Quantum Computing and Offensive Security: Analysis of Emerging Threats, Attack Vectors, and Defensive Frameworks

Krishna Agarwal, CEO
Adversary Holdings Private Limited
research@adversaryholdings.com

The emergence of quantum computing represents one of the most significant paradigm shifts in the history of computation, with profound implications for offensive security and cyber warfare. This comprehensive research paper presents a systematic analysis of quantum-enabled offensive capabilities, novel attack vectors targeting quantum systems themselves, and the evolving threat landscape at the intersection of quantum computing and artificial intelligence. We introduce the Q-THREAT Framework, a novel temporal risk assessment model that quantifies the "Harvest Now, Decrypt Later" threat across different data confidentiality lifetimes and sectoral exposures. This research synthesizes and categorizes recently documented attack vectors including quantum Rowhammer exploits, timing-based side-channel vulnerabilities in cloud quantum services, and multi-tenant quantum system intrusions. Recent research demonstrates that current quantum cloud platforms from major providers including IBM, Rigetti, and others exhibit significant security vulnerabilities that could be exploited by adversaries to compromise computational integrity, extract sensitive circuit information, and disrupt quantum computations. Furthermore, we analyze the convergence of quantum computing and artificial intelligence as a force multiplier for offensive cyber operations. We present evidence that quantum machine learning algorithms can demonstrate competitive or superior performance in certain cybersecurity applications compared to classical approaches in controlled experimental settings, with recent studies reporting high accuracies in tasks such as malware detection and intrusion detection on benchmark datasets. Our analysis of nation-state quantum programs reveals an accelerating global quantum arms race with significant implications for national security. Based on our findings, we propose a comprehensive defensive framework incorporating post-quantum cryptographic standards, crypto-agility principles, and quantum-safe architectural patterns. This research contributes to the nascent field of quantum cybersecurity by establishing foundational threat models, identifying critical research gaps, and providing actionable recommendations for organizations preparing for the quantum era.

Cyber Warfare, Harvest Now Decrypt Later, Offensive Security, Post-Quantum Cryptography

I. Introduction

A. Research Motivation

Quantum computing has transitioned from theoretical curiosity to practical reality, with commercial quantum computers now available through cloud platforms from IBM, Google, Amazon, Microsoft, and numerous other providers [1]. While much attention has focused on quantum computing's potential to break existing cryptographic systems, significantly less research has examined the offensive security implications of quantum technologies, including vulnerabilities within quantum systems themselves and the convergence of quantum computing with artificial intelligence for cyber warfare applications.

The stakes are exceptionally high. Modern cryptography underpins virtually every aspect of digital security, spanning financial transactions and secure communications to critical infrastructure control and national defense systems. The asymmetric encryption schemes that protect these systems, including RSA and Elliptic Curve Cryptography, derive their security from mathematical problems that quantum computers can solve exponentially faster than classical computers using Shor's algorithm [2].

Recent advances have dramatically accelerated quantum threat timelines. Historical estimates from Beauregard's 2003 circuit suggested 4,099 logical qubits (2n+3 formula) for factoring RSA-2048[3]. However, recent optimization by Gidney (2025) reduced this to between 1,399-1,730 logical qubits using magic state cultivation techniques, with physical qubit estimates of approximately 1 million depending on architectural assumptions[4]. These breakthroughs, achieved through algorithmic optimizations and error correction advances, suggest that cryptographically relevant quantum computers may arrive sooner than previously anticipated.

Perhaps more concerning is the “Harvest Now, Decrypt Later” (HNDL) threat model, in which adversaries collect encrypted data today with the explicit intention of decrypting it once quantum capabilities become available[5]. This temporal asymmetry transforms quantum computing from a future threat into an immediate security crisis for any organization handling data with long confidentiality lifetimes.

This temporal asymmetry transforms quantum computing from a future threat into an immediate security crisis for any organization handling data with long confidentiality lifetimes.

B. Research Questions

This research addresses the following fundamental questions:

1. What novel attack vectors emerge from quantum computing technologies themselves? Beyond the well-documented threat to cryptography, what vulnerabilities exist in quantum hardware, quantum cloud services, and the classical-quantum interface?

2. How can the HNDL threat be quantified and modeled? What framework can assess temporal risk across different sectors and data types with varying confidentiality lifetimes?

3. What are the offensive security implications of quantum-AI convergence? How might quantum machine learning enhance adversarial capabilities?

