A Detection Taxonomy for Quantum-Enabled Cyber Attacks: A Systems-Level Framework for Pre-CRQC Threat Monitoring

Robert E. Campbell *

Posted Date: 21 April 2026

doi: 10.20944/preprints202604.1363.v1

Keywords: quantum-enabled attacks; post-quantum cryptography; threat detection; hybrid cryptography; TLS telemetry; quantum reconnaissance; HNDL; systems security; quantum computing; cybersecurity taxonomy

 doi:10.20944/preprints202604.1363.v1

Article

A Detection Taxonomy for Quantum-Enabled Cyber Attacks: A Systems-Level Framework for Pre-CRQC Threat Monitoring

Robert E. Campbell

Independent Researcher, Upper Marlboro, MD 20772, USA; rc@medcybersecurity.com

Abstract

Quantum computing introduces a new class of cyber threats that challenge existing detection paradigms. While significant research has focused on post-quantum cryptography (PQC) and the long-term risk of cryptographic breakage, far less attention has been given to the detection of quantum-enabled attacks during the pre-cryptographically-relevant quantum (pre-CRQC) era. Current intrusion detection systems, network monitors, and cryptographic telemetry tools lack the conceptual models and operational indicators needed to identify adversaries who leverage quantum acceleration, quantum-optimized reconnaissance, or hybrid-mode downgrade strategies. This paper proposes QEADT-1, a systems-level taxonomy for detecting or monitoring quantum-enabled attack patterns against classical and PQC-transitioning infrastructure during the pre-CRQC era, addressing a gap in the literature, which has focused predominantly on prevention through PQC migration and on QKD or quantum-hardware concerns rather than operational detection. We classify six major attack classes, identify their underlying mechanisms, and map each to proposed observable indicators and required telemetry sources. A SOC-oriented detection matrix is introduced to operationalize the taxonomy as a synthesized detection model, followed by a systems architecture for quantum-attack monitoring that is designed to integrate with ongoing PQC migration. This work provides a foundational framework for organizations seeking to detect quantum-enabled threats before cryptographically relevant quantum computers emerge.

Keywords: quantum-enabled attacks; post-quantum cryptography; threat detection; hybrid cryptography; TLS telemetry; quantum reconnaissance; HNDL; systems security; quantum computing; cybersecurity taxonomy

1. Introduction

1.1. Motivation

Quantum computing is rapidly transitioning from theoretical curiosity to practical capability. Foundational work by Shor [1] and Grover [2] established that quantum algorithms can undermine the hardness assumptions underlying RSA, ECC, and symmetric-key search, and early policy-oriented analyses laid out the operational implications for enterprise cybersecurity [4]. A recent systematic review synthesizes the accelerating literature on these emerging threats [6]. Although today's devices cannot yet break modern cryptography, adversaries can, in principle, exploit quantum-assisted inference and quantum-inspired optimization [17,19], and the harvest-now, decrypt-later (HNDL) strategy is widely recognized as a serious strategic threat model in the transition period [15,16]. These emerging behaviors create a new class of cyber threats—quantum-enabled attacks—that operate long before cryptographically relevant quantum computers (CRQCs) exist.

Organizations worldwide are migrating to post-quantum cryptography (PQC), driven by the publication of NIST's first PQC standards [7–9], federal transition guidance [11,25,34,35], and expert-survey-based projections of the CRQC timeline [33], yet this migration focuses predominantly on

 doi:10.20944/preprints202604.1363.v1

prevention. The equally critical question—how do we detect quantum-enabled attacks?—remains largely unaddressed.

1.2. Problem Statement

Despite growing awareness of quantum risk, the field lacks:

1. A unified taxonomy of quantum-enabled attacks on classical systems.
2. A mapping between attack mechanisms and observable indicators.
3. A definition of the telemetry required to detect pre-CRQC threats.
4. A systems-level detection framework aligned with SOC workflows.

Existing research focuses on quantum key distribution (QKD) or quantum hardware attacks [16]. These domains do not address the broader challenge: detecting quantum-enabled attacks against classical networks, cryptographic stacks, and PQC-transitioning infrastructure.

1.3. Contributions

This paper makes five primary contributions:

1. QEADT-1, a systems-level taxonomy of quantum-enabled attacks positioned as a detection-oriented counterpart to existing prevention-oriented PQC migration guidance.
2. A structured mapping of proposed observable indicators to attack mechanisms.
3. A telemetry model identifying the data sources required for detection.
4. A SOC-oriented detection matrix that operationalizes the taxonomy as a synthesized model for analysis and engineering.
5. A systems architecture for quantum-attack monitoring integrated with PQC migration.

1.4. Paper Structure

Section 2 reviews the background. Section 3 establishes the threat model, operational context, adversary profile, and observability planes, and enumerates the six attack classes. Section 4 develops the detection taxonomy. Section 5 populates the detection matrix and summarizes row-level detection signatures in Table 1. Section 6 proposes the monitoring architecture, addressing PQC-migration integration and enterprise-scale deployment. Section 7 presents three synthetic case studies that walk end-to-end through the taxonomy. Section 8 discusses limitations and future work. Section 9 concludes.

2. Background

2.1. Quantum Computing and Emerging Cyber Threats

Quantum computing threatens classical cryptography by undermining hardness assumptions foundational to RSA, ECC, and symmetric-key search [1–3]. Hybrid quantum–classical models have been studied empirically in intrusion-detection settings [20], and the underlying quantum-kernel and quantum-feature-space foundations are well-established [17,18], suggesting adversaries may in principle leverage quantum-assisted inference to enhance reconnaissance or evasion.

2.2. Harvest-Now, Decrypt-Later (HNDL)

HNDL is one of the most widely recognized quantum-era cybersecurity threat models. It involves intercepting encrypted data today and storing it until quantum computers can break the underlying key exchange. A recent temporal risk model quantifies HNDL exposure and shows that long-lived data in sectors such as healthcare and satellite communications face decades-long exposure windows under delayed PQC adoption [15]. Broader analyses of cybersecurity in the quantum era similarly identify long-term confidentiality as a first-order concern rather than an abstract future risk [16], and enterprise migration analyses make the case that the HNDL risk calculus

 doi:10.20944/preprints202604.1363.v1

is already binding on data with confidentiality requirements extending beyond the FTQC arrival window [38].

2.3. PQC Migration and Hybrid Cryptography

PQC schemes standardized by NIST in August 2024—ML-KEM (FIPS 203, formerly CRYSTALS-Kyber) [7], ML-DSA (FIPS 204, formerly CRYSTALS-Dilithium) [8], and SLH-DSA (FIPS 205, based on SPHINCS+) [9]—offer strong quantum resistance, while earlier hash-based signature schemes such as XMSS and related stateful schemes are profiled for federal use in NIST guidance [12,40]. Enterprise adoption remains uneven and requires a phased transition under federal guidance [11,25]. A structured timeline analysis of enterprise PQC migration estimates 5–7 years for small, 8–12 years for medium, and 12–15+ years for large enterprises under baseline assumptions, driven by HSM replacement cycles, partner ecosystem coordination, and legacy IoT/OT constraints [38]. Hybrid deployments, which combine classical and post-quantum algorithms during the migration window, introduce new negotiation failure modes and downgrade risks that have been formally modeled [14], prototyped in TLS and SSH [36], and empirically benchmarked in real TLS deployments [13]. The viability of post-quantum X.509 certificates and the downstream PKI implications have been characterized in detail [32].

