Scientific Research Publishing

Journal of Quantum Information Science, 2026, 16(2), 191-225
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Quantum Cybersecurity: A Rising Strategic Imperative

Troy C. Troublefield[1,2,3]

[1]Department of Cyberpsychology, Capital Technology University, Laurel, USA
[2]Department of Information Technology, Capella University, Minneapolis, USA
[3]Department of International Business, International School of Management, Paris, France
Email: drtroytroublefield@yahoo.com

How to cite this paper: Troublefield, T.C. (2026) Quantum Cybersecurity: A Rising Strategic Imperative. *Journal of Quantum Information Science*, **16**, 191-225.
https://doi.org/10.4236/jqis.2026.162007

Received: April 3, 2026
Accepted: June 7, 2026
Published: June 10, 2026

Abstract

Quantum cybersecurity has emerged as a critical strategic issue at the intersection of national security, technological advancement, and digital sovereignty. As quantum computing technology advances toward practical implementation, the dual-edged nature of this revolutionary technology becomes increasingly apparent: while quantum computers threaten to break traditional encryption methods like RSA and ECC, they simultaneously promise to enable quantum-resistant algorithms through post-quantum cryptography (PQC). This comprehensive analysis examines the current state of quantum cybersecurity threats, the global investment landscape in quantum technologies, the vulnerability of critical sectors, and the urgent need for proactive migration to quantum-safe solutions. With NIST's finalization of post-quantum cryptography standards in 2024 and projected quantum threats materializing by 2030, organizations across defense, finance, healthcare, and critical infrastructure must accelerate their transition to quantum-resistant technologies. The geopolitical implications are profound, with China, the United States, and European Union engaging in an unprecedented quantum arms race that will determine future cybersecurity leadership and technological sovereignty.

Keywords

Quantum Cybersecurity, Post-Quantum Cryptography, Digital Security, Quantum Computing, National Security, Strategic Technology

1. Introduction

1.1. Background of the Study

The digital age has fundamentally transformed how nations conduct business,

warfare, and international relations. At the heart of this transformation lies cryptography, the mathematical foundation that secures everything from personal communications to state secrets. However, we stand at an inflection point where the very technology that promises to revolutionize computing also threatens to undermine the cryptographic systems upon which our digital civilization depends. Quantum computing, once confined to theoretical physics laboratories, is rapidly approaching practical implementation with profound implications for cybersecurity and national security.

The emergence of quantum cybersecurity as a strategic imperative reflects the dual nature of quantum computing technology. On the one hand, sufficiently powerful quantum computers threaten to break the mathematical foundations of current encryption standards, including RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange protocols, which secure most digital communications worldwide [1]. On the other hand, quantum technologies offer unprecedented opportunities to develop quantum-resistant cryptographic systems and quantum key distribution (QKD) networks that could provide theoretically unbreakable security.

Recent developments have accelerated the urgency of addressing quantum cybersecurity challenges. In August 2024, NIST finalized the first three post-quantum cryptography standards, FIPS 203, FIPS 204, and FIPS 205, marking a critical milestone in preparing for the quantum era [2]. These standards, based on CRYSTALS-Kyber, CRYSTALS-Di-lithium, and SPHINCS+ algorithms, provide the first standardized quantum-resistant cryptographic tools for organizations worldwide. However, the transition window is narrowing rapidly as quantum computing capabilities continue to advance.

The strategic implications extend far beyond technical considerations. Global powers are investing unprecedented resources in quantum technologies, with China leading at $15 billion, the European Union committing $7 billion, and the United States investing approximately $3.5 billion in quantum research and development [3]. This quantum arms race reflects the understanding that quantum supremacy will confer significant advantages in cryptography, communications, and information processing with direct implications for military, intelligence, and economic competitiveness.

Critical sectors face varying degrees of vulnerability to quantum threats. Defense systems, which rely heavily on encrypted communications and secure command-and-control networks, face an estimated 85% vulnerability by 2030 without post-quantum cryptography implementation [4]. Financial institutions, healthcare systems, and critical infrastructure operators each face substantial risks as quantum computers mature. The interconnected nature of modern digital systems means that vulnerabilities in one sector can cascade across others, amplifying the potential impact of quantum-enabled cyberattacks.

This article provides a comprehensive analysis of quantum cybersecurity as a rising strategic imperative. We examine the current state of quantum computing

technology, assess vulnerabilities across critical sectors, analyze global investment patterns and geopolitical competition, and outline the urgent steps necessary to build quantum-resilient digital infrastructure. The evidence demonstrates that quantum cybersecurity is not a distant future concern but an immediate strategic priority requiring coordinated action across government, industry, and international partners.

Three terms appear throughout this article and require precise definition at the outset. Quantum cybersecurity is the interdisciplinary domain concerned with protecting digital systems, communications, and data against threats enabled by quantum computing, as well as harnessing quantum-mechanical phenomena, such as quantum key distribution, to strengthen cryptographic security. Quantum-safe (used interchangeably with quantum-resistant) refers to cryptographic algorithms, protocols, or systems designed to remain computationally secure against both classical and quantum adversaries, as assessed against current cryptanalytic knowledge; the term does not imply unconditional or permanent security, since all cryptographic systems remain subject to future advances in mathematics and computation. The vulnerability percentage estimates presented in Section 4, 85% for defense, 78% for financial services, 70% for healthcare, and 65% for critical infrastructure, denote projected cryptographic asset exposure: the estimated proportion of encrypted assets within each sector that rely on algorithms (principally RSA and ECC) that a cryptographically relevant quantum computer could compromise using Shor's algorithm. These figures are sector-specific projections derived from industry and government assessments rather than measured attack probabilities or confirmed migration-readiness benchmarks; they are used to indicate relative urgency across sectors and should be interpreted accordingly.

1.2. Analytical Approach and Source Selection

This article is a policy-oriented narrative review and strategic synthesis rather than a systematic or scoping review. No formal search protocol, eligibility screening matrix, or PRISMA-style reporting was employed. The literature reviewed was selected through a theoretically directed process organized around five analytical pillars: 1) quantum computing hardware development and cryptographic threat trajectories, 2) post-quantum cryptography standardization and algorithmic foundations, 3) sectoral vulnerability and operational risk, 4) global investment patterns and geopolitical competition, and 5) implementation, regulatory, and policy dimensions of post-quantum migration. Sources were drawn primarily from the period 2018 through early 2025, with priority given to peer-reviewed journal articles, conference proceedings, and authoritative technical publications from recognized standards bodies, including NIST, NSA, NATO, and sector-specific regulatory organizations. Policy reports, government white papers, vendor roadmaps, and credible industry analyses were incorporated where peer-reviewed literature was unavailable for a given claim, particularly for investment figures and sectoral vulnerability projections. In those instances, the evidentiary basis is identified ex-

plicitly in the text or footnoted. Sectoral vulnerability estimates presented in Section 4 and the global investment figures in Section 5 are drawn from sector-specific reports and scenario-based projections; they are not derived from primary data collection and should be interpreted as directional indicators rather than precisely measured empirical quantities. Where the Abstract and Introduction refer to this work as a "comprehensive analysis", that phrase denotes breadth of topical coverage rather than exhaustive systematic literature retrieval.

2. The Quantum Computing and Cryptographic Vulnerabilities

Quantum computing is rapidly transitioning from theoretical research to practical technology, fundamentally reshaping the landscape of digital security. Unlike classical computers, quantum machines leverage quantum mechanical principles to solve certain problems with unprecedented speed, posing a direct threat to many widely used cryptographic systems. The prospect of quantum-enabled attacks capable of compromising current encryption standards that safeguard sensitive communications and critical infrastructure has shifted quantum security from a distant concern to an urgent priority. This section explores the fundamentals of quantum computing, the mechanisms behind its cryptographic threats, current vulnerabilities exposed by emerging quantum technologies, and the uncertainty surrounding the timeline for quantum impact, outlining why immediate action and strategic planning are essential for organizations reliant on robust digital security.

2.1. Quantum Computing Fundamentals and Capabilities

Quantum computing represents a fundamental departure from classical computing paradigms, harnessing quantum mechanical phenomena such as superposition, entanglement, and quantum interference to process information in revolutionary ways. Unlike classical bits that exist in definite states of 0 or 1, quantum bits (qubits) can exist in superposition states that are simultaneously 0 and 1, enabling quantum computers to explore multiple solution paths simultaneously [5].

The implications for computational problem-solving are profound. Where classical computers must evaluate potential solutions sequentially, quantum computers can leverage quantum parallelism to evaluate vast numbers of possibilities simultaneously. This advantage becomes particularly pronounced for specific classes of mathematical problems, including the integer factorization and discrete logarithm problems that underpin modern public-key cryptography.

Recent advances in quantum computing hardware have demonstrated steady progress toward practical implementation. IBM's quantum roadmap envisions 100,000-qubit systems by 2030, while Google's quantum AI division has made significant strides in quantum error correction and algorithm optimization [6]. Current systems, while limited to hundreds of qubits, have already demonstrated quantum advantage for specific optimization problems, foreshadowing the capabilities of larger systems will possess.

2.2. Shor's Algorithm and the Cryptographic Threat

The cryptographic threat posed by quantum computing was first articulated by mathematician Peter Shor in 1994, who developed a quantum algorithm that could efficiently factor large integers and solve discrete logarithm problems, the mathematical foundations of RSA, Elliptic Curve Cryptography, and Diffie-Hellman protocols [7]. Shor's algorithm promised exponential speedups over classical factoring algorithms, theoretically enabling quantum computers to break encryption systems that would require classical computers thousands of years to crack.

Recent research has dramatically reduced estimates of the quantum resources required to implement Shor's algorithm against real-world encryption systems. Google Quantum AI researcher Craig Gidney's 2024 analysis suggests that RSA-2048 encryption is a cornerstone of modern digital security that could be broken by a quantum computer with fewer than 1 million noisy qubits, operating for approximately 1 week [8]. This represents a twenty-fold reduction from previous estimates and significantly compresses the timeline for practical quantum threats.