4. What defensive measures are effective against quantum-enabled threats? How should organizations prioritize their post-quantum migration efforts?

C. Contributions

Primary Contributions of This Research

1. Q-THREAT Framework: We introduce a novel temporal risk assessment model that quantifies HNDL exposure across sectors based on data confidentiality lifetimes, adversary capabilities, and migration timelines.

2. Attack Vector Taxonomy: We present a comprehensive taxonomy of offensive security attacks targeting quantum systems themselves, including quantum Rowhammer, timing side-channels, and multi-tenant exploits.

3. Quantum-AI Threat Analysis: We analyze the convergence of quantum computing and artificial intelligence as a force multiplier for offensive operations, presenting empirical evidence of enhanced attack effectiveness.

4. Defensive Framework: We propose actionable defensive strategies incorporating NIST postquantum standards, crypto-agility principles, and sector-specific migration priorities.

II. BACKGROUND AND RELATED WORK

A. Quantum Computing Fundamentals

Quantum computers leverage the principles of quantum mechanics, superposition, entanglement, and interference to perform computations that would be infeasible for classical computers. Unlike classical bits that exist in definite states of 0 or 1, quantum bits can exist in superpositions of both states simultaneously, enabling exponential parallelism in certain computational tasks [5].

The current era of quantum computing is characterized as the Noisy Intermediate-Scale Quantum (NISQ) era, featuring quantum processors with hundreds to thousands of qubits but limited by decoherence and gate errors[6]. Despite these limitations, NISQ devices have demonstrated quantum advantage in specific tasks and are increasingly accessible through cloud platforms.

TABLE I. COMPARISON OF MAJOR QUANTUM COMPUTING PLATFORMS

Provider	Qubit Technology	Max Qubits (2026)	Cloud Access	Multi Tenant
IBM Quantum	Superconducting	1,121 (Condor)	Yes	Yes
Google Quantum	Superconducting	105 (Willow)	Limited	No
IonQ	Trapped Ion	64	Yes	Yes
Rigetti	Superconducting	84 (Ankaa-3)	Yes	Yes
D-Wave	Quantum Annealing	5,000+	Yes	Yes

Google's Willow chip (announced December 2024) demonstrated below-threshold error correction, achieving exponential error reduction as logical qubit size increases, a fundamental milestone for scalable quantum computing

B. Quantum Algorithms for Cryptanalysis

Two quantum algorithms pose fundamental threats to modern cryptography:

Shor's Algorithm

Developed by Peter Shor in 1994, this algorithm efficiently solves the integer factorization and discrete logarithm problems in polynomial time [7]. The algorithm reduces the complexity of factoring an n-bit integer from sub-exponential time (approximately $O(e^{\sqrt[3]{(\ln n)^2}})$ for the General Number Field Sieve) to polynomial time $O((\log n)^3)$.

$$|\psi\rangle = \sum_{a=0}^{q-1} |a\rangle |x^a \bmod N\rangle \quad (1)$$

Equation (1) represents the quantum state after modular exponentiation in Shor's algorithm, where q is a power of 2, x is a randomly chosen base, and N is the number to be factored. The quantum Fourier transform is then applied to extract the period, which yields the factors through continued fraction expansion.

Grover's Algorithm

Proposed by Lov Grover in 1996, this algorithm provides a quadratic speedup for unstructured search problems [8]. For a search space of size N, Grover's algorithm finds the target in $O(\sqrt{N})$ queries compared to $O(N)$ for classical search. Applied to cryptography, this effectively halves the security of symmetric ciphers, AES-256 provides only 128-bit equivalent security against quantum adversaries.

C. Related Research

Prior research on quantum computing security has primarily focused on post-quantum cryptographic algorithms designed to resist quantum attacks[9]. The NIST Post-Quantum Cryptography Standardization process, initiated in 2016, has evaluated 82 algorithms from 25 countries, resulting in the standardization of ML-KEM, ML-DSA, SLH-DSA, and FN-DSA[10].

Quantum system security research has been more limited. Recent work by Choudhury et al. demonstrated crosstalk-based side-channel attacks in multi-tenant NISQ computers[11]. Almaguer-Angeles et al. (2025) demonstrated the first quantum Rowhammer attack on IBM quantum computers[12]. Lu et al. (2024) identified timing-based side-channel vulnerabilities in IBM's quantum cloud service[13]. Erata et al. (2024) demonstrated power side-channel attacks capable of reconstructing quantum circuits from controller electronics[14].