2.4. Limitations of Existing Detection Approaches

Current IDS and network monitors are designed for classical threat models. A foundational critique of ML-based network intrusion detection articulates why laboratory results rarely translate to operational deployments [28], and subsequent surveys catalog the space of ML and data-mining methods used in the field [29]. Recent simulation-based feasibility work in quantum-enhanced federated security operations similarly documents structural barriers to quantum-era SOC integration, including operational alert volumes, correlation-mechanism gaps, and scalability constraints [37]. Even advanced ML-based IDS struggle with rare or borderline attacks, and preliminary quantum-classical hybrid detection studies suggest quantum feature spaces may offer measurable advantages on such edge cases [20,27]. Quantum-enhanced evasion against ML-based IDS is plausible given the underlying capability foundations [17–19], but empirical demonstrations against operational-scale enterprise IDS pipelines remain limited (see Section 8.1). PQC telemetry remains inconsistent across systems, and Internet-scale TLS and CT measurement studies reveal persistent heterogeneity in cryptographic deployment [13,21,22]. These gaps motivate a structured detection taxonomy.

3. Threat Model and Operational Context

3.1. Target Environment

QEADT-1 is scoped to the broad, cryptographically diverse infrastructure of modern enterprises, federal systems, and critical infrastructure. The framework assumes defenders are protecting:

- **Transport:** TLS 1.2/1.3, QUIC, SSH
- **Application:** API gateways, identity providers, certificate validation
- **Infrastructure:** VPNs, SD-WAN, cloud service meshes
- **Key management:** PKI, Certificate Transparency (CT), HSMs

These systems are currently being migrated to PQC (§2.3), with hybrid deployments as an interim step [14,36]. The framework operates during this transition period.

3.2. Adversary Model and Operational Assumptions

- **Adversary profile.** The detection framework presumes an externally positioned, campaign-capable adversary with the resources to sustain reconnaissance, harvesting, or manipulation

 doi:10.20944/preprints202604.1363.v1

campaigns over extended periods. The adversary is crypto-stack-aware—familiar with TLS, PKI, and PQC negotiation semantics—and has access to quantum-inspired optimization, quantum-assisted inference, and early-stage quantum computing. Pure insider threats and one-shot opportunistic attackers fall outside the primary threat model, though indicators surfaced by QEADT-1 may incidentally detect such activity. Different attack classes assume different adversary postures: HNDL (§4.1) requires campaign-level persistence and passive collection capacity, while PQC Downgrade and Hybrid-Mode Attacks (§4.1) require an active network position.

The framework further assumes four operational realities:

- Quantum-accelerated offensive capabilities are best understood as emerging and capability-founded rather than broadly deployed in operational cyber campaigns. Cryptographically relevant quantum computers do not yet exist, but the capability foundations for quantum-assisted inference, quantum-kernel feature spaces, and hybrid quantum-classical computation are well-established [17–19,27], and estimates of the qubit budgets required to break RSA-2048 [5] and the expected CRQC arrival window [33] have been analyzed in detail.
- PQC migration is incomplete and asymmetric. Empirical studies and NIST transition guidance show that PQC adoption remains uneven across services, vendors, and geographies [11,38], with hybrid deployments introducing new negotiation failure modes, downgrade opportunities, and implementation bugs as documented in hybrid KEM security analyses [14], TLS benchmarking [13], and migration-timeline frameworks that catalog the operational dependency chains [38]. This incompleteness is not a transitional inconvenience but a durable feature of the pre-CRQC window. In some sectors, the asymmetry is even more pronounced: analyses of blockchain PQC migration identify governance barriers that may stall adoption indefinitely absent a crisis-forcing event, because, unlike every prior cryptographic upgrade, PQC is a defensive downgrade imposing immediate costs on decentralized stakeholders with no near-term offsetting benefit [39].
- Long-lived data is at elevated risk today. HNDL threat models demonstrate that data with confidentiality lifetimes exceeding the attacker's quantum horizon is vulnerable to future decryption, even when intercepted under classical cryptography today [15,16]. Data classification—not just telemetry—therefore informs detection prioritization.
- Defenders rely exclusively on classical telemetry. Enterprise systems do not expose quantum-specific telemetry. Detection must therefore be constructed from classical signals—TLS handshake metadata [21,24], certificate lifecycle events and CT log access patterns [22], and network flow metadata—even when the underlying attack is hypothesized to be quantum-enabled.

3.3. Observability Planes

QEADT-1 organizes detection around three observability planes, each corresponding to a distinct class of telemetry sources and indicator types.

3.3.1. Cryptographic Plane

Operations related to key exchange, certificate validation, signature verification, and hybrid cryptographic negotiation. Hybrid key exchange introduces new negotiation failure modes and downgrade opportunities that must be monitored explicitly [14]. This plane primarily surfaces indicators for Quantum-Accelerated Cryptanalysis, Quantum-Assisted Side-Channel Attacks, and PQC Downgrade and Hybrid-Mode Attacks.

3.3.2. Network Plane

Traffic-level behavioral patterns, including timing irregularities, low-entropy scanning sequences, abnormal handshake retry patterns, and bulk traffic characteristics. High-speed key

 doi:10.20944/preprints202604.1363.v1

harvesting and scanning manifest primarily in this plane, building on well-studied Internet-wide scanning foundations [23] and quantum-algorithmic speedup basis [2,5]. The plane principally supports Quantum-Optimized Reconnaissance, Quantum-Enhanced Evasion, and HNDL.

3.3.3. Identity and Certificate Plane

PKI operations, CT log activity, certificate issuance, revocation, and renewal patterns. Large-scale certificate scraping and enumeration observable through Certificate Transparency logs [22] are documented precursors to long-term decryption campaigns [15]; the PKI-specific viability and migration challenges for post-quantum X.509 certificates are characterized in [32]. This plane most directly supports HNDL, Quantum-Optimized Reconnaissance, and Quantum-Accelerated Cryptanalysis.

3.4. Attack Class Enumeration

QEADT-1 recognizes six classes of quantum-enabled attacks against classical and PQC-transitioning infrastructure, each enabled by a distinct quantum-era capability: quantum-accelerated search [1,2,5], quantum-assisted inference [17–19], quantum-optimized reconnaissance, large-scale key harvesting [15,16], or hybrid-mode protocol manipulation [14], as surveyed in recent systematic reviews [3,6]. The six classes below name the mechanism each exploits and the supporting empirical basis. They are formally positioned as Level 1 of the detection taxonomy in Section 4.1, and their detection signatures across indicators, telemetry, and methods are populated in the Detection Matrix (Section 5).

The six classes do not all share the same evidentiary maturity: HNDL, PQC downgrade / hybrid-mode manipulation, and reconnaissance are comparatively more grounded in currently observable transition-era behaviors, whereas side-channel amplification, cryptanalysis detection, and evasion are included as capability-founded but more forward-looking classes.