The implications extend beyond academic interest. RSA-2048 encryption secures vast swaths of digital infrastructure, from online banking and e-commerce to government communications and military systems. The prospect of quantum computers breaking these systems within the next decade has transformed quantum cybersecurity from a theoretical concern to an immediate strategic priority [9].

2.3. Current Vulnerabilities and Attack Scenarios

The vulnerability of current cryptographic systems to quantum attack varies significantly based on the underlying mathematical problems and implementation details. Public-key cryptographic systems based on integer factorization (RSA) and the discrete logarithm problem (ECC, Diffie-Hellman) are fundamentally vulnerable to quantum attacks via Shor's algorithm. Symmetric encryption systems like AES, while more resistant, still face reduced effective key lengths under quantum attack via Grover's algorithm [10].

Recent demonstrations have provided concrete evidence of quantum cryptographic attacks, albeit at limited scales. Chinese researchers at Shanghai University reported using D-Wave quantum annealing systems to optimize an integer-factoring problem formulation, successfully factoring integers up to 22 bits, well below the key lengths used in practice, while also demonstrating quantum annealing-based attacks on simplified symmetric-cipher structures [11]. Both demonstrations are proof-of-concept results at scales many orders of magnitude smaller than operationally relevant targets, and neither represents a practical threat to deployed RSA-2048 or AES-128 implementations under current quantum hardware constraints.

The "harvest now, decrypt later" attack scenario presents an immediate threat even before large-scale quantum computers become available. Adversaries are actively collecting encrypted data with the intention of storing it until quantum

computers capable of breaking the encryption become available. This strategy is particularly concerning information with long-term value, such as state secrets, infrastructure plans, and personal information that has remained sensitive for decades [12].

2.4. Uncertainty Avoidance

Estimating the timeline for practical quantum threats is highly uncertain, as quantum computing development faces significant technical challenges, including quantum error correction, qubit coherence, and scalability. However, recent progress has accelerated the pace of expert predictions and narrowed the estimated timeframe for quantum cryptographic threats [13].

Multiple research groups and organizations have provided timeline estimates based on current progress trajectories. IBM's quantum roadmap suggests that fault-tolerant quantum computers capable of running Shor's algorithm may emerge by 2030 [6]. Google Quantum AI's recent algorithmic improvements suggest that the resource requirements for breaking RSA-2048 may be achievable sooner than previously anticipated [8]. The National Security Agency (NSA) has recommended beginning post-quantum cryptography transitions immediately, citing the possibility of quantum computers capable of cryptographically relevant operations emerging within 10 - 15 years [14].

The consensus among experts points to the 2030 timeframe as a critical threshold when quantum computers may achieve sufficient capability to threaten widely deployed cryptographic systems. This timeline has informed NIST's recommendations that organizations deprecate vulnerable algorithms by 2030 and prohibit their use entirely by 2035 [1]. The relatively short transition window requires immediate action to assess vulnerabilities, plan migrations, and implement quantum-resistant alternatives.

3. Post-Quantum Cryptography: The Defense against Quantum Threats

The impending reality of quantum computing poses a substantial risk to current cryptographic systems, driving a global search for solutions that withstand both classical and quantum attacks. Post-quantum cryptography (PQC) represents this new generation of cryptographic algorithms, specifically designed to remain secure even as quantum computers mature. In response to the urgency of the quantum threat, national and international standards bodies, led by the U.S. National Institute of Standards and Technology (NIST), have accelerated efforts to evaluate, select, and standardize robust quantum-resistant algorithms. This section examines the development and features of post-quantum cryptography standards, explores the mathematical approaches behind quantum-resistant security, outlines the implementation challenges for organizations transitioning to PQC, and highlights the importance of standardization and interoperability in fostering a secure and resilient global cryptographic ecosystem.

3.1. NIST Post-Quantum Cryptography Standardization

The National Institute of Standards and Technology launched its Post-Quantum Cryptography Standardization project in 2016, recognizing the urgent need to develop cryptographic systems resistant to both classical and quantum computer attacks. After evaluating 82 algorithms from 25 countries over multiple rounds of analysis, NIST finalized the first three post-quantum cryptography standards in August 2024: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [2].

These standards represent different approaches to quantum-resistant cryptography. ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), derived from CRYSTALS-Kyber, provides key establishment capabilities based on the difficulty of solving lattice problems, mathematical structures believed to be resistant to both classical and quantum attacks. ML-DSA (Module-Lattice-Based Digital Signature Algorithm), based on CRYSTALS-Dilithium, offers digital signature capabilities using similar lattice-based mathematics. SLH-DSA (Stateless Hash-Based Digital Signature Algorithm), derived from SPHINCS+, provides an alternative digital signature approach based on hash functions [15].

In March 2025, NIST selected HQC (Hamming Quasi-Cyclic) as a fifth algorithm for standardization, providing backup capabilities for general encryption based on mathematical foundations different from those of ML-KEM (NIST, 2025). This diversification reflects the cryptographic community's recognition that multiple algorithmic approaches may be necessary to ensure long-term security against evolving quantum threats [16].

3.2. Algorithmic Approaches to Quantum Resistance

Post-quantum cryptographic algorithms rely on mathematical problems believed to be difficult for both classical and quantum computers to solve. The primary families of quantum-resistant algorithms include lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptography (though the latter has faced recent cryptanalytic attacks) [17].

Lattice-based cryptography, which forms the foundation of NIST's primary standards, relies on problems such as Learning With Errors (LWE) and Ring Learning With Errors (RLWE). These problems involve finding short vectors in high-dimensional lattices, a task that appears to remain difficult even for quantum computers. The security of lattice-based systems is supported by decades of cryptanalytic research and worst-case hardness assumptions, which provide strong theoretical foundations [18].

Hash-based signatures offer an alternative approach with well-understood security properties. These systems base their security on the collision resistance of cryptographic hash functions, which are generally considered quantum-resistant when appropriately increased output sizes are used. The stateless nature of newer hash-based signature schemes addresses practical deployment challenges while maintaining strong security guarantees.

Code-based cryptography relies on error-correcting codes and the difficulty of decoding random linear codes, a problem that remains challenging for quantum computers. While code-based systems often require larger key sizes than lattice-based alternatives, they offer strong security foundations and represent an important diversification strategy for post-quantum cryptography.

3.3. Implementation Challenges and Considerations

The transition to post-quantum cryptography presents significant technical and operational challenges that organizations must address to ensure successful migration. Key size increases represent perhaps the most immediate challenge, as post-quantum algorithms typically require larger keys and signatures than current systems. ML-KEM requires public keys of 800 - 1568 bytes compared to 256 bytes for P-256 elliptic curve keys, while ML-DSA signatures range from 2420 - 4595 bytes compared to 64 bytes for ECDSA signatures [2].

Performance implications vary significantly across different post-quantum algorithms and use cases. While some algorithms, such as ML-KEM, demonstrate competitive performance for key establishment, others may require more computational resources or memory than current systems. Organizations must carefully evaluate performance requirements and select appropriate algorithms for each use case.

Cryptographic agility, the ability to rapidly transition between different cryptographic algorithms, becomes critical in the post-quantum era. Systems designed with cryptographic agility can more easily adopt new algorithms as they become standardized or migrate away from algorithms that may face future cryptanalytic attacks. This approach requires modular cryptographic implementations and clear separation between cryptographic and application logic.

Hybrid approaches that combine classical and post-quantum algorithms offer a transitional strategy that provides security against both current and future threats. These systems use both traditional algorithms (for protection against classical attacks) and post-quantum algorithms (for protection against quantum attacks), ensuring security even if one approach fails. However, hybrid implementations require careful design to avoid introducing new vulnerabilities while managing increased complexity.

3.4. Standardization and Interoperability

International coordination of post-quantum cryptography standards is essential to ensure global interoperability and avoid fragmentation of the cryptographic ecosystem. While NIST has taken a leadership role in post-quantum standardization, other regional and international standards bodies are developing complementary standards and guidelines.

The European Telecommunications Standards Institute (ETSI) has published technical specifications for quantum-safe cryptography, while ISO/IEC joint technical committees are developing international standards for post-quantum cryp-

tographic algorithms. China's State Cryptography Administration has published national standards for quantum-resistant algorithms, some of which differ from NIST selections.

Ensuring interoperability between different post-quantum implementations requires careful attention to algorithm parameters, encoding formats, and protocol specifications. Standardization efforts must balance security requirements, performance considerations, and practical deployment constraints while maintaining compatibility across diverse systems and platforms.

A critical distinction in implementation planning separates post-quantum cryptography from quantum key distribution, two technologies that are frequently discussed together but differ substantially in practical deployment and timescale. Post-quantum cryptography, the algorithmic standards now finalized by NIST (FIPS 203, 204, 205, and the forthcoming HQC standard), are software-implementable on existing classical hardware and are deployable today across internet protocols, enterprise systems, and embedded devices; it represents the near-term, primary migration path for the overwhelming majority of organizations. Quantum key distribution, by contrast, requires dedicated optical fiber infrastructure or line-of-sight satellite links, is currently limited to point-to-point or hub-and-spoke network architectures with distance constraints typically below 300 km without quantum repeaters, and is practical primarily for government, defense, and high-value financial communications with specialized physical security requirements. QKD should be understood as a complementary, longer-horizon option for high-assurance environments rather than a scalable alternative to algorithmic PQC migration for general enterprise use. Organizations should prioritize PQC migration immediately and regard QKD as a specialized supplement, with its infrastructure requirements and cost profile operationally justified.