III. Methodology

This research employs a systematic literature review methodology combined with quantitative risk modeling to analyze the quantum threat landscape.

A. Literature Review Process

Search Strategy: We conducted systematic searches across academic databases (IEEE Xplore, ACM Digital Library, arXiv, Springer) and industry sources using keywords: "quantum computing security," "quantum cryptanalysis," "post-quantum cryptography," "quantum side-channel attacks," "NISQ vulnerabilities," and "quantum machine learning cybersecurity."

Inclusion Criteria: Publications from 2016-2026 focusing on quantum computing security, offensive capabilities,

cryptanalysis, side-channel attacks, and defensive frameworks. We prioritized peer-reviewed conference papers, journal articles, and preprints from reputable institutions.

Exclusion Criteria: Publications in non-English languages, purely theoretical works without security implications, and works lacking technical depth or reproducibility.

Quality Assessment: Each source was evaluated for technical rigor, reproducibility, citation quality, and contribution to the field.

B. Q-THREAT Framework Development

The Q-THREAT (Quantum Temporal Hazard Risk Evaluation and Assessment Tool) framework was developed through:

1. Analysis of existing risk assessment methodologies.
2. Integration of temporal dimensions specific to HNDL threats.
3. Consultation of industry reports on data confidentiality lifetimes.
4. Mathematical formalization of risk components.
5. Application to representative sectoral case studies.

C. Limitations of This Study

This research acknowledges several limitations:

- The Q-THREAT framework is a theoretical model requiring empirical validation through real-world case studies.
- Our literature review is limited to English-language publications accessible through academic databases.
- The rapid evolution of quantum technology means findings may date quickly as capabilities advance.
- We lack access to classified nation-state quantum programs, limiting our analysis to publicly available information.
- Quantum machine learning assessments are based on published benchmark results in controlled settings, not production deployments.

IV. THE QUANTUM THREAT LANDSCAPE

A. Harvest Now, Decrypt Later (HNDL)

The HNDL threat model represents a fundamental shift in cybersecurity risk assessment. Unlike conventional threats that materialize at the moment of attack, HNDL operates across temporal dimensions, weaponizing the gap between data collection and future decryption capability [15].

HNDL Adversarial Model Definition

An HNDL adversary is a persistent, resource-accumulating entity operating within the temporal dimension of communication security. The adversary possesses three evolving resources:

- Collection capability: the capacity to intercept and store ciphertexts at scale.

- Decryption capability: latent computational power from anticipated quantum advances.

- Temporal horizon: strategic patience enabling deferred exploitation.

The HNDL attack proceeds in three phases:

- Harvest Phase: Adversaries opportunistically collect encrypted traffic from communication channels, archival repositories, and distributed ledgers.
- Storage Phase: Harvested data is archived for years or decades, often in government repositories or private cloud environments.
- Decryption Phase: Once quantum computers capable of running Shor's algorithm become available, stored ciphertext is decrypted retrospectively.

TABLE II. SECTORAL EXPOSURE TO HNDL ATTACKS BY DATA CONFIDENTIALITY LIFETIME

Data Type	Confidentiality Lifetime	Exposure Level	Primary Risk
Financial Transactions	Months–1 year	Low	Transactional fraud
Corporate IP/Contracts	3-7 years	Medium	Competitive disadvantage
Personal Health Records	10-30 years	High	Privacy violation
State Intelligence	30+ years	Critical	National security compromise

B. Quantum Cryptanalysis Capabilities

Recent advances have significantly refined estimates of the resources required for quantum cryptanalysis. Table III presents current estimates for breaking major cryptographic standards:

TABLE III. QUANTUM RESOURCES REQUIRED FOR CRYPTANALYSIS (2026 ESTIMATES)

Target	Logical Qubits	Physical Qubits	Runtime	Source
RSA-2048	$\sim$1,730	$\sim$1 million	$\sim$1 week	Gidney (2025)[4]
ECC-256	$\sim$1,500	$\sim$13 million	$\sim$24 hours	Gheorghiu & Mosca (2019)[17]
AES-256 (Grover)	$\sim$6,600	Impractical	Infeasible	NIST[18]

These estimates reveal that ECC-256 may be the first widely-deployed cryptographic standard to fall, requiring fewer logical qubits than comparably-secure RSA keys. Organizations relying on elliptic curve cryptography should prioritize migration to post-quantum alternatives.