- **Quantum-Accelerated Cryptanalysis** — a forward-looking class covering attacks that would leverage quantum speedups — Grover-like quadratic reductions [2] and Shor-style factoring once viable [1], with current qubit-budget analyses informing feasibility discussions [5] — to reduce the complexity of brute-force search, key recovery, or optimization-based cryptanalysis against symmetric and asymmetric primitives.
- **Quantum-Optimized Reconnaissance** — scanning, enumeration, or fingerprinting enhanced by quantum-assisted optimization or inference [19], built on top of well-characterized Internet-wide scanning baselines [23], enabling faster identification of vulnerable endpoints, weak certificates, or misconfigured hybrid cryptographic deployments.
- **Quantum-Assisted Side-Channel Attacks** — a capability-founded but still largely prospective class involving the hypothesized use of quantum-inspired ML or hybrid quantum-classical models [17–19] to accelerate inference from noisy or partial side-channel data, including timing, power, and electromagnetic leakage, potentially reducing the samples required to extract partial key material; empirical demonstrations remain scarce (see Section 8.1).
- **Quantum-Enhanced Evasion** — a forward-looking class covering techniques that could exploit quantum-optimized perturbations and hybrid quantum-classical models [17–19] to evade ML-based intrusion detection systems, potentially reducing classifier detection rates below operational thresholds; this class is explicitly scoped as prospective in Section 8.1.
- **PQC Downgrade and Hybrid-Mode Attacks** — exploitation of negotiation failures, fallback paths, or misconfigurations in hybrid PQC deployments, forcing downgrade to classical (non-PQC) algorithms; formal analyses of hybrid KEMs identify negotiation-failure modes as a principled security concern [14], measurement studies of real PQC TLS deployments document operational downgrade risks [13], and enterprise migration analyses catalog the operational failure modes that create these opportunities at scale — HSM capacity constraints, certificate chain size inflation, middlebox incompatibility, and partner synchronization gaps [38].

 doi:10.20944/preprints202604.1363.v1

- **HNDL (Harvest-Now, Decrypt-Later)** — bulk interception and storage of classically-encrypted data for future quantum decryption; temporal risk models demonstrate that long-lived data faces decades-long exposure windows under delayed PQC adoption [15], and broader cybersecurity analyses identify HNDL as a first-order concern [16].

4. Quantum-Enabled Attack Detection Taxonomy (QEADT-1)

The QEADT-1 taxonomy (Figure 1) provides a structured framework for classifying quantum-enabled attacks and identifying the observable indicators and telemetry required for detection. It is organized into five hierarchical levels: (1) attack class, (2) mechanism, (3) observable indicators, (4) required telemetry, and (5) detection techniques. The taxonomy is proposed as a synthesized systems model derived from current literature and operational transition realities; it is not yet benchmark-validated across all six classes.

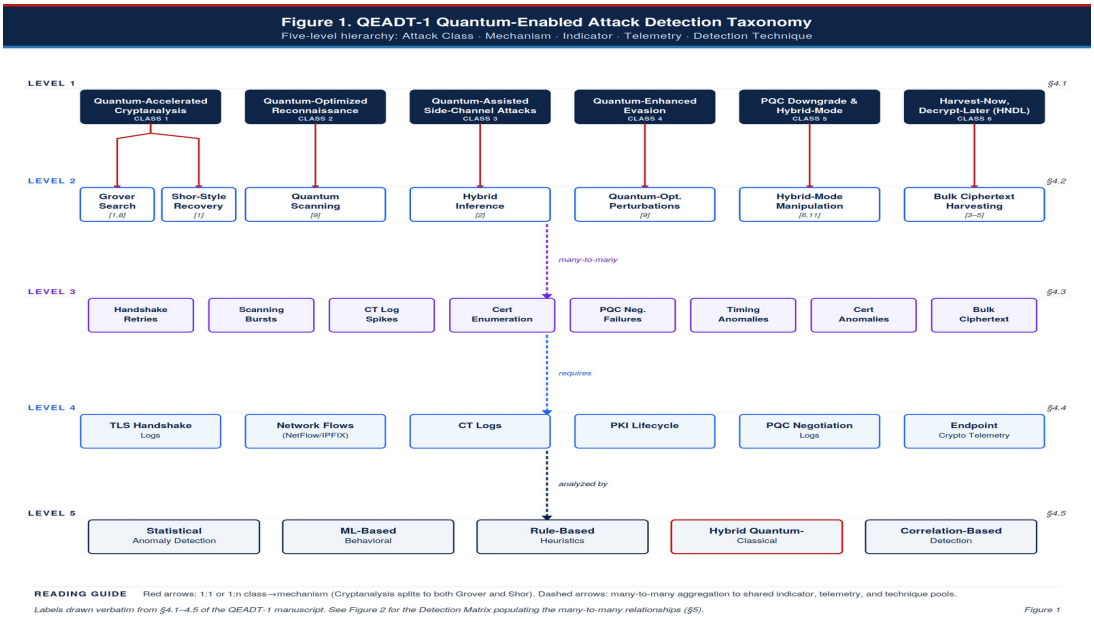

Figure 1. QEADT-1 taxonomy: five hierarchical levels mapping attack classes through mechanisms, observable indicators, required telemetry, to detection techniques (Sections 4.1–4.5).

4.1. Level 1 — Attack Class

The taxonomy defines six primary classes of quantum-enabled attacks, derived from the threat model in Section 3:

- Quantum-Accelerated Cryptanalysis
- Quantum-Optimized Reconnaissance
- Quantum-Assisted Side-Channel Attacks
- Quantum-Enhanced Evasion
- PQC Downgrade and Hybrid-Mode Attacks
- Harvest-Now, Decrypt-Later (HNDL)

These classes span two evidentiary strata. HNDL [15,16] and PQC Downgrade / Hybrid-Mode Attacks [13,14,38] are grounded in empirical campaign patterns and documented deployment failure modes. Quantum-Accelerated Cryptanalysis, Quantum-Assisted Side-Channel Attacks, and Quantum-Enhanced Evasion are capability-founded, forward-looking projections whose algorithmic foundations [1–5], systematic threat reviews [6], and quantum-machine-learning capability foundations [17–19] are well established in the literature, even though scaled attack realizations have

 doi:10.20944/preprints202604.1363.v1

not been publicly reported. Quantum-Optimized Reconnaissance sits between the two strata, extending well-characterized classical scanning baselines [23] with quantum-assisted optimization [19].

4.2. Level 2 — Mechanisms

Each attack class is associated with one or more mechanisms:

- Grover-accelerated search (reduced brute-force complexity) [2]
- Shor-style key recovery simulation (partial factorization or lattice reduction) [1,5]
- Quantum-optimized scanning (accelerated enumeration of endpoints, extending classical scanning baselines [23]) [19]
- Hybrid inference-based side-channel reconstruction [17,18]
- Quantum-optimized perturbations for IDS evasion (forward-looking; see Section 8.1) [17–19]
- Hybrid-mode negotiation manipulation [13,14]
- Bulk ciphertext harvesting for future decryption [15,16]

These mechanisms form the operational basis for detection. Quantum-Accelerated Cryptanalysis is associated with both Grover-accelerated search and Shor-style key recovery, reflecting the dual quantum-algorithmic threat to symmetric and asymmetric primitives; the remaining classes map to single primary mechanisms.