4. Sectoral Vulnerability Analysis

The transition to quantum computing poses unique and urgent risks across key sectors that underpin national security, economic stability, public health, and essential infrastructure. Each of these sectors relies heavily on cryptographic systems that are increasingly vulnerable to advancing quantum capabilities. This sectoral vulnerability analysis examines the specific quantum cybersecurity challenges confronting defense and national security, financial services, healthcare systems, and critical infrastructure. The analysis highlights both the scale of potential exposures and the operational, regulatory, and technical complexities involved in post-quantum migration. By understanding sector-specific impacts and requirements, organizations and policymakers can prioritize resources and develop targeted strategies to achieve quantum resilience in the years ahead.

4.1. Defense and National Security

Defense systems represent perhaps the most critical sector for quantum cybersecurity concerns, given their role in national security and the potentially cata-

strophic consequences of cryptographic failures. Military communications, command-and-control systems, weapons platforms, and intelligence networks rely extensively on encrypted communications that could be vulnerable to quantum attacks.

Sector assessments estimate that defense systems will face approximately 85% cryptographic asset exposure to quantum attacks by 2030 without the implementation of post-quantum cryptography [19]. A figure representing the projected proportion of defense-sector encrypted assets relying on RSA and ECC algorithms, derived from DHS and CISA preparedness analyses rather than from direct measurement of attack probability.

The classified nature of many defense systems creates additional challenges for post-quantum migration. These systems often use proprietary or classified cryptographic implementations that may not easily accommodate standardized post-quantum algorithms. The security clearance requirements and specialized hardware used in classified systems can significantly extend migration timelines and increase implementation costs.

International defense cooperation adds another layer of complexity, as allied nations must coordinate post-quantum transitions to maintain interoperability. NATO has recognized quantum threats in its first quantum strategy, published in January 2024, emphasizing the need for alliance-wide approaches to quantum-ready defense systems [20].

The Department of Defense has initiated comprehensive efforts to address quantum threats through the Quantum Information Science strategy and increased funding for quantum-resistant technologies. However, the scale and complexity of defense systems require sustained investment and coordination across military services, defense contractors, and international partners.

4.2. Financial Services

The financial services sector faces substantial quantum cybersecurity risks due to its extensive reliance on cryptographic protection for transactions, communications, and data storage. Banking systems, payment networks, trading platforms, and financial communications infrastructure collectively handle trillions of dollars in daily transactions, protected by cryptographic systems that are vulnerable to quantum attacks.

Industry vulnerability assessments estimate approximately 78% cryptographic exposure for financial systems by 2030 without post-quantum cryptography implementation [21], reflecting the projected share of financial-sector assets secured by quantum-vulnerable public-key protocols; this figure is a scenario-based projection from FS-ISAC intelligence reporting and should be interpreted as a directional risk indicator rather than a confirmed empirical measurement.

The real-time nature of financial systems presents unique challenges for post-quantum migration. High-frequency trading systems, payment processors, and settlement networks operate under strict latency requirements that may be af-

fected by the increased computational overhead of some post-quantum algorithms. Performance testing and optimization will be critical to ensure that quantum-resistant systems maintain the speed and reliability required for financial operations.

Regulatory compliance adds another dimension to financial sector post-quantum transitions. Financial regulators worldwide are beginning to address quantum threats, with some jurisdictions proposing mandatory timelines for post-quantum adoption. The Federal Financial Institutions Examination Council (FFIEC) has issued guidance on quantum risk management, while the European Central Bank has initiated assessments of quantum threats to payment systems [22].

International coordination is essential given the global nature of financial markets and payment systems. Cross-border transactions, correspondent banking relationships, and international settlement systems require coordinated approaches to post-quantum migration to maintain global financial connectivity and stability.

4.3. Healthcare Systems

Healthcare systems face significant quantum cybersecurity challenges due to their extensive use of digital health records, medical devices, and telemedicine platforms that rely on cryptographic protection. The sector's vulnerability is compounded by the long-term sensitivity of health information and the potential for "harvest now, decrypt later" attacks targeting medical data.

Healthcare sector vulnerability assessments suggest approximately 70% exposure to quantum cryptographic threats by 2030 without post-quantum implementation [23], a scenario-based projection from HIMSS policy analysis reflecting the estimated proportion of health IT systems relying on RSA, ECC, and classical TLS implementations rather than a measured attack-likelihood figure.

The diversity of healthcare IT infrastructure presents particular challenges for post-quantum migration. Healthcare systems often include legacy medical devices, proprietary health information systems, and specialized clinical applications that may require extensive updates or replacement to support post-quantum algorithms. The long lifespan of medical devices, often 10 - 15 years, means that equipment installed today may still be in use when quantum threats materialize.

Patient safety considerations add critical urgency to healthcare quantum cybersecurity preparations. Cyberattacks on healthcare systems can directly impact patient care, from disrupting electronic health records to compromising medical device functionality. The potential for quantum-enabled attacks to cause widespread failures in healthcare systems underscores the need for proactive post-quantum implementation.

Privacy and compliance requirements in healthcare create additional complexities for quantum cybersecurity planning. HIPAA and international health privacy regulations may require specific approaches to implementing post-quantum cryptography, while the sensitivity of health information demands robust security

throughout migration processes.

4.4. Critical Infrastructure

Critical infrastructure sectors, including energy, transportation, water systems, and telecommunications, face substantial quantum cybersecurity risks due to their essential role in society and their extensive use of industrial control systems and communication networks that are protected by vulnerable cryptographic systems.

DHS-based infrastructure vulnerability assessments project approximately 65% cryptographic exposure to quantum threats across critical infrastructure sectors by 2030 without post-quantum intervention [24], which is an estimate representing the share of SCADA, ICS, and communications assets secured by quantum-vulnerable algorithms, derived from preparedness scenario modeling rather than direct threat measurement.

The interconnected nature of critical infrastructure amplifies quantum cybersecurity risks, as failures in one sector can cast causal to others. For example, cyberattacks on electrical grid systems can impact healthcare facilities, financial data centers, and telecommunications networks, creating system-wide vulnerabilities that quantum-enabled attackers could exploit.

Legacy industrial control systems present particular challenges for post-quantum migration due to their long operational lifespans and often limited ability to support cryptographic updates. Many SCADA and industrial control systems were designed before cybersecurity became a primary concern and may require significant modifications or replacement to support post-quantum algorithms.

Public-private coordination is essential for critical infrastructure quantum cybersecurity, as many systems are operated by private entities but provide essential public services. Government agencies are working with infrastructure operators to develop sector-specific guidance for post-quantum transitions while maintaining operational continuity and security.

Table 1. Quantum vulnerability estimates by sector for 2030.

Sector	Estimated Vulnerability Without PQC (%)	Primary Risks	Notes
Defense & Nat. Security	85	Military communications, C2, intelligence	Long upgrade cycles, classified systems
Financial Services	78	Transactions, payment systems	Real-time operations, regulatory mandates
Healthcare	70	Digital health records, medical devices	Legacy devices, patient safety
Critical Infrastructure	65	Energy, transport, SCADA, telecom	Legacy controls, cascading dependencies

Table 1 summarizes the projected vulnerabilities of sector-core attacks to quantum attacks by 2030 if post-quantum cryptography is not adopted. Defense and national security face the highest risk, at 85%, due to their critical reliance on encrypted systems and long system upgrade cycles. Financial services (78%) and healthcare (70%) are also highly vulnerable due to their reliance on secure, real-time transactions, sensitive data, and complex regulatory pressures. Critical infrastructure is projected to be 65% vulnerable, challenged by aging technologies and sector interdependencies. Each sector's main risks, such as proprietary systems in defense, latency in finance, patient safety in healthcare, and cascading failures in infrastructure, reinforce the urgency for timely migration and sector-specific strategies. The table provides a concise snapshot to help prioritize quantum-safe investments in the most exposed domains.

5. Global Investment Landscape and Geopolitical Competition

The accelerating global race to achieve quantum capabilities has created a new arena for technological investment and international competition, with profound implications for national security, economic growth, and scientific leadership. Major powers, including China, the United States, and the European Union, are committing substantial public and private resources to quantum research, development, and infrastructure. At the same time, a diverse group of other nations is launching significant quantum initiatives to secure a stake in this emerging field. This section provides an overview of the evolving global investment landscape in quantum technologies, analyzes the competitive strategies of leading countries and regions, and highlights the geopolitical dynamics shaping the future of quantum science and technology. These investment figures represent publicly acknowledged government budget commitments and official program announcements as reported by Merics [3], The Quantum Insider [4], and regional parliamentary and government sources [25]; they do not include classified spending, private sector co-investment, or procurement-embedded research budgets, and therefore represent minimum floor estimates rather than comprehensive national quantum expenditure totals.

5.1. Chinese Quantum Investments and Strategy

China has emerged as the global leader in quantum technology investment, with officially acknowledged public spending reaching approximately $15 billion as of 2024 [3]. This massive investment reflects China's recognition of quantum technologies as pivotal to global science and technology competition, with direct implications for military advantages in cryptology, communication, and information processing.

China's quantum development strategy is primarily state-governed, with the National Laboratory for Quantum Information Sciences in Hefei serving as the flagship research institution. The laboratory received an initial investment of 7

billion yuan ($1 billion) for construction, with ongoing operational budgets that remain classified but are believed to be substantial [3].

Chinese quantum capabilities have achieved notable milestones in quantum communications, where China operates the world's largest quantum communication network spanning 12,000 kilometers and including two quantum satellites. This infrastructure provides China with quantum-secure communication capabilities that are theoretically immune to interception, offering significant advantages for government and military communications.

However, China's quantum ecosystem faces challenges in research commercialization and private sector engagement. Unlike the United States, where companies like Google, IBM, and IonQ drive much of the innovation, China's quantum development remains heavily concentrated in state-led research institutes with limited private investment [3].

Recent collaborative efforts between China and Russia, including testing of "unbreakable" quantum satellite communication systems connecting Moscow and Ürümqi, signal the emergence of quantum technology alliances that could challenge Western technological leadership [26].