C. Nation-State Quantum Programs

A global quantum arms race is underway, with major powers investing billions in quantum computing research and development. The FBI has identified economic espionage targeting quantum technologies as a critical national security concern[18].

China's Five-Year Plan explicitly identifies quantum computing as a strategic technology target, alongside semiconductors, artificial intelligence, and biotechnology[18]. In March 2023, China and Russia agreed to deepen scientific cooperation, including military technology research. The implications for offensive security are profound. State-backed Advanced Persistent Threat (APT) groups may gain access to quantum computing capabilities before they are commercially available.

Security analysts believe nation-state actors are already engaged in widespread HNDL data collection, anticipating future quantum decryption capabilities[19]. The “Q-Day” scenario, when a nation achieves cryptographically-relevant quantum computing and potentially keeps it secret, represents an existential threat to encrypted communications.

V. NOVEL ATTACK VECTORS IN QUANTUM SYSTEMS

A. Quantum Cloud Security Vulnerabilities

Quantum cloud platforms have democratized access to quantum computing but introduced novel security vulnerabilities. Recent research by multiple teams reveals significant risks across three architectural layers.

1. Classical-Quantum Interface Vulnerabilities: The classical-quantum interface connects isolated qubits with room-temperature control electronics. Research by Mustafa and Köse (2024) demonstrated that Single Flux Quantum (SFQ) circuits exhibit significant side-channel leakage through bias current variations[20]. An insider with access to room-temperature electronics can potentially decode internal signals and reconstruct quantum circuits. Research by Erata et al. (2024) demonstrated that power side-channel attacks on quantum computer controllers can recover quantum circuits by measuring power consumption of control electronics[14]. Their work showed that attackers with access to power traces can

reconstruct secret quantum circuits through both per-channel and total power measurement approaches.

2. Multi-Tenant Isolation Failures: Most commercial quantum cloud platforms employ multi-tenancy, allowing multiple users to share quantum hardware. This architecture introduces crosstalk vulnerabilities where operations by one user affect computations of others sharing the same device[11].

B. Quantum Rowhammer Attacks

In 2025, researchers demonstrated the first quantum Rowhammer (QubitHammer) attacks on commercial quantum computers, including the work by Almaguer-Angeles et al.[12] and extensive analysis by Tan et al.[21]. Campbell (2025) demonstrated a Clifford-only Quantum Rowhammer attack using just X and CNOT gates that injects faults on IBM's Eagle processors[22].

Attack Mechanism: Quantum Rowhammer exploits the unintended interactions (crosstalk) between neighboring qubits in superconducting quantum processors. By repeatedly applying quantum gates near a target qubit, attackers can induce sufficient crosstalk to flip the target's state. Experiments on IBM's 127-qubit Eagle processors demonstrated successful qubit flipping with high probability using controlled-NOT (CNOT) gate sequences.

The implications are severe. In multi-tenant environments, a malicious user could corrupt another tenant's computation results without direct access to their qubits. QubitHammer attacks achieve variational distance up to 0.938 from the expected outcome, demonstrating their potential to significantly degrade victim computation[21]. Research by Das et al. (2024) showed that bit flips in FPGA control electronics can cause Total Variation Distance increases as high as approximately 200%, demonstrating substantial degradation of quantum computation[23].

C. Timing Side-Channel Attacks

Lu et al. (2024) demonstrated timing-based side-channel attacks against IBM's quantum cloud service that can identify the specific quantum processor being used with just 10 measurements[13]. More concerning, their attack could reconstruct Grover oracle circuits with as few as 500 measurements.

TABLE IV. TIMING SIDE-CHANNEL ATTACK EFFECTIVENESS ON IBM QUANTUM CLOUD

Attack Type	Target Information	Minimum Measurements	Success Rate
Quantum Processor Identification	Hardware backend	10	100%
User Circuit Identification	Circuit type	1–18,712	60-100%
Circuit Oracle Identification	Oracle structure	500–20M	Variable

D. Multi-Tenant Exploitation

Multi-tenant quantum cloud systems are vulnerable to multiple exploitation vectors:

- Crosstalk Channel Attacks: Choudhury et al. (2024) demonstrated that crosstalk in multi-tenant NISQ computers can be exploited to extract unauthorized information about victim circuits, including the number of CNOT gates[11]. Their graph-based model achieved accurate circuit identification using crosstalk signatures.