4.3. Level 3 — Observable Indicators

Observable indicators represent the proposed behavioral signatures that defenders can monitor or test for in telemetry:

- Abnormal TLS handshake retry patterns
- Low-entropy, high-speed scanning bursts
- Certificate transparency (CT) log access spikes
- Large-scale certificate enumeration
- Hybrid key exchange negotiation failures
- Timing anomalies in key exchange
- Unusual certificate renewal or revocation patterns
- High-volume ciphertext collection events

These indicators are synthesized from empirical PQC migration and hybrid KEM studies [13,14], HNDL threat models [15,16], and broader operational reasoning about what would likely surface in classical telemetry during pre-CRQC attack activity.

4.4. Level 4 — Required Telemetry

Detection requires telemetry from multiple planes:

- TLS handshake logs (cipher suites, key shares, retries)
- Network flow metadata (timing, entropy, scanning patterns)
- Certificate transparency logs (queries, anomalies)
- PKI lifecycle events (issuance, renewal, revocation)
- PQC negotiation logs (hybrid failures, fallback events)
- Endpoint cryptographic telemetry (key generation, rotation)

NIST PQC standardization reports and transition guidance underscore the broader need for structured transition visibility across these domains [10,11], even though no mature, universally adopted PQC telemetry schema yet exists.

4.5. Level 5 — Detection Techniques

Detection techniques include:

- Statistical anomaly detection (timing, frequency, entropy)

 doi:10.20944/preprints202604.1363.v1

- Machine-learning-based behavioral detection [20]
- Rule-based heuristics (downgrade detection, CT anomalies)
- Hybrid quantum–classical detection models, building on quantum feature-space and variational quantum algorithm foundations, are included here as future-facing extensions rather than operationally mature SOC components [17,18,27,31]
- Correlation-based detection (linking CT logs, TLS anomalies, and scanning patterns; related physical-cyber correlation mechanism design has been explored in simulation for quantum-enhanced federated security operations [37])

These techniques form the operational basis for the detection matrix in Section 5.

5. Detection Matrix

The Detection Matrix (Figure 2) operationalizes the QEADT-1 taxonomy by populating a grid of six attack classes (rows) against twenty detection dimensions (columns): one primary mechanism per class, eight observable indicators (Section 4.3), six telemetry sources (Section 4.4), and five detection techniques (Section 4.5). For each attack class, the matrix records which indicators are expected to fire, which telemetry streams must be available for those indicators to be constructed, and which detection techniques are applicable. Reading the matrix row-wise yields a detection signature for a given attack class; reading it column-wise identifies which attack classes would activate a given indicator, telemetry source, or technique. The matrix should be interpreted as a proposed detection model synthesized from the literature and system-design analysis, not as a fully benchmark-validated empirical classifier across all six classes.

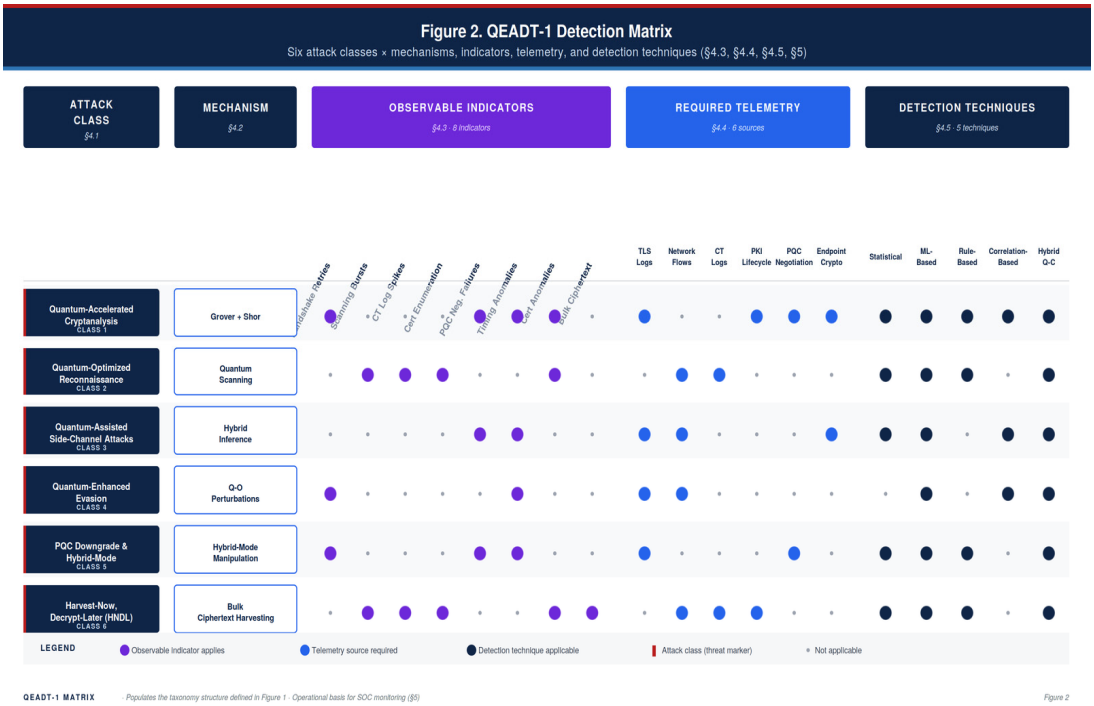

Figure 2. QEADT-1 Detection Matrix: six attack classes × twenty dimensions (1 mechanism + 8 indicators + 6 telemetry + 5 techniques). See Table 1 for row-level summary.

Several structural patterns emerge from the matrix. HNDL (Class 6) has the widest indicator footprint, activating five of the eight indicators — reflecting its dependence on bulk-traffic characteristics, certificate enumeration patterns, and CT log activity that span multiple observability planes. Quantum-Accelerated Cryptanalysis (Class 1) is mapped to every detection technique in the proposed matrix because its hypothesized observable manifestations — timing anomalies,

 doi:10.20944/preprints202604.1363.v1

handshake retries, and certificate-lifecycle irregularities — would, if present, cut across statistical, ML-based, rule-based, and correlation-based analytic methods. PQC Downgrade and Hybrid-Mode Attacks (Class 5) concentrate on the cryptographic plane: hybrid negotiation failures, handshake anomalies, and certificate chain inconsistencies map to PQC negotiation logs and TLS handshake logs as the primary telemetry dependency. Quantum-Enhanced Evasion (Class 4) has the narrowest indicator set, reflecting honest scoping of a forward-looking class (see Section 8.1).

Operationally, defenders should use the matrix in two directions. When building a new detection capability, they should select an attack class of interest and identify the minimum telemetry set required to construct the indicators associated with that class — this defines the instrumentation requirements for that coverage. When triaging an alert, they should consult the matrix column-wise from the firing indicator back to the candidate attack classes, which narrows the hypothesis space for investigation. Table 1 summarizes illustrative dominant row-level detection signatures and serves as a quick-reference adjunct to Figure 2; it is intentionally reductive and does not replace the multi-source logic of the full matrix.