5.2. United States Quantum Initiative

The United States has allocated approximately $3.5 billion in public quantum technology investments, a figure that, while smaller than China's commitment, is complemented by substantial private sector investment from technology giants and quantum startups [27]. The National Quantum Initiative Act of 2018 established a coordinated approach to quantum research across federal agencies, while the CHIPS and Science Act of 2022 provided additional funding for quantum research and development.

U.S. quantum leadership has historically relied on its world-class universities, entrepreneurial ecosystem, and private sector innovation. Companies like IBM, Google, IonQ, and Rigetti have made significant advances in quantum hardware and software, often building on research conducted at universities with federal funding support.

The U.S. approach emphasizes public-private partnerships and technology transfer from academic research to commercial applications. The Bayh-Dole Act enables universities to license federally funded research to private companies, creating incentives for commercial quantum development. However, recent policy proposals to expand march-in rights could potentially discourage private investment in quantum technologies [27].

Strategic concerns about Chinese quantum advancement have led to new export controls and investment restrictions targeting quantum technologies. The Treasury Department's October 2024 restrictions on U.S. investments in Chinese quantum companies reflect growing recognition of quantum technologies' national security implications [28].

The United States maintains significant advantages in quantum talent and re-

search output, with American universities attracting leading quantum researchers from around the world. However, sustaining this leadership requires continued investment and policy support for quantum research, education, and commercial development.

5.3. European Union Quantum Flagship

The European Union has committed approximately $7 billion to quantum technologies through the Quantum Flagship program and related initiatives, positioning Europe as a significant player in global quantum competition [25]. The EU's approach emphasizes technological sovereignty and coordinated development across member states.

The European Quantum Communication Infrastructure (EuroQCI) initiative aims to build a continental quantum communication network connecting strategic sites via terrestrial fiber and satellite-based links. This infrastructure would provide quantum-secure communications for government, critical infrastructure, and sensitive commercial applications across Europe.

Individual European countries have launched substantial quantum programs, with France announcing a 1.8-billion-euro five-year investment plan in 2021 and Germany allocating significant resources through its quantum initiative. The coordination of national and EU-level programs aims to create collaboration while avoiding duplication of effort.

European quantum policy emphasizes controls on dual-use technology and the protection of critical quantum capabilities from foreign investment and technology transfer. The EU has identified quantum technologies as critical for economic security and has proposed enhanced screening of foreign investments in quantum companies.

The March 2024 European Declaration on Quantum Technologies, signed by 21 member states, commits Europe to becoming the "quantum valley" of the world, emphasizing the strategic importance of quantum leadership for European competitiveness and security [25].

5.4. Other National Quantum Programs

Numerous other countries have launched significant quantum technology programs, recognizing the strategic importance of quantum capabilities for national competitiveness and security. Japan's Q-LEAP initiative, launched in 2018, focuses on quantum simulation, sensing, and computing with substantial government investment [29].

Australia has invested AU$893 million in quantum technologies, with the Centre of Excellence for Quantum Computation and Communication Technology (CQC2T) leading research efforts. The country has produced notable quantum scientists, such as Professor Michelle Simmons, who was named Australian of the Year in 2018 for her contributions to quantum computing [29].

Canada, the United Kingdom, India, and other nations have established quan-

tum programs with varying focuses and levels of investment. The UK government committed $905 million to quantum computing development, while India has launched national missions in quantum technologies.

Russia has established the Quantum Technologies Roadmap-, with support from state-owned organizations, including Rosatom, targeting the construction of 30 - 100 qubit computers by 2024 and 1000-qubit systems by 2030. The program includes quantum computing, communications, and sensing components [4].

These diverse national programs create a complex global quantum ecosystem with opportunities for collaboration and competition. International coordination through organizations such as the Global Partnership on AI and through bilateral quantum cooperation agreements helps manage this complexity while advancing quantum science and technology.

Table 2 captures the scale of national and multinational commitment to quantum science, highlighting that strategic focus, funding models, and policy direction differ across geopolitical blocs. These investments are leading to regional differences in innovation, standard-setting, and preparedness for quantum cybersecurity risks, factors that will shape cryptographic agility, technology access, and cyber resilience globally.

Table 2. Global quantum technology investment landscape (2024).

Country/Region	Estimated Public Investment (USD)	Strategic Focus Areas	Notable Initiatives/Features
China	$15 billion	Quantum comm, computing, defense	National Laboratory for Quantum Info Sciences, 12,000+ km quantum comm network, state-driven
European Union	$7 billion	Quantum comm, computing, sovereignty	Quantum Flagship, EuroQCI continental network, coordinated through 21 states
United States	$3.5 billion	Quantum R&D, commercialization	National Quantum Initiative Act, strong public-private sector, CHIPS Act funding
Japan	(not specified; large)	Quantum simulation, sensing, computing	Q-LEAP, government-led research, significant talent and infrastructure investments
Australia	AU$893 million	Quantum computation, commercialization	Centre of Excellence for Quantum Computation and Communication Technology (CQC2T)
United Kingdom	$905 million	Quantum computing, innovation	National Quantum Technologies Programme, talent and industry focus
Russia	(not specified; large)	Quantum computing, comm, sensing	Quantum Technologies Roadmap, 1000-qubit goal by 2030 (state-led)
India	(not specified; large)	National missions, various domains	Launch of national missions in quantum tech
Canada	(not specified)	Quantum science and applications	Longstanding research and collaborative initiatives

6. Strategic Timeline and Critical Milestones

The rapid evolution of quantum computing and the associated cryptographic risks have made strategic planning and timely action essential for organizations worldwide. A coordinated transition to quantum-resistant security requires clear awareness of emerging standards, regulatory timelines, and the projected pace of quantum advancements. This section outlines the key phases and milestones shaping the global post-quantum migration, from the introduction of new cryptographic standards and early adoption efforts to the anticipated timeline for quantum threats and the long-term goal of quantum-safe digital infrastructure. By understanding this strategic timeline, organizations and policymakers can prioritize resources, mitigate risk, and ensure resilience as the quantum era approaches.

6.1. 2024-2025: Standards and Early Adoption

The period from 2024-2025 represents a critical juncture for quantum cybersecurity preparedness, marked by the finalization of NIST post-quantum cryptography standards and the beginning of organizational transition planning. The August 2024 publication of FIPS 203, FIPS 204, and FIPS 205 provides organizations with standardized quantum-resistant algorithms for immediate implementation [2].

Early adoption during this period focuses on risk assessment, algorithm evaluation, and pilot implementations. Organizations must inventory their cryptographic assets, assess quantum vulnerability, and develop migration strategies that balance security requirements with operational constraints. The selection of additional algorithms, including HQC in March 2025, provides backup options and algorithmic diversity for long-term security [30].

Industry leaders are beginning to implement quantum-safe cryptography, with companies like Apple introducing post-quantum cryptography for iMessage in February 2024 and Google adopting ML-KEM for internal communications [30]. These early implementations provide valuable experience and best practices for broader organizational adoption.

Regulatory guidance continues to evolve during this period, with government agencies developing sector-specific recommendations for post-quantum transitions. The Quantum Computing Cybersecurity Preparedness Act requires federal agencies to inventory vulnerable systems and prepare for migration, while similar initiatives are emerging at state and international levels [31].

6.2. 2025-2028: Global Transition Period

The 2025-2028 timeframe represents the critical window for large-scale migration to post-quantum cryptography across government, industry, and critical infrastructure. This period allows organizations to complete comprehensive transitions before quantum threats become practical realities [32].

Government agencies must lead by example during this transition period, implementing post-quantum cryptography across federal systems while providing

guidance and support for private sector adoption. The Office of Management and Budget (OMB) is required to issue detailed migration guidance within 1 year of the NIST standard's publication, establishing timelines and requirements for federal agency transitions [33].

Critical infrastructure sectors must prioritize high-risk systems and essential services for early post-quantum implementation. Power grids, financial payment systems, healthcare networks, and defense communications are priority targets for quantum-resistant upgrades due to their national security and economic importance [34].

International coordination becomes increasingly important during this period as organizations implement systems that must interoperate across borders. Standards harmonization, mutual recognition of post-quantum implementations, and coordinated vulnerability assessments help ensure global cyber resilience.

The technology industry must scale post-quantum cryptography implementations to support mass adoption. Hardware security modules, cryptographic libraries, and security protocols require updates to support post-quantum algorithms while maintaining performance and compatibility with existing systems.

6.3. 2030: Projected Quantum Threat Emergence

The year 2030 represents a consensus estimate for when quantum computers may achieve sufficient capability to threaten widely deployed cryptographic systems. While substantial uncertainty remains around this timeline, the potential consequences of being unprepared necessitate treating 2030 as a critical deadline for post-quantum readiness.

NIST's guidance recommends deprecating vulnerable cryptographic systems by 2030, meaning organizations should stop deploying new systems that use quantum-vulnerable algorithms and begin phasing out existing implementations. This timeline provides a buffer against uncertainty while recognizing the lead time required for comprehensive transitions [1].

Quantum computing capabilities are likely to emerge gradually rather than suddenly, with early systems potentially capable of breaking smaller key sizes before advancing to full RSA-2048 capability. Organizations must monitor developments in quantum computing and adjust their security postures accordingly.

The 2030 timeframe also represents a deadline for international cooperation on quantum cybersecurity standards and incident response. As quantum capabilities emerge, the international community must establish frameworks to address quantum-enabled cyberattacks and coordinate defensive responses.

6.4. Post-2030: Quantum-Safe Digital Infrastructure

Beyond 2030, the digital ecosystem must assume that quantum computers capable of breaking traditional cryptography are available to potential adversaries. This requires comprehensive implementation of quantum-resistant systems and ongoing vigilance against new quantum threats [35].