- Reset Gate Vulnerabilities: Research by Mi et al. (2022) showed that reset operations in NISQ computers do not fully clear data, enabling information leakage across reset gates on shared qubits[24]. This vulnerability allows adversaries to eavesdrop on previous computations.

- SWAP Path Attacks: Lee et al. (2025) introduced SWAP attacks that exploit the SWAP path in multi-tenant quantum cloud systems[25]. These attacks can be categorized as Active SWAP Attacks (disrupting Grover's algorithm) or Passive SWAP Attacks (stealing circuit info from Simon's algorithm). By positioning qubits strategically, attackers can disrupt victim circuits and reduce output accuracy.

VI. THE QUANTUM-AI CONVERGENCE THREAT

A. Quantum Machine Learning for Offensive Operations

The convergence of quantum computing and artificial intelligence represents a paradigm shift in offensive cybersecurity capabilities. Quantum machine learning (QML) algorithms have the theoretical potential to process certain tasks with quantum speedup than classical AI, enabling new attack vectors[26].

Recent research has explored quantum machine learning algorithms for cybersecurity applications, including intrusion detection systems, malware classification, and DDoS attack detection. Hybrid quantum-classical approaches and quantum-enhanced classifiers (e.g., quantum support vector machines and quantum neural networks) have demonstrated promising results in controlled experimental settings, often achieving high accuracies on benchmark datasets and, in some cases, outperforming classical baselines on specific tasks[27][28]. However, scalability to production environments and real-world attack scenarios remains an open research question.

This quantum advantage in adversarial operations has profound implications:

- Enhanced Social Engineering: QML can analyze massive datasets of personal information to craft hyper-personalized phishing campaigns with unprecedented success rates.

- Polymorphic Malware Generation: Quantum-enhanced algorithms can develop malware that evolves faster than signature-based detection systems can adapt.

- Vulnerability Discovery: QML can accelerate the identification of zero-day vulnerabilities through quantum-accelerated fuzzing and symbolic executions.

B. Autonomous Quantum-Enabled Attacks

The marriage of quantum computing and autonomous AI (“agentic AI”) creates the potential for self-directed cyberattacks of unprecedented scale and sophistication[29]. Security analysts warn that this convergence could enable:

- Automated Quantum Decryption: AI agents could autonomously manage the decryption of harvested data once quantum capabilities become available.

- Adaptive Attack Orchestration: Quantum-enhanced AI could optimize attack strategies in real-time, adapting to defensive measures faster than human defenders can respond.

- Massive Identity Theft: LLMs sifting through quantum-decrypted databases could automate large-scale identity theft operations.

Research indicates that state-aligned hacker groups from Russia, China, Iran, and North Korea have been experimenting with using LLMs to assist in cyber operations, such as generating malicious code and content for phishing campaigns[30]. For instance, North Korea's Kimsuky group uses LLMs to generate content for phishing campaigns targeting organizations focused on North Korean defense. Adding quantum computing capabilities would exponentially amplify these threats.

VII. POST-QUANTUM CRYPTOGRAPHY: ASSESSMENT AND GAPS

A. NIST Standardization Efforts

In August 2024, NIST published the first three finalized post-quantum cryptographic standards[10]:

- FIPS 203 (ML-KEM): Module-Lattice-Based Key-Encapsulation Mechanism based on CRYSTALS-Kyber, for general encryption.

- FIPS 204 (ML-DSA): Module-Lattice-Based Digital Signature Algorithm based on CRYSTALS-Dilithium, for digital signatures.

- FIPS 205 (SLH-DSA): Stateless Hash-Based Digital Signature Algorithm based on SPHINCS+, as a backup signature method.

NIST continues work on additional algorithms. A fourth standard based on FALCON (FN-DSA/FIPS 206) is in draft review, with expectations for release in late 2026 to early 2027. Additionally, NIST has selected HQC for standardization, providing a code-based alternative to lattice-based KEM[31].

B. Implementation Vulnerabilities

Post-quantum cryptographic algorithms, while mathematically resistant to quantum attacks, remain vulnerable to implementation-level side-channel attacks. Research has demonstrated successful key recovery attacks against lattice-based schemes exploiting leakage in polynomial multiplication, modular reductions, and Number Theoretic Transform (NTT) datapaths[32].