Because several attack classes are inherently multi-plane and correlation-dependent, Table 1 presents only the dominant indicator, telemetry source, and analytic technique for each row rather than the full detection dependency structure shown in Figure 2.

Table 1. Illustrative dominant attack-class detection signatures (simplified row-level summary of Figure 2).

Attack Class	Primary Indicator	Primary Telemetry	Primary Technique
Quantum-Accelerated Cryptanalysis	Timing anomalies in key exchange	TLS handshake logs	Statistical
Quantum-Optimized Reconnaissance	Low-entropy scanning bursts	Network flow metadata	ML-based
Quantum-Assisted Side-Channel Attacks	Timing anomalies, handshake anomalies	Endpoint crypto telemetry	ML-based
Quantum-Enhanced Evasion	Handshake anomalies, timing anomalies	Network flow metadata	Correlation-based
PQC Downgrade and Hybrid-Mode Attacks	Hybrid negotiation failures	PQC negotiation logs	Rule-based
Harvest-Now, Decrypt-Later (HNDL)	Bulk ciphertext events, CT log spikes	CT logs, network flows	Correlation-based

6. System Architecture for Quantum-Attack Monitoring

To make QEADT-1 actionable, we propose a four-stage monitoring architecture (Figure 3). The architecture translates the taxonomy into a concrete pipeline that defenders can instantiate in an existing SOC.

6.1. Telemetry Ingestion

The ingestion layer collects six classes of telemetry spanning transport, certificate, PKI, negotiation, and endpoint surfaces:

- **TLS handshake logs** — cipher suites, key shares, ALPN negotiation, retries
- **Network flow metadata** — NetFlow/IPFIX records capturing timing, entropy, and scanning patterns
- **Certificate Transparency logs** — issuance feeds, query volumes, and enumeration anomalies
- **PKI lifecycle events** — certificate issuance, rotation, and revocation activity
- **PQC negotiation logs** — hybrid handshake outcomes and fallback events
- **Endpoint cryptographic telemetry** — host-level key generation, rotation, and cryptographic operations

 doi:10.20944/preprints202604.1363.v1

NIST PQC standardization and transition documents reinforce the need for structured migration visibility and implementation awareness across these sources [10,11], while TLS and hybrid KEM measurement studies underscore the need for monitoring hybrid cryptographic deployments [13,14].

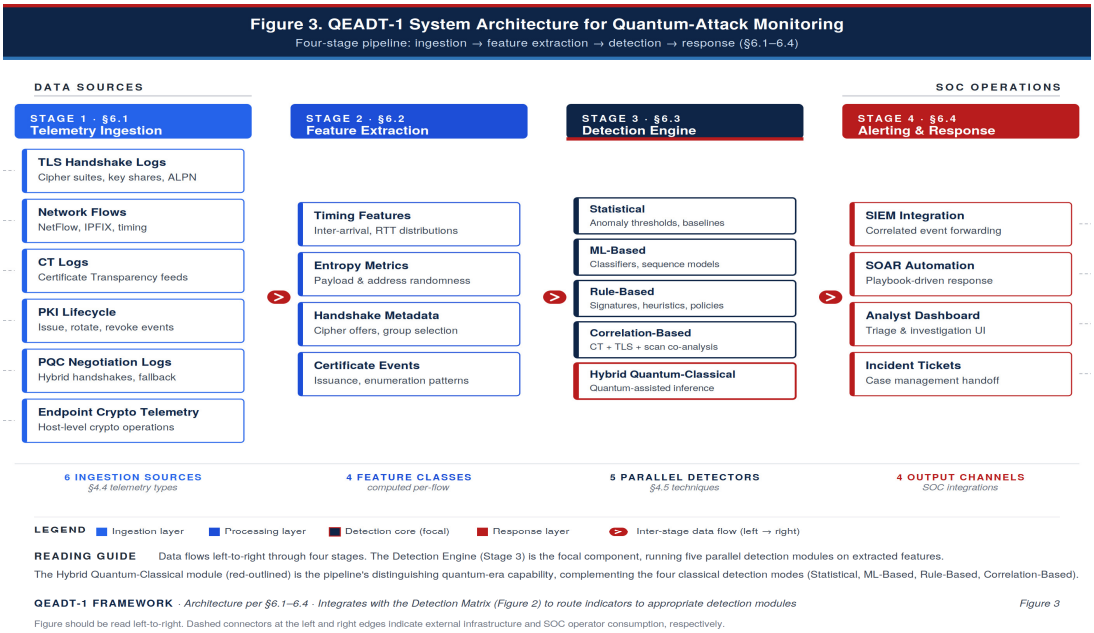

Figure 3. QEADT-1 system architecture: four-stage pipeline from telemetry ingestion through feature extraction, five-module detection engine, to SOC integration (Sections 6.1–6.4).

6.2. Feature Extraction

Ingested telemetry is normalized into four feature classes consumed by the detection engine:

- **Timing features** — inter-arrival distributions, round-trip times, handshake latencies
- **Entropy metrics** — payload randomness and address-space distribution (indicator of scanning)
- **Handshake metadata** — cipher offers, named group selection, extension patterns
- **Certificate events** — issuance velocity, enumeration patterns, lifecycle anomalies

6.3. Detection Engine

The detection engine runs five parallel detection modules over extracted features, corresponding to Level 5 of the taxonomy (Section 4.5):

- **Statistical anomaly detection** — threshold-based outlier detection over timing, frequency, and entropy features
- **Machine-learning-based behavioral detection** — classifiers and sequence models trained on labeled or synthetically generated traffic, depending on dataset availability [20,30]
- **Rule-based heuristics** — signature matches for downgrade attempts, CT-log anomalies, and enumeration patterns [22], and known evasion patterns
- **Correlation-based detection** — cross-source linkage connecting CT log activity, TLS anomalies, and network-flow patterns; a related correlation-mechanism formulation for quantum-enhanced federated security operations has been explored in simulation [37]
- **Hybrid quantum-classical detection** — a future-facing module for quantum-assisted inference over high-dimensional feature spaces, drawing on QML foundations and variational quantum algorithms, but not assumed here to be operationally mature at enterprise SOC scale [17,18,27,31]

 doi:10.20944/preprints202604.1363.v1

6.4. Alerting and Response

Detection outputs are routed through four channels corresponding to standard SOC triage and response pipelines:

- **SIEM integration** — forwarding correlated events for retention and analyst review
- **SOAR automation** — playbook-driven containment (certificate revocation, connection blocking, cryptographic agility triggers)
- **Analyst dashboard** — triage and investigation UI scoped to quantum-attack indicators
- **Incident tickets** — case management handoff with structured indicator metadata

6.5. Integration with PQC Migration

Detection must co-evolve with cryptographic migration. As organizations adopt ML-KEM, ML-DSA, and SLH-DSA [7–9], the detection architecture is instrumented to monitor four migration-specific concerns:

- Hybrid handshake failures
- Algorithm downgrade attempts
- Certificate chain inconsistencies
- PQC fallback events

The migration window exposes the largest PQC attack surface: hybrid TLS deployments introduce new negotiation paths [14], PQC certificate rollouts create enumeration opportunities [22,32], and enterprise adoption runs on timelines measured in years rather than quarters [38]. Integrating detection into the PQC migration program ensures defenders gain visibility as the environment changes, rather than after the fact.