Continued algorithm research and standardization will be necessary as quantum computing capabilities advance and new cryptanalytic techniques emerge. The cryptographic community must maintain multiple algorithmic approaches and be prepared to transition to new systems if current post-quantum algorithms are successfully attacked.

Quantum key distribution and other quantum-native security technologies may complement post-quantum cryptography to provide additional layers of protection. However, these technologies require specialized infrastructure and may not be practical for all applications. However, QKD's dependence on specialized photonic hardware, dedicated fiber or satellite links, and point-to-point topology makes it unsuitable as a general replacement for algorithmic PQC; it remains best suited for high-assurance, infrastructure-rich environments such as inter-data-center government links or central bank settlement networks, while PQC provides the practical migration path for broad organizational deployment. The post-2030 period will require ongoing assessment of quantum threats and adaptive security measures that can respond to evolving capabilities. Organizations must build cryptographic agility into their systems to enable rapid responses to new threats or breakthrough attacks against existing algorithms [36].

7. Implementation Challenges and Organizational Preparedness

Preparing organizations for the transition to post-quantum cryptography is a complex undertaking, requiring both technical upgrades and comprehensive change management. The migration involves overcoming significant implementation barriers, adapting legacy systems, budgeting for new costs, and building workforce expertise. Organizations must also ensure consistent testing and validation to maintain security and operational reliability throughout the transition. This section explores the key challenges associated with deploying quantum-resistant cryptography, emphasizing the importance of organizational readiness, risk management, and coordinated action to achieve resilient security in the quantum era.

7.1. Technical Implementation Barriers

The transition to post-quantum cryptography presents numerous technical challenges that organizations must address to ensure successful migration. Performance implications represent perhaps the most immediate concern, as post-quantum algorithms often require more computational resources and memory than current systems. ML-KEM key establishment, while generally competitive with elliptic curve alternatives, may require optimization for high-throughput applications [2].

Signature verification times can be significantly longer for some post-quantum algorithms, with ML-DSA requiring 2-10 times more computation than ECDSA depending on parameter sets and implementation optimization [37]. Organiza-

tions must evaluate these performance implications for their specific use cases and consider hardware upgrades or architectural changes to maintain acceptable response times.

Key and signature size increases present another significant challenge, particularly for bandwidth-constrained environments and embedded systems. ML-DSA signatures range from 2420 to 4595 bytes compared to 64 bytes for ECDSA signatures, potentially impacting network protocols, storage systems, and device memory requirements [38].

Legacy system integration poses particular difficulties, as older systems may lack the computational resources or architectural flexibility to support post-quantum algorithms. Industrial control systems, embedded devices, and specialized hardware platforms may require significant modifications or complete replacement to achieve quantum resistance.

Cryptographic library updates across diverse software ecosystems require coordinated effort from vendors, developers, and system administrators. Ensuring that all components in complex systems support consistent post-quantum implementations while maintaining security and interoperability requires careful planning and testing.

7.2. Technical Implementation Barriers

Post-quantum cryptography migration requires comprehensive organizational change management that extends beyond technical implementation to encompass policy, training, and cultural adaptation. Senior leadership must understand quantum threats and commit resources necessary for effective transitions, often requiring substantial investment in technology, personnel, and process changes [39].

Workforce development represents a critical challenge, as many IT professionals lack deep familiarity with cryptographic systems and may require training to understand post-quantum algorithms, implementation requirements, and security implications. Organizations must invest in education and skill development to build internal capabilities for post-quantum transitions [40].

Risk assessment and prioritization frameworks must be developed to guide migration decisions, balancing quantum threat timelines against operational requirements, budget constraints, and technical feasibility. Organizations need systematic approaches to identify high-priority systems, evaluate migration options, and sequence implementation activities [41].

Vendor management becomes increasingly complex as organizations depend on third-party providers for post-quantum cryptography implementations. Procurement policies must include quantum-readiness requirements, while vendor assessment processes must evaluate post-quantum capabilities, roadmaps, and support commitments.

Supply chain considerations extend beyond immediate vendors to encompass the entire ecosystem of hardware, software, and service providers that support or-

ganizational operations. Ensuring quantum resilience requires coordinated effort across supply chains to address vulnerabilities and maintain security standards [42].

7.3. Cost and Resource Requirements

Post-quantum cryptography migration involves substantial costs that organizations must plan for and budget appropriately. Hardware upgrades may be necessary to support the increased computational requirements of post-quantum algorithms, particularly for high-throughput applications and performance-sensitive systems.

Software licensing and development costs can be high, especially for organizations with custom applications or specialized systems that require post-quantum integration. Professional services for migration planning, implementation, and testing add to the overall cost of transition [43].

Training and workforce development represent ongoing investments in organizational capability building. Cryptographic expertise is specialized and expensive, requiring organizations to either develop internal capabilities or rely on external consultants and service providers.

Compliance and audit costs may increase as organizations implement post-quantum systems while maintaining regulatory compliance. Demonstrating the security and effectiveness of new cryptographic implementations may require additional testing, documentation, and third-party validation.

Opportunity costs from delayed implementation can be substantial if quantum threats materialize faster than expected. Organizations that delay migration may face emergency transitions with higher costs, reduced security, and greater operational disruption.

7.4. Testing and Validation Framework

Comprehensive testing and validation frameworks are essential to ensure that post-quantum implementations provide the expected level of security while maintaining operational reliability. Cryptographic testing must verify that post-quantum algorithms are implemented correctly and provide appropriate security levels for specific use cases [44].

Interoperability testing becomes critical as organizations implement post-quantum systems that must communicate with partners, customers, and service providers using different cryptographic implementations. Standardized test suites and validation tools help ensure compatibility across diverse systems and platforms.

Performance testing under realistic operational conditions is necessary to validate that post-quantum systems meet response time, throughput, and reliability requirements. Load testing, stress testing, and long-term stability testing help identify potential issues before production deployment [45].

Security validation requires ongoing assessment of post-quantum implementations against evolving threats and attack techniques. Regular security audits, penetration testing, and vulnerability assessments help maintain security posture as

quantum capabilities advance [46].

Compliance validation ensures that post-quantum implementations meet regulatory requirements and industry standards. This may require formal certification processes, third-party assessments, and ongoing compliance monitoring [47].

Table 3 outlines the major technical, operational, and organizational hurdles that must be addressed when migrating to post-quantum cryptography across core sectors. It highlights challenges such as the higher computational and storage demands of post-quantum algorithms, difficulties integrating these algorithms into older systems, the need for robust testing and validation, increased costs, shortages of skilled personnel, vendor coordination issues, and the importance of effective change management. These issues affect sectors differently but collectively underscore the complexity and urgency of preparing for quantum-resistant security amidst evolving threats and infrastructural constraints.

Table 3. Major challenges in migrating to post-quantum cryptography.

Challenge Type	Description	Sectoral Impact	Example/Notes
Performance Impact	PQC algorithms often require more computational resources for key establishment and signatures.	All sectors, especially finance, defense	Signature verification may be 2 - 10 times slower.
Key & Signature Size	Post-quantum keys/signatures are significantly larger, affecting bandwidth/storage.	Embedded & constrained systems, critical infra	ML-DSA signatures: 2420 - 4595 bytes vs. 64 bytes (ECDSA).
Integration with Legacy Systems	Older systems may lack resources or flexibility to support PQC.	Critical infrastructure, healthcare, defense	May require extensive upgrades or replacements.
Testing & Validation	Ensuring correct and secure PQC implementation, interoperability, and compliance.	All sectors	Demands extensive testing, validation, and new protocols.
Cost & Resources	Upgrades in hardware, software, training, and compliance burden increased overall costs.	All sectors	Delays or hurried migrations can raise costs/disruption.
Workforce Skills	A shortage of professionals trained in PQC hinders implementation.	All sectors	Ongoing investment in education/training required.
Vendor & Ecosystem	Need for quantum-readiness in third-party solutions and throughout the supply chain.	All sectors	Complex vendor coordination, contracts, SLAs.
Change Management	Need for leadership buy-in, risk frameworks, and clear communication across the organization.	All sectors	Essential for efficient, coordinated migration.

8. Policy and Regulatory Considerations

The rise of quantum computing and its implications for cybersecurity demand comprehensive policy and regulatory responses from governments, standard-set-

ting bodies, and industries worldwide. Developing effective frameworks is essential to ensuring national security, protecting critical infrastructure, and maintaining trust in digital systems as organizations transition to quantum-resistant cryptography. This section examines the evolving landscape of quantum cybersecurity policy, exploring national security priorities, international cooperation, regulatory compliance, industry standards, and legal considerations. By addressing these areas, stakeholders can build resilient and adaptive governance structures that support secure operations in the quantum era.

8.1. National Security Policy Framework

Quantum cybersecurity policy development requires coordination across multiple government agencies and levels of authority, from national security organizations to sector-specific regulators. The Quantum Computing Cybersecurity Preparedness Act of 2022 established a framework for federal agency preparation, requiring an inventory of vulnerable systems and migration planning within specified timelines [48].

The National Security Agency has issued guidance recognizing quantum threats and recommending immediate action to implement quantum-resistant cryptography. The NSA's Commercial National Security Algorithm Suite includes post-quantum-approved algorithms and provides implementation guidance for national security systems [14].

Export control policies must balance national security concerns with the need for international cooperation and commercial development. Recent restrictions on quantum technology investments in China reflect a growing recognition of the strategic importance of quantum capabilities, while allies require coordination to maintain technological interoperability.

Critical infrastructure protection policies must address quantum vulnerabilities while maintaining operational continuity and economic competitiveness. Sector-specific regulations and public-private partnerships provide mechanisms for coordinated response to quantum threats [49].

Intelligence and defense policies must address both offensive and defensive quantum capabilities, ensuring that national security organizations can maintain technological advantages while protecting against quantum-enabled threats from adversaries [50].