The "KyberSlash" vulnerability discovered in December 2023 demonstrated that timing attacks could recover secret keys from CRYSTALS-Kyber implementations by sending fabricated ciphertext and measuring decryption time[33]. This vulnerability affected multiple implementations of the Kyber Post-Quantum Key Encapsulation Mechanism. Bernstein et al. presented KyberSlash1 and KyberSlash2, two timing vulnerabilities in several implementations including the official reference code of Kyber, demonstrating exploitability on Raspberry Pi 2 and Arm Cortex-M4 microprocessors[34].

C. Migration Challenges

The transition to post-quantum cryptography faces significant challenges:

TABLE V. POST-QUANTUM MIGRATION CHALLENGES BY DOMAIN

Challenge	Domain Specific Issues	Impact
Performance	Larger key sizes, slower operations	Resource-constrained devices
Compatibility	Protocol modifications required	Legacy system integration
Crypto-Agility	Static cryptographic	Update deployment
Validation	Formal verification gaps	Implementation errors

VIII. Q-THREAT MODEL FRAMEWORK

A. Framework Overview

We introduce the Q-THREAT (Quantum Temporal Hazard Risk Evaluation and Assessment Tool) framework, a novel model for quantifying and managing quantum-era cybersecurity risks. The framework addresses the temporal asymmetry of HNDL threats by integrating three key dimensions:

$$R(t) = P(H_a(t) \geq L_d) \cdot I \cdot V \quad (2)$$

Where $R(t)$ is the time-dependent risk function, $H_a(t)$ represents the adversary's decryption horizon at time t, L_d is the required data confidentiality lifetime, I is the impact of compromise, and V is the vulnerability of the data to harvesting.

Framework Components are:

- Temporal Risk Assessment: Evaluates the probability that quantum decryption capability arrives before data confidentiality expires.
- Sectoral Exposure Mapping: Categorizes organizations by data lifetime characteristics and quantum exposure, explicitly relating the data confidentiality lifetime (L_d) to the Security Categories (1 through 5) defined in NIST FIPS 203.
- Migration Priority Scoring: Quantifies the urgency of post-quantum migration based on risk metrics.
- Countermeasure Effectiveness: Evaluates risk mitigation from various defensive strategies.

B. Temporal Risk Assessment

The Q-THREAT model formalizes the HNDL adversary's capability evolution. Let $T_{\text{break}}(n, t)$ represent the expected time to break an n-bit RSA modulus at time t:

$$T_{\text{break}}(n, t) = \frac{\alpha \cdot n \cdot \text{ECC}(t)^3}{Q(t)} \quad (3)$$

Where α is a constant factor, $\text{ECC}(t)$ is the error-correction overhead, and $Q(t)$ is the logical qubits available to the adversary. The compromise condition

occurs when $H_a(t) \geq L_d$, meaning the adversary achieves decryption capability while the data still requires protection.

TABLE VI. Q-THREAT RISK SCORES BY SECTOR (EXAMPLE APPLICATION)

Sector	Avg. Data Lifetime	Quantum Timeline	Risk Score	Priority
Financial Services	7 years	10 years (median)	0.65	High
Healthcare	25 years	10 years (median)	0.95	Critical
Government	30+ years	10 years (median)	0.98	Critical

C. Mitigation Strategies

Based on Q-THREAT analysis, we propose a tiered mitigation approach:

Immediate Actions:

- Inventory all cryptographic assets and dependencies.
- Identify long-lived sensitive data requiring protection beyond 2035.
- Deploy hybrid post-quantum key exchange for TLS.
- Establish supply chain visibility into all cryptographic dependencies.
- Implement crypto-agility frameworks for rapid algorithm transition.

Mid-Term Actions:

- Complete migration of key agreement ML-KEM (CRYSTALS-Kyber).
- Deploy ML-DSA for digital signatures in high-security applications.
- Establish quantum-safe certificate authorities.
- Implement quantum key distribution (QKD) for critical infrastructure.

Long-Term Actions:

- Full transition to post-quantum cryptography.
- Continuous monitoring for cryptanalytic advances.
- Development of quantum-resistant security architectures.

IX. DISCUSSION AND FUTURE DIRECTIONS

This research reveals that the quantum threat extends far beyond the well-documented risks to public-key cryptography. Our analysis demonstrates that quantum systems themselves harbor significant vulnerabilities, including quantum Rowhammer attacks, timing side-channels, and multi-tenant exploitation that could compromise the integrity of quantum computations before quantum cryptanalysis becomes practical.