6.6. Scalability and Deployment Considerations

Operational deployment at enterprise scale must address four engineering concerns that determine the architecture's feasibility outside a laboratory setting:

- **Cloud-native telemetry pipelines** — stream-based ingestion compatible with Kafka-, Kinesis-, or Pub/Sub-style backbones, with schemas aligned to standardized structured-logging formats
- **Efficient storage of high-volume TLS metadata** — aggressive sampling, aggregation, and tiered retention to contain storage cost while preserving long-tail forensic value
- **Privacy-preserving CT log monitoring** — aggregate-only access patterns that avoid per-certificate lookup amplification, protecting against both metadata leakage and disproportionate CT-log strain
- **Low-overhead endpoint cryptographic telemetry** — agent-based collection that imposes negligible compute and network overhead on production endpoints, with opt-in instrumentation

Together, these considerations are intended to improve the feasibility of deploying QEADT-1 at enterprise scale rather than leaving it purely as an architectural concept.

7. Case Studies

The following case studies are synthetic engineering scenarios designed to exercise the indicator-to-telemetry-to-technique logic of QEADT-1; they are not presented as reconstructed real-world incidents with ground truth.

7.1. PQC Downgrade Attempt

Consider a mid-sized enterprise completing its PQC migration pilot, in which a subset of servers advertise hybrid key exchange combining X25519 with ML-KEM-768 (FIPS 203 [7]). An adversary on the network path between a PQC-capable client and server injects modified ClientHello messages, stripping the hybrid key share and forcing the negotiation to fall back to X25519 alone. From the

 doi:10.20944/preprints202604.1363.v1

defender's perspective, the attack surfaces through three concurrent indicators (Section 4.3): Hybrid Negotiation Failures spike on otherwise-PQC-capable endpoints; Handshake Anomalies register an elevated retry rate; and PQC Fallback Events appear in the PQC negotiation logs. The required telemetry spans TLS handshake logs and PQC negotiation logs (Section 4.4). Rule-Based heuristics catch the pattern via signature matches on the suppressed supported_groups extension, while Correlation-based detection confirms the attack by tying the fallback events across many clients to a small number of intermediate hops. The alert is routed through SOAR automation (Section 6.4), triggering an automated advisory to PKI operators and a playbook that quarantines the affected network segments. This scenario demonstrates that detection does not require post-quantum cryptanalysis capabilities on the defender's part; it requires telemetry discipline and correlation across PQC negotiation events during the migration window [13,14].

7.2. Quantum-Optimized Scanning

Consider a reconnaissance campaign enumerating TLS endpoints and hybrid-cryptographic misconfigurations across a target's public attack surface. The adversary is assumed to combine classical Internet-wide scanning techniques [23] with quantum-inspired optimization [19] to prioritize the probe order — plausibly exploiting structure in the target address space to reach high-value endpoints faster than a uniform scan. From the defender's perspective, two indicators fire (Section 4.3): Low-Entropy Scanning Bursts register in network-flow metadata (address-space entropy is abnormally low relative to brute-force baselines), and CT Log Spikes appear as the adversary fingerprints certificate issuance across the target's domain portfolio. Required telemetry (Section 4.4) is network flow metadata and CT logs. Statistical anomaly detection thresholds the entropy deviation, ML-based behavioral models classify the scan pattern against known reconnaissance profiles, and Correlation-based detection links the scanning activity to the downstream CT queries — producing a higher-confidence Reconnaissance alert than any single-source indicator would support. The alert is forwarded via SIEM integration to a dashboard scoped to quantum-attack indicators (Section 6.4).

7.3. HNDL Certificate Harvesting

Consider an adversary executing a sustained HNDL campaign against the encrypted communications of a sector with long-retention confidentiality requirements — for example, healthcare or satellite communications, which recent temporal risk models identify as particularly exposed in the event of delayed migration [15]. The campaign has two complementary arms: (i) bulk collection of TLS-encrypted traffic for later decryption, and (ii) enumeration of the target's certificate portfolio via Certificate Transparency logs [22], to identify which key exchanges are worth storing. From the defender's perspective, this activity surfaces through five indicators (Section 4.3): CT Log Spikes from the CT queries, Large-Scale Certificate Enumeration matching a known target's domain structure, Bulk Ciphertext Collection Events in network-flow metadata, Unusual Certificate Lifecycle Anomalies as the adversary correlates renewal cadence with retention windows, and Low-Entropy Scanning Bursts during the enumeration phase. Required telemetry spans CT logs, network flows, and PKI lifecycle events (Section 4.4). Correlation-based detection is the decisive technique: no single indicator distinguishes HNDL from benign certificate monitoring, but the joint activation across CT, TLS, and network-flow planes produces a high-confidence HNDL alert. Data-classification context (Section 3.3) prioritizes the alert based on the confidentiality lifetime of the targeted data, and the alert is delivered through the Analyst Dashboard with structured indicator metadata for forensic investigation [16].

 doi:10.20944/preprints202604.1363.v1

8. Discussion

8.1. Limitations

Four limitations bound the scope of QEADT-1 and frame how the taxonomy should be interpreted. First, cryptographically relevant quantum computers (CRQCs) capable of breaking modern deployed public-key cryptography at operational scale do not yet exist, and no real CRQC-enabled cyber attacks have been empirically observed. The taxonomy, therefore, classifies quantum-enabled attack classes that are either (i) capability-founded today through quantum-assisted inference and quantum-inspired optimization [17–19], (ii) grounded in observable transition-era behaviors and strategic threat models, as with HNDL and downgrade-oriented migration abuse [13–16], or (iii) principled forward-looking projections whose capability foundations are established even if scaled empirical cyber demonstrations remain limited. The Side-Channel and Evasion classes (Sections 3.4, 4.1) fall into the third category and are scoped accordingly.

Second, the case studies in Section 7 are synthetic, reflecting the absence of public datasets containing labeled quantum-enabled attack traces; existing network-intrusion-detection datasets surveyed in [30] cover classical threat traces only, and adjacent simulation-based work in quantum-era security operations has adopted the same rigorous-limitations-first framing [37]. Each scenario is constructed to exercise the indicator-to-telemetry-to-technique path the taxonomy prescribes, but none derives from a real incident with ground truth. This limits the empirical strength of the framework at present and motivates the benchmark-dataset initiative discussed in Section 8.2. Synthetic approximations are the best available baseline in the pre-CRQC era, but defenders should treat detection rates on synthetic data as upper bounds rather than operational guarantees.

Third, the telemetry assumptions in Sections 3.2 and 4.4 presume that defenders can ingest TLS handshake logs, network flows, CT logs, PKI lifecycle events, PQC negotiation logs, and endpoint cryptographic telemetry. Real enterprise deployments reveal significant heterogeneity across vendors, services, and geographies [11,13,21], and some environments may lack entire telemetry classes (e.g., air-gapped networks, consumer IoT). The taxonomy remains valid in such environments, but the applicable detection signatures narrow to the subset supported by the available telemetry.