8.2. International Cooperation and Standards

International cooperation on quantum cybersecurity standards and policies is essential given the global nature of digital communications and the transnational character of cyber threats. Organizations such as NATO have begun developing quantum strategies to maintain interoperability among allies and collective defense capabilities [20].

Bilateral and multilateral agreements on quantum technology cooperation help coordinate research, share best practices, and maintain technological partnerships

between allied nations. The U.S.-EU quantum cooperation agreements and similar partnerships with other allies provide frameworks for ongoing collaboration.

International standards organizations, including ISO, IEC, and ITU, are developing quantum cybersecurity standards that complement national efforts like NIST's post-quantum cryptography standardization. Harmonization of international standards helps ensure global interoperability and reduces compliance complexity for multinational organizations [51].

Trade policy considerations include managing technology transfer restrictions while maintaining open research collaboration and commercial development. Balancing national security concerns with innovation and economic growth requires nuanced approaches to quantum technology policy.

Diplomatic initiatives must address quantum cybersecurity as part of broader cyber norms and responsible state behavior in cyberspace. International frameworks for responding to quantum-enabled cyberattacks and maintaining stability in the quantum era require ongoing diplomatic engagement [52].

8.3. Regulatory Compliance and Industry Standards

Financial services regulators are beginning to address quantum threats through examination guidance, supervisory expectations, and risk management requirements. The FFIEC has issued guidance on quantum risk assessment and preparedness planning for financial institutions [22].

Healthcare regulators must balance quantum cybersecurity requirements with patient safety, privacy protection, and operational continuity. HIPAA and international health privacy regulations may require specific approaches to post-quantum implementation that protect patient information while maintaining care delivery capabilities [53].

Critical infrastructure regulations across sectors, including energy, transportation, and telecommunications, must incorporate quantum cybersecurity requirements while avoiding prescriptive mandates that could quickly become outdated as technology evolves [49].

Professional and industry standards organizations are developing quantum cybersecurity frameworks that provide practical guidance for implementation while maintaining flexibility for technological evolution. These frameworks help organizations understand requirements and best practices for post-quantum transitions [47].

Audit and compliance requirements must evolve to address post-quantum cryptography implementations, including validation of algorithm implementations, security assessments, and ongoing monitoring of quantum threat developments.

8.4. Legal and Liability Considerations

Legal frameworks for quantum cybersecurity must address liability, negligence, and duty of care as organizations implement post-quantum protections. Courts and regulators may increasingly expect reasonable quantum cybersecurity measures

as standards become established and threats materialize [54].

Intellectual property considerations include patent landscapes for post-quantum algorithms, licensing requirements, and potential constraints on implementation. NIST has carefully evaluated intellectual property issues for standardized algorithms, but organizations must consider broader patent implications for their implementations [55].

Data breach notification requirements may need updating to address quantum-specific threats and "harvest now, decrypt later" scenarios where data compromise may not be immediately apparent. Legal frameworks must account for the delayed nature of quantum cryptographic attacks [56].

Contract and procurement law must evolve to include quantum cybersecurity requirements, service level agreements, and liability allocation for post-quantum implementations. Standard contract terms and industry practices must reflect quantum threat realities.

International legal cooperation on quantum cybersecurity includes mutual legal assistance treaties, extradition agreements, and frameworks for attribution and response to quantum-enabled cyberattacks. Legal mechanisms must keep pace with technological developments to maintain effective deterrence and accountability [54] [57].

9. Discussion

Quantum cybersecurity has firmly established itself as a critical strategic priority at the intersection of technological innovation, national security, and economic competitiveness. The rise of quantum computing fundamentally disrupts the assumptions underpinning modern digital security. As quantum hardware advances rapidly toward practical implementation, with projections for fault-tolerant systems emerging around 2030, the threat to legacy encryption systems, most notably those dependent on RSA and elliptic-curve cryptography, has shifted from distant speculation to an immediate risk. Shor's algorithm, coupled with experimental progress and algorithmic improvements, has slashed the resources needed to break widely used cryptosystems [8] [58] [59], with recent findings suggesting that breaking RSA-2048 is achievable with fewer than one million noisy qubits over a short timeframe. This acceleration has shifted the window for defensive preparation, creating an urgent need for organizations to address quantum risks before they materialize. The vulnerability landscape spans every critical sector, but with varying levels of exposure. Defense and military networks are particularly at risk, with 85% vulnerability projected by 2030 without the timely implementation of post-quantum cryptography, followed closely by financial services (78%), healthcare (70%), and critical infrastructure sectors (65%). The cascading risks posed by quantum threats in one sector can ripple into others due to the interconnected nature of digital infrastructure, directly impacting economic stability, public health, and national security. The "harvest now, decrypt later" scenario amplifies these concerns, as adversaries stockpile encrypted data with the intention of decrypting

it once quantum resources become available, jeopardizing not only sensitive current communications but also archival data that may retain strategic value for decades [60].

In response to these threats, the cryptographic community, with leadership from the U.S. National Institute of Standards and Technology, has developed and finalized a new generation of post-quantum cryptography standards, such as FIPS 203, 204, and 205, with additional diversity provided by new algorithms like HQC. These standards offer a foundation for quantum-resistant security, but their deployment is technically and logistically complex. Organizations must navigate challenges, including increased key and signature sizes, greater computational resource demands, performance variability across different algorithms, and the intricate work required to integrate new cryptography within legacy systems and complex software environments [61]. Cryptographic agility, designing systems to quickly shift between different cryptographic schemes as threats evolve, has become a cornerstone requirement [36] [39], as hybrid deployments balancing both classical and post-quantum primitives provide transitional security but also introduce new complexities. Early industry adopters have begun rolling out quantum-safe systems, offering valuable lessons for sector-wide migration, but a comprehensive transition remains a work in progress, hampered by the scale of global cryptographic reliance and the long lifecycles of many critical systems.

The geopolitical context further intensifies the urgency of decisive action. A quantum arms race is underway, with China's state-led investment reaching $15 billion, Europe's coordinated "Quantum Flagship" programs totaling $7 billion, and the United States channeling about $3.5 billion into both government and private research, supported by robust academic and corporate ecosystems. Each of these actors recognizes the immense military, economic, and technological power at stake in quantum leadership. Alliances and rivalries are evolving as policy and export controls are put in place, international science collaborations are recalibrated, and states move to secure not only quantum-technical advantages but also cryptographic sovereignty. Smaller countries, too, engage with bespoke programs, contributing to a diverse yet competitive quantum ecosystem that both enables vital scientific progress and raises new risks related to fragmentation and standardization.

Transitioning to a quantum-safe digital world is as much an organizational and governance challenge as it is a technical one. Organizations must formulate comprehensive migration strategies, starting from the inventory and risk assessment of their cryptographic assets, continuing through prioritized implementation and extensive testing, and requiring sustained workforce development and supply chain management. The costs are high, not just in hardware upgrades and software development, but in the investment of time, skills, and organizational change management. Delay imposes its own risks, including higher costs, emergency transitions, and greater disruption if threats materialize faster than anticipated. Regulatory frameworks are evolving to mandate quantum readiness, with initia-

tives like the U.S. Quantum Computing Cybersecurity Preparedness Act and new guidance from sector-specific regulators in financial services and healthcare. International standardization bodies are moving to harmonize requirements, as interoperability is essential for global commerce and security, but this momentum must be matched by legal adaptations to address quantum-specific threats, liability, and data-breach implications.

Going forward, the quantum cybersecurity landscape will be shaped by ongoing advances in quantum computing, cryptographic research, and regulatory coordination. Organizations and nations must enable continual monitoring and adaptation as threat models change and new defensive technologies mature. Investing in cryptographic agility, AI-based threat detection, and multi-layered security approaches, alongside continuous workforce development and international collaboration, will be key to preserving digital trust. The long-term vision is a resilient, quantum-safe digital ecosystem, where privacy, efficiency, and innovation co-exist with sustained public and organizational confidence. Acting now, before the full quantum threat materializes, confers not only a protective advantage but also positions organizations and states to harness the benefits of quantum technology for secure growth and leadership in the digital era [62].

Several limitations of this analysis warrant acknowledgment to allow readers to calibrate its conclusions appropriately. First, the timeline for cryptographically relevant quantum computers remains fundamentally uncertain: the 2030 threshold cited throughout this article represents an expert-consensus planning horizon endorsed by NIST and NSA rather than a confirmed engineering prediction, and quantum hardware development could prove either faster or substantially slower depending on progress in error correction, qubit coherence, and fault-tolerant algorithm compilation. Second, the sectoral vulnerability percentages reported in Section 4 are scenario-based projections derived from sector-specific government and industry reports rather than primary empirical data; they reflect the proportion of assets that rely on vulnerable algorithms, not directly measured probabilities of successful quantum attacks at any given time. Third, the national investment figures presented in Section 5 draw primarily on publicly announced government commitments, policy documents, vendor roadmaps, and journalistic sources; they exclude classified expenditure, embedded procurement, and private-sector co-investment, and should be read as directional magnitudes rather than as audited national accounts. Fourth, quantum computing is a rapidly evolving field, and new algorithmic improvements, hardware breakthroughs, or successful cryptanalytic attacks on standardized post-quantum algorithms could alter the risk calculus faster than this or any static review can reflect. Readers are encouraged to monitor NIST, NSA, and peer-reviewed cryptography literature for developments that may revise the timeline, algorithmic, or investment conclusions presented here.

10. Future Outlook and Strategic Recommendations

As quantum technologies advance, organizations and policymakers face an evolv-

ing landscape of both risks and opportunities. The future of quantum cybersecurity will be shaped by emerging technical developments, the ongoing adoption of post-quantum cryptography, and the strength of national and international collaboration. Proactive preparation, investment in workforce development, and flexible security strategies are essential to keep pace with technological progress and shifting threat timelines. This section explores the road ahead for quantum cybersecurity, offering strategic recommendations and highlighting the long-term vision for creating a secure, resilient, and trusted digital ecosystem in the quantum era.