The convergence of quantum computing and artificial intelligence presents perhaps the most concerning long-term threat. Quantum-enhanced machine learning algorithms have shown promising results in controlled experimental settings, with some studies reporting competitive performance on specific benchmark datasets in controlled experimental settings, and autonomous quantum-enabled attacks may soon operate at machine speeds beyond human defensive capabilities.

We believe several critical research gaps require attention:

- Quantum System Security: The security community must develop formal threat models and defensive mechanisms specifically for quantum computing platforms, analogous to the decades of research that secured classical computing systems.
- Side-Channel Resistant PQC: Post-quantum cryptographic implementations require rigorous side-channel analysis and countermeasures, as demonstrated by vulnerabilities like KyberSlash.
- Quantum Network Security: As quantum networks and the quantum internet emerge, new security protocols must be developed to protect quantum communications.
- Quantum-AI Defenses: Defensive applications of quantum machine learning should be explored to counter quantum-enabled offensive operations.

X. CONCLUSION

Quantum computing represents both an unprecedented opportunity and an existential threat to cybersecurity. This comprehensive analysis has demonstrated that the quantum threat landscape extends far beyond cryptanalysis to include vulnerabilities within quantum systems themselves and the convergence of quantum computing with artificial intelligence for offensive operations.

Our Q-THREAT framework provides organizations with a quantitative tool for assessing their temporal exposure to HNDL attacks and prioritizing their post-quantum migration efforts. The framework reveals that sectors with long data confidentiality lifetimes, specifically healthcare, government, and critical infrastructure, face critical risk levels requiring immediate action.

Recent research discoveries of quantum Rowhammer attacks (Almaguer-Angeles et al., 2025; Tan et al., 2025; Campbell, 2025), timing side-channels in quantum cloud services (Lu et al., 2024), multi-tenant exploitation vectors (Choudhury et al., 2024; Lee et al., 2025), and power side-channel attacks (Erata et al., 2024) demonstrate that quantum systems are not inherently secure.

As quantum computing transitions from research curiosity to commercial infrastructure, the security community must apply the lessons learned from decades of classical cybersecurity to this new domain. The quantum-AI convergence threat demands particular attention. The combination of quantum decryption capabilities with autonomous AI agents could enable cyberattacks of unprecedented scale and sophistication.

We believe this is the perfect time to start preparation. The HNDL threat model means that data encrypted today with vulnerable algorithms may already be compromised, decryption has not yet happened, but the window for protection is closing. Organizations that delay their post-quantum migration in the hope that quantum computers remain years away are gambling with secrets that may need protection for decades.

ACKNOWLEDGMENTS

This research was conducted independently by the author. No external funding was received. The author declares no conflicts of interest.

REFERENCES

[1] H. T. Nguyen, P. Krishnan, D. Krishnaswamy, M. Usman, and R. Buyya, "Quantum cloud computing: A review, open problems, and future directions," arXiv preprint arXiv:2404.11420, 2024.

[2] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134.

[3] S. Beauregard, "Circuit for Shor's algorithm using 2n+3 qubits," Quantum Information & Computation, vol. 3, no. 2, pp. 175-185, 2003.

[4] C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv preprint arXiv:2505.15917, 2025.

[5] F. Kharitonov et al., "A temporal cybersecurity risk in the quantum transition," Cryptography, vol. 6, no. 4, p. 100, 2025.

[6] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2010.

[7] J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum, vol. 2, p. 79, 2018.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 1996, pp. 212-219.

[10] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188-194, 2017.

[11] National Institute of Standards and Technology, "NIST releases first 3 finalized post-quantum encryption standards," NIST News, 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[12] N. Choudhury, C. N. Mude, S. Das, P. C. Tikkireddi, S. Tannu, and K. Basu, "Crosstalk-induced side channel

threats in multi-tenant NISQ computers," arXiv preprint arXiv:2412.10507, 2024.

[13] F. Almaguer-Angeles et al., "Hacking quantum computers with row hammer attack," arXiv preprint arXiv:2503.21650, 2025.

[14] C. Lu, E. Telang, A. Aysu, and K. Basu, "Quantum leak: Timing side-channel attacks on cloud-based quantum services," in Proceedings of the Great Lakes Symposium on VLSI 2025, ACM, 2025, pp. 1-6.

