideration — it is a present-day strategic imperative. The harvest now, decrypt later threat means that VPN traffic being transmitted today over classically-encrypted tunnels is already potentially at risk from sophisticated adversaries with long planning horizons. The maturation of NIST post-quantum standards, the growing availability of PQC implementations in major cryptographic libraries and VPN platforms, and the publication of clear migration guidance from NIST, NSA, and CISA collectively eliminate the technical uncertainty that might once have justified delay.

The organizations best positioned for this transition will be those that act now on three fronts: developing visibility into their cryptographic inventory through comprehensive CBOM tooling; beginning hybrid PQC deployment on the highest-sensitivity VPN connections without waiting for universal ecosystem support; and demanding PQC roadmap commitments from VPN hardware and software vendors as a condition of procurement decisions.

The post-quantum transition will test the institutional capacity of security organizations in ways that previous cryptographic migrations did not. The SHA-1 deprecation and TLS 1.0/1.1 sunset were painful but relatively contained. The post-quantum migration touches every asymmetric cryptographic operation in enterprise infrastructure simultaneously — VPNs, PKI, code signing, email encryption, hardware authentication tokens, and more. VPN infrastructure, as the perimeter of the enterprise network, represents both a critical priority and an opportunity to build migration expertise that can be applied across the broader cryptographic transformation ahead.

The quantum era is not approaching — it is arriving. The organizations that move with deliberate urgency today will be the ones that face it from a position of security rather than vulnerability.

## 9. References and Bibliography

---

### Standards and Government Publications

- National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. U.S. Department of Commerce.
- National Security Agency/Central Security Service. (2022). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). NSA Cybersecurity Advisory.
- Fluhrer, S. (2020). RFC 8784: Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 for Post-quantum Security. IETF.
- Tjhai, C., et al. (2023). RFC 9370: Multiple Key Exchanges in IKEv2. IETF.
- Rescorla, E. (2018). RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3. IETF.
- Cybersecurity and Infrastructure Security Agency. (2024). Post-Quantum Cryptography Migration Roadmap. CISA.

### Academic and Research Publications

- Shor, P.W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE.
- Grover, L.K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing. ACM.
- Bernstein, D.J. & Lange, T. (2017). Post-Quantum Cryptography. *Nature*, 549(7671), 188-194.
- Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, 16(5), 38-41.
- Sikeridis, D., et al. (2020). Post-Quantum Authentication in TLS 1.3: A Performance Study. Network and Distributed System Security (NDSS) Symposium.
- Campagna, M., et al. (2015). Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. ETSI White Paper No. 8.
- Schwabe, P. & Westerbaan, B. (2016). Solving Binary MQ with Grover's Algorithm. *Security, Privacy, and Applied Cryptography Engineering (SPACE)*. Springer.

### Industry and Technical Reports

- Google Security Blog. (2024). Protecting Chrome Traffic with Hybrid Kyber KEM. Google LLC.
- Cloudflare Blog. (2024). Post-Quantum Cryptography at Scale: Year in Review. Cloudflare, Inc.

- IBM Research. (2024). IBM Quantum Heron: Architecture and Performance Benchmarks. IBM Corporation.
- Gartner Research. (2025). Market Guide for Post-Quantum Cryptography Solutions. Gartner, Inc.
- Open Quantum Safe Project. (2025). liboqs 0.11 Release Notes and Algorithm Documentation. Linux Foundation.
- GSMA. (2024). Post Quantum Telco Network Task Force — Key Findings and Recommendations. GSMA Intelligence.
- Center for Security and Emerging Technology. (2025). Quantum Computing Timelines and Cryptographic Risk: Updated Analysis. Georgetown University CSET.

---

**Bruce Tyson, SecurityX**

bruce@brucetyson.com | www.brucetyson.com

© 2026 Bruce Tyson. .This document is provided for informational and educational purposes.