10.1. Emerging Technological Developments

Quantum cybersecurity will continue evolving as both quantum computing capabilities and defensive technologies advance. Hardware improvements in quantum computers may accelerate threat timelines, while advances in quantum error correction could enable larger-scale quantum algorithms sooner than currently anticipated. Organizations must stay current with quantum computing developments and adjust their security strategies accordingly.

Post-quantum cryptography will likely see continued algorithm development and standardization as researchers identify new mathematical approaches and address limitations of current systems. NIST's ongoing evaluation of additional algorithms provides backup options and algorithmic diversity, while international standardization efforts may introduce alternative approaches that organizations should consider.

Quantum key distribution and quantum-native security technologies may complement post-quantum cryptography by providing additional layers of protection for high-value communications and data. While QKD requires specialized infrastructure and has distance limitations, advances in quantum repeaters and satellite-based systems may expand its practical applicability.

Hybrid classical-quantum cryptographic systems may emerge as practical approaches that combine the proven security of classical algorithms with the quantum resistance of post-quantum systems. These approaches could provide additional security margins while maintaining compatibility with existing infrastructure.

Artificial intelligence and machine learning may play increasing roles in quantum cybersecurity, from optimizing post-quantum algorithm implementations to detecting quantum-enabled attacks and automating defensive responses. The integration of AI with quantum cybersecurity tools could enhance both offensive and defensive capabilities.

10.2. Organizational Prioritization

Organizations must prioritize immediate assessment of their quantum vulnerability and development of comprehensive migration strategies. This includes inventorying cryptographic assets, evaluating post-quantum options, and establishing implementation timelines aligned with threat projections and business re-

quirements.

Investment in cryptographic agility should be a top priority, enabling organizations to rapidly adopt new algorithms as they become available or migrate away from compromised systems if attacks emerge. Modular cryptographic implementations and clear separation between cryptographic and application logic facilitate future transitions.

Workforce development in quantum cybersecurity requires ongoing investment in training, certification, and skill building. Organizations should identify key personnel responsible for quantum cybersecurity and equip them with the necessary education and resources to lead organizational transitions.

Partnership and collaboration strategies should encompass vendors, industry groups, government agencies, and international partners to share best practices, coordinate responses, and maintain interoperability. No organization can address quantum cybersecurity challenges in isolation.

Continuous monitoring and adaptation capabilities are essential as quantum threats evolve and new defensive technologies emerge. Organizations must establish processes to track quantum developments, assess their implications, and adjust security strategies accordingly.

10.3. Governmental Policies

National governments should accelerate the adoption of post-quantum cryptography across government systems while providing leadership and guidance for private-sector transitions. Government procurement policies can drive market adoption by requiring quantum-resistant capabilities in technology acquisitions.

International cooperation frameworks must be strengthened to address the global nature of quantum cybersecurity challenges. This includes harmonizing standards, coordinating incident response, and maintaining technological partnerships between allied nations.

Regulatory agencies should develop quantum cybersecurity requirements that provide clear expectations while maintaining flexibility for technological evolution. Risk-based approaches that focus on outcomes rather than specific technologies allow organizations to choose appropriate solutions for their circumstances.

Research and development investment must continue in both quantum computing and quantum-resistant technologies to maintain technological leadership and security capabilities. Public-private partnerships can leverage government resources while enabling commercial innovation and deployment.

Education and workforce development programs should be expanded to build national capabilities in quantum cybersecurity. University programs, professional training, and public awareness initiatives help ensure adequate human resources for the quantum transition.

10.4. Long-Term Vision for Quantum-Safe Society

The ultimate goal of quantum cybersecurity efforts is to create a digital ecosystem

that remains secure and trustworthy in the presence of quantum computers. This requires not only technical implementation of quantum-resistant cryptography but also adaptation of policies, processes, and organizational cultures to address quantum realities.

Quantum-safe digital infrastructure should provide security, privacy, and trust that equals or exceeds current capabilities while enabling new applications and services. Post-quantum cryptography, quantum key distribution, and other quantum-safe technologies should work together to create comprehensive protection.

International stability and cooperation in the quantum era require shared norms, standards, and frameworks that promote responsible development and use of quantum technologies. Preventing a "quantum divide" between nations and ensuring broad access to quantum-safe technologies serve global security interests.

Economic competitiveness in the quantum era will depend on early adoption of quantum-safe technologies and continued investment in quantum research and development. Nations and organizations that successfully navigate the quantum transition will be better positioned for future growth and innovation.

Public trust in digital systems must be maintained throughout the quantum transition through transparent communication, effective security implementation, and demonstration of continued protection for personal and organizational data. Success requires not only technical achievement but also public confidence and acceptance.

11. Conclusion

Quantum computing is transitioning from theoretical possibility to operational threat on a compressed timeline. Recent algorithmic advances suggest that RSA-2048 encryption, the backbone of modern digital infrastructure, could be compromised by a quantum computer with fewer than 1 million noisy qubits operating for approximately 1 week, a 20-fold reduction from prior estimates. With major quantum hardware programs targeting systems of that scale by 2030, the window for preventive action is narrowing. The finalization of NIST's post-quantum cryptography standards in August 2024, FIPS 203, 204, and 205, provides the algorithmic foundation for quantum-safe migration, but standards alone are insufficient. A comprehensive cryptographic transition requires asset inventory, prioritized migration planning, cryptographic agility, legacy system remediation, and sustained workforce development across all sectors. Sectoral exposure is both substantial and uneven. Defense and national security systems face the highest projected cryptographic vulnerability (approximately 85% by 2030), followed by financial services (78%), healthcare (70%), and critical infrastructure (65%). These figures reflect the proportion of sector assets that rely on RSA and ECC protocols rather than on measured attack probabilities, but they signal clear priorities for investment and regulatory attention. The "harvest now, decrypt later" threat extends the urgency beyond Q-Day itself: data collected today under classical encryption may be decrypted by adversaries once quantum capabilities arrive, mak-

ing delay in migration decisions a present-day risk, not a future one. Geopolitically, quantum technology has become a dimension of strategic competition. China's state-led investment of approximately $15 billion, Europe's €7 billion Quantum Flagship, and the United States' $3.5 billion public commitment reflect each power's recognition that quantum leadership carries decisive advantages in cryptography, communications, and intelligence. Maintaining technological sovereignty and alliance interoperability in this environment requires coordinated adoption of post-quantum standards, export discipline, and sustained international cooperation. The strategic imperative is unambiguous: organizations and governments that act now, conducting vulnerability assessments, implementing PQC pilots, and embedding cryptographic agility into system architectures, will be positioned to protect data, maintain operational continuity, and leverage quantum technologies for competitive advantage. Those who defer will face emergency transitions under adversarial conditions. The standards exist, the threat is advancing, and the cost of preparation is far lower than the cost of cryptographic failure.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] National Institute of Standards and Technology (2024) What Is Post-Quantum Cryptography? NIST Cybersecurity Resource Center.

[2] National Institute of Standards and Technology (2024) NIST Releases First 3 Finalized Post-Quantum Encryption Standards. NIST News Release.

[3] Merics (2024) China's Long View on Quantum Tech Has the US and EU Playing Catch-Up. Mercator Institute for China Studies.

[4] The Quantum Insider (2024) 15 Leading Quantum Computing Countries in 2024. The Quantum Insider.

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

[6] IBM Quantum (2024) Quantum Computing Roadmap and Milestones. IBM Research.

[7] Shor, P.W. (1994) Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings* 35*th Annual Symposium on Foundations of Computer Science*, Santa Fe, 20-22 November 1994, 124-134. https://doi.org/10.1109/sfcs.1994.365700

[8] Gidney, C. (2024) Factoring Integers with Sublinear Resources on a Superconducting Quantum Processor. Google Quantum AI.

[9] Ali, S., Wadho, S.A., Talpur, K.R., Talpur, B.A., Alshudukhi, K.S., Humayun, M. and Shah, A. (2025) Next-Generation Quantum Security: The Impact of Quantum Computing on Cybersecurity—Threats, Mitigations, and Solutions. *Computers and Electrical Engineering*, **128**, Article ID: 110649. https://doi.org/10.1016/j.compeleceng.2025.110649

[10] Grover, L.K. (1996) A Fast Quantum Mechanical Algorithm for Database Search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Compu-*

*ting-STOC'*96, Philadelphia, 22-24 May 1996, 212-219. https://doi.org/10.1145/237814.237866

[11] Pei, Z., Hong, C., Xia, F. and Wang, C. (2025) An Innovative Algorithm for Attacking Symmetric Ciphers Using D-Wave Quantum Annealing. *Tsinghua Science and Technology*, **30**, 2184-2194. https://doi.org/10.26599/tst.2024.9010231

[12] Singh, H. (2024) Managing the Quantum Cybersecurity Threat. In: Hammoudeh, M., Alessa, A.T., Sherbeeni, A.M., Firth, C.M. and Alessa, A.S., Eds., *Quantum Computing*, CRC Press, 142-158. https://doi.org/10.1201/9781003475286-9

[13] Aslam, A. (2025) Quantum Computing Threats to Cryptography: A Comprehensive Analysis of Vulnerabilities, Countermeasures, and Future-Proofing Strategies. https://doi.org/10.21203/rs.3.rs-6795420/v1

[14] National Security Agency (2022) Quantum Computing and Post-Quantum Cryptography. NSA Cybersecurity Information Sheet.

[15] Chen, L., Moody, D. and Liu, Y. (2017) NIST Post-Quantum Cryptography Standardization. *Transition*, **800**, Article 164.

[16] Gaborit, P., Aguilar-Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., *et al.* (2025) Hamming Quasi-Cyclic (HQC). NIST Post-Quantum Standardization, 4th Round. National Institute of Standards and Technology: Gaithersburg.