[15] F. Erata, C. Xu, R. Piskac, and J. Szefer, "Quantum circuit reconstruction from power side-channel attacks on quantum computer controllers," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2024, no. 2, pp. 735-763, 2024.

[16] Sectigo, "Harvest now, decrypt later attacks & the quantum threat," 2025. [Online]. Available: https://www.sectigo.com/blog/harvest-now-decrypt-later-quantum-threat

[17] V. Gheorghiu and M. Mosca, "Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," arXiv preprint arXiv:1902.02332, 2019.

[18] National Institute of Standards and Technology, "On the practical cost of Grover for AES key recovery," in Fifth PQC Standardization Conference, 2024.

[19] Federal Bureau of Investigation, "Protecting quantum science and technology," 2024. [Online]. Available: https://www.fbi.gov/news/stories/protecting-quantum-science-and-technology

[20] SecurityWeek, "Cyber Insights 2026: Quantum computing and the potential synergy with advanced AI," 2026. [Online]. Available: https://www.securityweek.com/cyber-insights-2026-quantum-computing-and-the-potential-synergy-with-advanced-ai/

[21] Y. Mustafa and S. Köse, "Side-channel attacks targeting classical-quantum interface in quantum computers," in 2024 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2024, pp. 1-5.

[22] Y. Tan, N. Choudhury, K. Basu, and J. Szefer, "QubitHammer attacks: Qubit flipping attacks in multi-tenant superconducting quantum computers," arXiv preprint arXiv:2504.07875, 2025.

[23] D. Campbell, "Exploring the Quantum Rowhammer Attack," arXiv preprint arXiv:2509.06318, 2025.

[24] S. Das, A. Chatterjee, and S. Ghosh, "Investigating impact of bit-flip errors in control electronics on quantum computation," arXiv preprint arXiv:2405.05511, 2024.

[25] A. Mi, S. Deng, and J. Szefer, "Securing reset operations in NISQ quantum computers," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, 2022, pp. 2279-2293.

[26] W. J. B. Lee, S. Wang, S. Dutta, W. E. Maouaki, and A. Chattopadhyay, "Swap attack: Stealthy side-channel attack on multi-tenant quantum cloud system," arXiv preprint arXiv:2502.10115, 2025.

[27] M. T. West et al., "Towards quantum enhanced adversarial robustness in machine learning," Nature Machine Intelligence, vol. 5, no. 6, pp. 648-659, 2023.

[28] Cyber Technology Insights, "How quantum computing is reshaping cybersecurity in 2025," 2025. [Online]. Available: https://cybertechnologyinsights.com/cybertech-staff-articles/how-quantum-computing-is-reshaping-the-future-of-cybersecurity-in-2025/

[29] O. M. Alnahas et al., "Quantum machine learning for intrusion detection systems: A comprehensive review," IEEE Access, vol. 11, pp. 82765-82784, 2023.

[30] Spherity, "Q-Day and Agentic AI: The ultimate nightmare in cybersecurity," 2025. [Online]. Available: https://www.spherity.com/post/q-day-and-agentic-ai-the-ultimate-nightmare-in-cybersecurity

[31] Microsoft & OpenAI, "Cyber threat actors use AI in attack operations," Microsoft Security Blog, 2024.

[32] National Institute of Standards and Technology, "Post-quantum cryptography standardization," 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[33] R. Zeitoun, "The challenge of side-channel countermeasures on post-quantum crypto," in Fourth PQC Standardization Conference, NIST, 2022.

[34] CyberArk, "NEW risks to post-quantum Kyber KEM: What are timing attacks and how do they threaten encryption?," 2024. [Online]. Available: https://www.cyberark.com/resources/blog/new-risks-to-post-quantum-kyber-kem

[35] D. J. Bernstein et al., "KyberSlash: Exploiting secret-dependent division timings in Kyber

implementations," IACR Cryptology ePrint Archive, 2023.

[36] J. Coupel and T. Farheen, "Security vulnerabilities in quantum cloud systems: A survey on emerging threats," arXiv preprint arXiv:2504.19064, 2025.

[37] D. B. Rawat and C. Bajracharya, "The intersection of quantum computing, AI, and cybersecurity: Challenges and opportunities," in IEEE Conference on Trust, Privacy and Security in Intelligent Systems, IEEE, 2024, pp. 1-8.

[38] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure," arXiv preprint arXiv:2404.10659, 2024.