Fourth, the Hybrid Quantum-Classical detection module in Section 6.3 is forward-facing. The underlying quantum-kernel feature-space methods are well-established [17,18] and preliminary intrusion-detection studies exist [20], but deploying a hybrid quantum-classical detector at enterprise SOC scale is not yet practical. QEADT-1 includes this module to make the taxonomy extensible as the capability matures, not to assert that such detectors are operationally ready today.

8.2. Future Work

Four lines of future work follow directly from the taxonomy and its limitations. The first and most consequential is a public benchmark dataset, tentatively named Q-ATTACK-TRACE-1, consisting of labeled telemetry traces for each of the six attack classes. Such a dataset would include synthetic and emulated captures of PQC downgrade attempts, quantum-optimized scanning traffic, HNDL certificate-harvesting campaigns, and quantum-inspired evasion attempts against common ML-based IDS. The classical NIDS dataset literature surveyed in [30] provides precedent for the structure and labeling discipline such a benchmark should adopt, and a phased validation roadmap of the kind proposed for adjacent quantum-era security capabilities [37] — proceeding from synthetic baselines, through small-scale empirical testbeds, to adversarial red-team evaluation — could serve as a structural template. A shared benchmark would enable empirical comparison of detection techniques across research groups and elevate the pre-CRQC detection literature above the current state of isolated, non-comparable studies.

The second line is quantum-assisted detection itself. The Hybrid Quantum-Classical module in Section 6.3 remains forward-facing today, but as quantum feature-space methods [17,18] mature beyond proof-of-concept and into accessible tooling, empirical comparison of classical and quantum-

 doi:10.20944/preprints202604.1363.v1

assisted detectors on the Q-ATTACK-TRACE-1 benchmark would answer the open question of whether quantum-era defenders gain an asymmetric detection advantage against quantum-era adversaries. Preliminary intrusion-detection work with quantum models [20] suggests the answer is non-trivial.

The third line is PQC telemetry standardization. The architecture in Section 6 assumes defenders can emit structured PQC negotiation logs, hybrid handshake outcomes, and fallback events, but no industry standard currently defines the schema or semantics of such logs. NIST's transition guidance [11] supports the broader need for transition visibility but does not prescribe a concrete enterprise PQC telemetry specification. A standardized PQC telemetry schema — ideally aligned with existing structured-log formats — would close the gap between architectural recommendations and deployable detection.

The fourth line is a scope extension. QEADT-1 is deliberately scoped to enterprise networks, federal systems, and critical infrastructure, but adjacent domains have distinct observability surfaces and attack mechanisms worth taxonomizing separately — for example, distributed-ledger environments expose transit-phase attack windows during transaction propagation that have no analog in classical enterprise telemetry [39]. A family of domain-specific detection taxonomies, cross-walked to a common indicator and telemetry vocabulary, would be a natural outgrowth of the framework proposed here.

9. Conclusions

This paper has introduced QEADT-1, a systems-level detection taxonomy for quantum-enabled cyber attacks against classical and PQC-transitioning infrastructure during the pre-CRQC era. The taxonomy is organized into five hierarchical levels — attack class, mechanism, observable indicator, required telemetry, and detection technique (Figure 1) — and is conceptually operationalized through a six-by-twenty detection matrix (Figure 2, Table 1) and a four-stage monitoring architecture with five parallel detection modules (Figure 3). Three synthetic case studies (Section 7) illustrate how the taxonomy translates into end-to-end detection workflows for PQC downgrade attempts, quantum-optimized reconnaissance, and HNDL certificate harvesting.

The practical contribution of QEADT-1 is to propose a shared vocabulary and instrumentation checklist that SOC operators, PQC migration teams, and standards bodies can use for pre-CRQC threat monitoring and capability planning. SOC operators can use Table 1 and the Detection Matrix to scope telemetry coverage against a prioritized subset of attack classes. PQC migration teams can use the architecture in Section 6, and particularly the PQC-Migration integration in Section 6.5, to couple detection into their hybrid-cryptography rollouts rather than treating detection as an orthogonal downstream concern. Standards bodies — including NIST, NSA, and ETSI communities that have already published foundational PQC transition guidance [10,11,25,26] — could use the telemetry layer as input toward a standardized PQC monitoring schema, which Section 8.2 identifies as one of the most consequential open problems. The pre-CRQC window is finite, and operational detection capability must be built before cryptographically relevant quantum computers arrive, not after. QEADT-1 is a step toward closing that gap.

Author Contributions: Conceptualization, investigation, methodology, writing—original draft, writing—review and editing, R.E.C. The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The author acknowledges the broader post-quantum cryptography research community, including NIST, NSA, ETSI, and academic contributors whose foundational standards and analyses informed this taxonomy.

 doi:10.20944/preprints202604.1363.v1

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CBOM	Cryptographic Bill of Materials
CNSA	Commercial National Security Algorithm Suite
CRQC	Cryptographically Relevant Quantum Computer
CT	Certificate Transparency
DoD	Department of Defense
ECC	Elliptic Curve Cryptography
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
FTQC	Fault-Tolerant Quantum Computer
HNDL	Harvest-Now, Decrypt-Later
HSM	Hardware Security Module
IDS	Intrusion Detection System
KEM	Key Encapsulation Mechanism
ML-DSA	Module-Lattice Digital Signature Algorithm
ML-KEM	Module-Lattice Key Encapsulation Mechanism
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QEADT-1	Quantum-Enabled Attack Detection Taxonomy (version 1)
QKD	Quantum Key Distribution
QML	Quantum Machine Learning
RSA	Rivest–Shamir–Adleman
SIEM	Security Information and Event Management
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
TLS	Transport Layer Security
VQA	Variational Quantum Algorithm
XMSS	eXtended Merkle Signature Scheme
ZTA	Zero Trust Architecture

References

1. Shor, P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 1994, pp. 124–134.
2. Grover, L. K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), ACM, 1996, pp. 212–219.
3. Bernstein, D. J.; Lange, T. Post-Quantum Cryptography. Nature 2017, 549, 188–194. https://doi.org/10.1038/nature23461.
4. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy 2018, 16 (5), 38–41. https://doi.org/10.1109/MSP.2018.3761723.
5. Gidney, C.; Ekerå, M. How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. Quantum 2021, 5, 433. https://doi.org/10.22331/q-2021-04-15-433.
6. Barrett-Danes, F.; Ahmad, F. Quantum Computing and Cybersecurity: A Rigorous Systematic Review of Emerging Threats, Post-Quantum Solutions, and Research Directions (2019–2024). Discover Applied Sciences 2025, 7, 1083. https://doi.org/10.1007/s42452-025-07322-5.