[17] Sharma, S., Ramkumar, K.R., Kaur, A., Hasija, T., Mittal, S. and Singh, B. (2023) Post-Quantum Cryptography: A Solution to the Challenges of Classical Encryption Algorithms. In: Agrawal, R., Kishore Singh, C., Goyal, A. and Singh, D.K., Eds., *Lecture Notes in Electrical Engineering*, Springer, 23-38. https://doi.org/10.1007/978-981-19-6383-4_3

[18] D'Anvers, J., Van Beirendonck, M. and Verbauwhede, I. (2023) Revisiting Higher-Order Masked Comparison for Lattice-Based Cryptography: Algorithms and Bit-Sliced Implementations. *IEEE Transactions on Computers*, **72**, 321-332. https://doi.org/10.1109/tc.2022.3197074

[19] Cybersecurity and Infrastructure Security Agency (2024) Quantum Computing Cybersecurity Preparedness Guidance. Department of Homeland Security.

[20] NATO (2024) NATO Quantum Strategy Summary. North Atlantic Treaty Organization.

[21] Financial Services Information Sharing and Analysis Center (2024) Quantum Threats to Financial Services Infrastructure. FS-ISAC Intelligence Report.

[22] Federal Financial Institutions Examination Council (2024) Quantum Computing Risks and Preparedness Guidance. FFIEC.

[23] Healthcare Information and Management Systems Society (2024) Quantum Cybersecurity Preparedness in Healthcare. HIMSS Policy Brief.

[24] Department of Homeland Security (2024) Critical Infrastructure Quantum Cyber-Security Assessment. DHS Office of Cybersecurity and Communications.

[25] European Parliament (2024) Quantum: What Is It and Where Does the EU Stand? European Parliamentary Research Service.

[26] Weber, V. (2024) The New Quantum Technology Race. *International Politik Quarterly*.

[27] Kim, J. and Monroe, C. (2024) America Is the Undisputed World Leader in Quantum Computing Even though China Spends 8x More on the Technology—But an Own Goal Could Soon Erode U.S. Dominancey. *Fortune*.

[28] Dobberstein, L. (2024) Chinese Chips, Quantum and AI Now on US Investment

Blacklist. *The Register*.

[29] Qureca (2025) Quantum Initiatives Worldwide 2025. Qureca Limited.

[30] World Economic Forum (2024) Quantum Computing Could Threaten Cybersecurity Measures. Here's Why and How Tech Firms Are Responding. World Economic Forum.

[31] United States Congress (2025) Quantum Computing Cybersecurity Preparedness Act. Public Law No: 117-260. https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf

[32] Coates, R. and Chhetri, M.B. (2024) Quantum Readiness: Unlocking the Quantum Advantage for Australian Industries. 2024 *IEEE International Conference on Quantum Computing and Engineering* (*QCE*), Montreal, 15-20 September 2024, 61-64. https://doi.org/10.1109/QCE60285.2024.10253

[33] Newhouse, W., Souppaya, M., Barker, W., Brown, C., Kampanakis, P., Manzano, M., *et al*. (1800) Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery. Nist Special Publication, 38B. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf

[34] Ricciardi Celsi, M. and Ricciardi Celsi, L. (2024) Quantum Computing as a Game Changer on the Path Towards a Net-Zero Economy: A Review of the Main Challenges in the Energy Domain. *Energies*, **17**, Article 1039. https://doi.org/10.3390/en17051039

[35] Imran, M., Altamimi, A. B., Khan, W., Hussain, S. and Alsaffar, M. (2024) Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Access*, **12**, 180048-180078.

[36] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O. and Hansen, R. (2022) Transitioning Organizations to Post-Quantum Cryptography. *Nature*, **605**, 237-243. https://doi.org/10.1038/s41586-022-04623-2

[37] Dinu, D. (2025) Migration to Post-Quantum Cryptography: From ECDSA to ML-DSA. https://eprint.iacr.org/2025/2025.pdf

[38] Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S. and Das, S. (2025) Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey. arXiv:2510.10436.

[39] Hasan, K.F., Simpson, L., Baee, M.A.R., Islam, C., Rahman, Z., Armstrong, W., *et al*. (2024) A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. *IEEE Access*, **12**, 23427-23450. https://doi.org/10.1109/access.2024.3360412

[40] Victor, D. (2025) Workforce Skill Gaps and Training Needs for Implementing Post-Quantum Encryption. https://www.researchgate.net/publication/397012939_Workforce_Skill_Gaps_and_Training_Needs_for_Implementing_Post-Quantum_Encryption

[41] Arslan, B., Ulker, M., Akleylek, S. and Sagiroglu, S. (2018) A Study on the Use of Quantum Computers, Risk Assessment and Security Problems. 2018 6*th International Symposium on Digital Forensic and Security* (*ISDFS*), Antalya, 22-25 March 2018, 1-6. https://doi.org/10.1109/isdfs.2018.8355318

[42] Biswas, J., Mijwil, M.M., Farhan, L. and Alkattan, H. (2025) Quantum Computing in Risk Management and Supply Chain Resilience. In: Dutta, P.K., Bhattacharya, P., Verma, J.P., Chopra, A., Kundu, N.K. and Aurangzeb, K., Eds., *Quantum Computing and Artificial Intelligence in Logistics and Supply Chain Management*, Chapman and Hall/CRC, 119-128. https://doi.org/10.1201/9781003498292-8

[43] Weinberg, A.I. (2025) Preparing for the Post Quantum Era: Quantum Ready Architecture for Security and Risk Management (QUASAR)—A Strategic Framework for Cybersecurity. arXiv:2505.17034.

[44] Fernando, P. (2025) Post-Quantum Cryptography: Current Developments, Challenges, and Future Directions. *Path of Science*, **11**, 4001-4012. https://doi.org/10.22178/pos.119-4

[45] Montenegro, J.A., Rios, R. and Lopez-Cerezo, J. (2026) A Performance Evaluation Framework for Post-Quantum TLS. *Future Generation Computer Systems*, **175**, Article 108062. https://doi.org/10.1016/j.future.2025.108062

[46] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., *et al.* (2023) Post-Quantum Security: Opportunities and Challenges. *Sensors*, **23**, Article 8744. https://doi.org/10.3390/s23218744

[47] Erol, V. (2025) The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. https://www.preprints.org/manuscript/202509.1720/download/final_file

[48] Congress.gov (2022) H.R.7535—Quantum Computing Cybersecurity Preparedness Act. https://www.congress.gov/bill/117th-congress/house-bill/7535

[49] Kumar, S., Klappenecker, A., Brown, G. and Saravanan, S. (2025) Quantum Apocalypse: Fortifying Critical Infrastructure in the Age of Cyber Warfare. *European Conference on Cyber Warfare and Security*, **24**, 293-301. https://doi.org/10.34190/eccws.24.1.3757

[50] Naseer ALSarmi, H.S. (2025) Strategic Review of Quantum Capabilities in Military and National Cyber Defense. 2025 3*rd International Conference on Inventive Computing and Informatics* (*ICICI*), Bangalore, 4-6 June 2025, 1556-1562. https://doi.org/10.1109/icici65870.2025.11069595

[51] Geremew, A. and Mohammad, A. (2024) Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing. *International Journal on Engineering, Science and Technology*, **6**, 338-365. https://doi.org/10.46328/ijonest.240

[52] Radanliev, P. (2025) Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, **9**, 28-78. https://doi.org/10.1080/23742917.2024.2312671

[53] Gupta, K., Saxena, D., Rani, P., Kumar, J., Makkar, A., Kumar Singh, A., *et al.* (2025) An Intelligent Quantum Cyber-Security Framework for Healthcare Data Management. *IEEE Transactions on Automation Science and Engineering*, **22**, 6884-6895. https://doi.org/10.1109/tase.2024.3456209

[54] Balarabe, K. (2025) Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap. *European Journal of Risk Regulation*, **16**, 794-813. https://doi.org/10.1017/err.2025.8

[55] Alex, M. (2021) Quantum Technologies: A Review of the Patent Landscape. arXiv: 2102.04552.

[56] Le, T.D., Do, P.H., Dinh, T.D. and Pham, V.D. (2025) Are Enterprises Ready for Quantum-Safe Cybersecurity? arXiv:2509.01731.

[57] Ahmed, N., Zhang, L. and Gangopadhyay, A. (2025) A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries. 2025 *IEEE International Conference on Quantum Computing and Engineering* (*QCE*), Albuquerque, 30 August 2025-5 September 2025, 906-917. https://doi.org/10.1109/qce65121.2025.00102

[58] Mosca, M. and Piani, M. (2022) 2021 Quantum Threat Timeline Report. Global Risk

Institute.
https://info.quintessencelabs.com/hubfs/Quantum-Threat-Timeline-Report-2021-full-report-final%20(1).pdf

[59] Bernstein, D.J. (2025) Post-quantum Cryptography. In: Jajodia, S., Samarati, P. and Yung, M., Eds., *Encyclopedia of Cryptography, Security and Privacy*, Springer, 1846-1847. https://doi.org/10.1007/978-3-030-71522-9_386

[60] Campagna, M., Chen, L., Dagdelen, O., Ding, J., Fernick, J., Gisin, N. and Zhang, Z. (2015) Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. European Telecommunications Standards Institute, 1-64.

[61] Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T. and Smith-Tone, D. (2022) Status Report on the Third Round of the Nist Post-Quantum Cryptography Standardization Process.
https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

[62] Barker, E., Chen, L., Keller, S., Roginsky, A., Vassilev, A. and Davis, R. (2017) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (No. NIST Special Publication (SP) 800-56A Rev. 3 (Draft)). National Institute of Standards and Technology.
https://csrc.nist.gov/CSRC/media/Publications/sp/800-56a/rev-3/draft/documents/sp800-56ar3-draft.pdf