 doi:10.20944/preprints202604.1363.v1

7. National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203, August 2024. https://doi.org/10.6028/NIST.FIPS.203.
8. National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204, August 2024. https://doi.org/10.6028/NIST.FIPS.204.
9. National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard. FIPS 205, August 2024. https://doi.org/10.6028/NIST.FIPS.205.
10. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Liu, Y.-K.; Miller, C.; Moody, D.; Peralta, R.; Perlner, R.; Robinson, A.; Smith-Tone, D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Internal Report 8413, 2022. https://doi.org/10.6028/NIST.IR.8413.
11. National Institute of Standards and Technology. Transition to Post-Quantum Cryptography Standards. NIST Internal Report 8547, Initial Public Draft, November 2024. https://doi.org/10.6028/NIST.IR.8547.ipd.
12. Hülsing, A.; Butin, D.; Gazdag, S.-L.; Rijneveld, J.; Mohaisen, A. XMSS: eXtended Merkle Signature Scheme. Internet Engineering Task Force RFC 8391, May 2018. https://doi.org/10.17487/RFC8391.
13. Paquin, C.; Stebila, D.; Tamvada, G. Benchmarking Post-Quantum Cryptography in TLS. In Post-Quantum Cryptography (PQCrypto 2020), Lecture Notes in Computer Science, vol. 12100; Springer: Cham, 2020; pp. 72–91. https://doi.org/10.1007/978-3-030-44223-1_5.
14. Bindel, N.; Brendel, J.; Fischlin, M.; Goncalves, B.; Stebila, D. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In Post-Quantum Cryptography (PQCrypto 2019), Lecture Notes in Computer Science, vol. 11505; Springer: Cham, 2019; pp. 206–226. https://doi.org/10.1007/978-3-030-25510-7_12.
15. Kagai, F.; Branch, P.; But, J.; Allen, R. Harvest-Now, Decrypt-Later: A Temporal Cybersecurity Risk in the Quantum Transition. Telecom 2025, 6 (4), 100. https://doi.org/10.3390/telecom6040100.
16. Wallden, P.; Kashefi, E. Cyber Security in the Quantum Era. Communications of the ACM 2019, 62 (4), 120. https://doi.org/10.1145/3241037.
17. Schuld, M.; Killoran, N. Quantum Machine Learning in Feature Hilbert Spaces. Physical Review Letters 2019, 122 (4), 040504. https://doi.org/10.1103/PhysRevLett.122.040504.
18. Havlíček, V.; Córcoles, A. D.; Temme, K.; Harrow, A. W.; Kandala, A.; Chow, J. M.; Gambetta, J. M. Supervised Learning with Quantum-Enhanced Feature Spaces. Nature 2019, 567, 209–212. https://doi.org/10.1038/s41586-019-0980-2.
19. Dunjko, V.; Briegel, H. J. Machine Learning & Artificial Intelligence in the Quantum Domain: A Review of Recent Progress. Reports on Progress in Physics 2018, 81 (7), 074001. https://doi.org/10.1088/1361-6633/aab406.
20. Payares, E. D.; Martinez-Santos, J. C. Quantum Machine Learning for Intrusion Detection of Distributed Denial of Service Attacks: A Comparative Overview. In Proceedings of SPIE 11699, Quantum Computing, Communication, and Simulation, 116990B, 2021. https://doi.org/10.1117/12.2593297.
21. Holz, R.; Amann, J.; Mehani, O.; Wachs, M.; Kaafar, M. A. TLS in the Wild: An Internet-Wide Analysis of TLS-Based Protocols for Electronic Communication. In Proceedings of the Network and Distributed System Security Symposium (NDSS), Internet Society, 2016. https://doi.org/10.14722/ndss.2016.23055.
22. Scheitle, Q.; Gasser, O.; Nolte, T.; Amann, J.; Brent, L.; Carle, G.; Holz, R.; Schmidt, T. C.; Wählisch, M. The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem. In Proceedings of the Internet Measurement Conference (IMC), ACM, 2018; pp. 343–349. https://doi.org/10.1145/3278532.3278539.
23. Durumeric, Z.; Wustrow, E.; Halderman, J. A. ZMap: Fast Internet-Wide Scanning and Its Security Applications. In Proceedings of the 22nd USENIX Security Symposium, USENIX Association, 2013; pp. 605–620.
24. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force RFC 8446, August 2018. https://doi.org/10.17487/RFC8446.
25. National Security Agency. Announcing the Commercial National Security Algorithm Suite 2.0. NSA Cybersecurity Advisory, September 2022. Available online:

 doi:10.20944/preprints202604.1363.v1

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF (accessed on 19 April 2026).

26. European Telecommunications Standards Institute. Quantum-Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. ETSI White Paper No. 8, 2015.
27. Biamonte, J.; Wittek, P.; Pancotti, N.; Rebentrost, P.; Wiebe, N.; Lloyd, S. Quantum Machine Learning. Nature 2017, 549, 195–202. https://doi.org/10.1038/nature23474.
28. Sommer, R.; Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010; pp. 305–316. https://doi.org/10.1109/SP.2010.25.
29. Buczak, A. L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials 2016, 18 (2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502.
30. Ring, M.; Wunderlich, S.; Scheuring, D.; Landes, D.; Hotho, A. A Survey of Network-Based Intrusion Detection Data Sets. Computers & Security 2019, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005.
31. Cerezo, M.; Arrasmith, A.; Babbush, R.; Benjamin, S. C.; Endo, S.; Fujii, K.; McClean, J. R.; Mitarai, K.; Yuan, X.; Cincio, L.; Coles, P. J. Variational Quantum Algorithms. Nature Reviews Physics 2021, 3, 625–644. https://doi.org/10.1038/s42254-021-00348-9.
32. Kampanakis, P.; Panburana, P.; Daw, E.; Van Geest, D. The Viability of Post-Quantum X.509 Certificates. IACR Cryptology ePrint Archive, Report 2018/063, 2018. Available online: https://eprint.iacr.org/2018/063 (accessed on 19 April 2026).
33. Mosca, M.; Piani, M. 2024 Quantum Threat Timeline Report. Global Risk Institute: Toronto, ON, Canada, December 2024. Available online: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/ (accessed on 19 April 2026).
34. The White House. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10). Washington, DC, USA, May 4, 2022. Available online: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (accessed on 19 April 2026).
35. Office of Management and Budget. Memorandum M-23-02: Migrating to Post-Quantum Cryptography. Executive Office of the President, Washington, DC, USA, November 18, 2022. Available online: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (accessed on 19 April 2026).
36. Crockett, E.; Paquin, C.; Stebila, D. Prototyping Post-Quantum and Hybrid Key Exchange and Authentication in TLS and SSH. IACR Cryptology ePrint Archive, Report 2019/858, 2019. Available online: https://eprint.iacr.org/2019/858 (accessed on 19 April 2026).
37. Campbell, R., Sr. A Simulation Study on the Theoretical Potential of Quantum-Enhanced Federated Security Operations. Sensors 2025, 25 (19), 5949. https://doi.org/10.3390/s25195949.
38. Campbell, R. Enterprise Migration to Post-Quantum Cryptography: Timeline Analysis and Strategic Frameworks. Computers 2026, 15, 9. https://doi.org/10.3390/computers15010009.
39. Campbell, R. Hybrid Post-Quantum Signatures for Bitcoin and Ethereum: A Protocol-Level Integration Strategy. The Journal of the British Blockchain Association 2026, 9 (1), 2. https://doi.org/10.31585/jbba-9-1-(2)2026.
40. National Institute of Standards and Technology. Recommendation for Stateful Hash-Based Signature Schemes. NIST Special Publication 800-208, October 2020. https://doi.org/10.6028/NIST.SP.800-208.