Review

Quantum Readiness: A Review on Dynamics in Academia and the Cybersecurity Sector

Volkan Erol *

Posted Date: 15 September 2025

doi: 10.20944/preprints202509.1146.v1

Keywords: Quantum Computing; Post-Quantum Cryptography; Cybersecurity; Quantum Readiness; Shor's Algorithm; NIST, Crypto-Agility; Quantum Threat

 doi:10.20944/preprints202509.1146.v1

Review

Quantum Readiness: A Review on Dynamics in Academia and the Cybersecurity Sector

Volkan Erol

Independent Researcher; volkan.erol@gmail.com

Abstract

The cybersecurity infrastructure of the digital age is facing an unprecedented threat with the rise of quantum computing. Current public-key cryptographic systems are at risk of being broken by quantum algorithms such as Shor's and Grover's. This threat has triggered a global effort, known as **quantum readiness**, which necessitates a proactive approach in both academia and the industry. This review article examines the fundamental dynamics of quantum readiness, academic research worldwide, and concrete applications in the cybersecurity sector. The article details the international competition led by the National Institute of Standards and Technology (NIST) to define post-quantum cryptography (PQC) standards. It also analyzes the national PQC strategies of the US, the EU, China, and other Western countries, the transition processes in critical sectors like finance and telecommunications, and key concepts like **crypto-agility**. This study reveals that the quantum threat is not merely a theoretical possibility but a strategic security issue, and that preparing for this threat is vital for a seamless digital security future.

Keywords: quantum computing; post-quantum cryptography; cybersecurity; quantum readiness; Shor's algorithm; NIST; crypto-agility; quantum threat

PACS: 03.67.Dd, 89.20.-f, 03.67.Lx

1. Introduction

The foundation of information security in the digital age relies on the power of cryptographic algorithms based on mathematically difficult problems. However, this foundation may soon be shaken. The rapid advancements in the field of quantum computing hold the potential to break even today's strongest encryption methods. The **quantum threat** is no longer a distant science fiction scenario but a concrete and imminent risk to national security, financial systems, and cyberspace security [1]. This risk emerges as quantum algorithms like **Shor's** and **Grover's** provide the computational power needed to break existing encryption standards. For example, Shor's algorithm can solve integer factorization and logarithm problems—the basis of today's most common public-key encryption systems, RSA and ECC (Elliptic Curve Cryptography)—at a speed far exceeding that of classical computers [2]. This situation endangers not only today's encrypted data but also data stored today to be decrypted later ("harvest now, decrypt later") when powerful quantum computers become available in the future [3].

This article explores the concept of **quantum readiness**, which means getting ready for this future challenge. This concept, addressing both the opportunities presented by quantum computing and the threats it poses to existing cybersecurity infrastructures, has become a broad area of discussion and work in both the academic world and the cybersecurity industry. Quantum readiness is not just about developing new algorithms; it also requires organizations to evaluate their current cryptographic systems, understand their risks, and define strategies for a seamless transition to post-quantum resistant (PQC) solutions [4].

The purpose of this review article is to comprehensively examine the dynamics of quantum readiness, related academic research, and concrete applications in the cybersecurity sector. The article

 doi:10.20944/preprints202509.1146.v1

will shed light on the theoretical foundations of the topic, global standardization efforts (especially those of **NIST**), and national strategies in different regions (including the **US, EU, China, Far East, and Australia**). It will also analyze the role of academia, industry solutions, and how organizations are preparing for this transition. This aims to provide readers with a holistic view of the challenges and opportunities that the quantum era will bring. This review seeks to fill significant gaps in the current literature, as most studies focus either on technical details or sectoral applications, while this article brings both dynamics together.

2. Theoretical Foundations: An Overview of Quantum Threats

Unlike bits (0 or 1) used by classical computers, quantum computing works with units called **qubits**. Qubits can represent multiple states simultaneously due to quantum mechanics principles like superposition and entanglement. This property provides immense parallel processing power for certain algorithms and can far surpass classical computers in solving the mathematical problems that form the basis of our cryptographic security [2]. This is precisely where the quantum threat arises.

Shor's algorithm poses the greatest threat to today's public-key cryptography systems. This algorithm can factor a large number into its prime factors at a speed that is virtually impossible for classical methods. Modern digital communication and secure commerce, which are the backbone of systems like **RSA** and **Elliptic Curve Cryptography (ECC)**, rely on the difficulty of this factorization problem [2]. Running Shor's algorithm on a sufficiently powerful quantum computer could break these encryption methods in seconds, leaving all digital signature and key exchange processes vulnerable. This creates a serious security gap in every area, from financial transactions to the protection of state secrets.

Another significant threat is **Grover's algorithm**. This algorithm can solve search problems quadratically faster than classical algorithms. Grover's algorithm presents a direct attack possibility on symmetric-key encryption systems (e.g., **AES**). The impact of this threat can be mitigated by doubling the key length of AES; for example, using AES-256 instead of AES-128 can increase resistance against a Grover attack. However, this is only a temporary solution and is not as comprehensive as the Shor threat to asymmetric encryption.

The risk posed by these algorithms enables a strategy known as **"harvest now, decrypt later"** [3]. Malicious actors collect today's encrypted data and wait for quantum computers to become available in the future. This poses a serious danger, especially for sensitive and persistent data like inter-state communications, long-term trade secrets, or personal health information. Therefore, quantum readiness is a strategic necessity aimed at both protecting existing infrastructures and building a secure cryptographic ecosystem for the future.

3. Post-Quantum Cryptography (PQC) Standardization Efforts and National Strategies

The most proactive response to the threat posed by quantum computers is the steps taken in the field of post-quantum cryptography (PQC). PQC aims to develop algorithms that can run efficiently on classical computers but cannot be broken by quantum algorithms like Shor's or Grover's. Standardization efforts in this field are of great importance globally, especially for protecting critical infrastructures and national security.

3.1. National Institute of Standards and Technology (NIST)

The **National Institute of Standards and Technology (NIST) PQC Competition** is at the center of these efforts. Launched in 2016 and conducted in several rounds, this competition has rigorously evaluated new algorithms proposed by cryptographers from all over the world in terms of security, performance, and ease of use [4]. This competition has allowed for the public testing and cryptanalysis of competing algorithms. Following the third round of the competition, NIST announced the four main algorithms that will become the first standards: **CRYSTALS-Kyber (ML-KEM)** for key exchange mechanisms and **CRYSTALS-Dilithium (ML-DSA)**, **Falcon**, and **SPHINCS+ (SLH-DSA)** [5]. These

 doi:10.20944/preprints202509.1146.v1

algorithms aim to resist quantum attacks by relying on different mathematical problems, such as lattice-based cryptography. NIST plans to officially publish these standards by 2024, and this process is expected to provide a roadmap for the global PQC transition. While these standards will be mandatory for US federal agencies, they are also expected to be widely adopted by the global industry.

3.2. European Union (EU) and Other Countries

The **European Union (EU)** has also adopted PQC as a strategic priority. The European Commission is allocating significant funds for quantum technologies and cryptographic research through programs like **Horizon Europe** and **EIC** [6]. The EU's **EuroQCI (European Quantum Communication Infrastructure)** initiative aims to build a quantum communication infrastructure across the continent and plans to use both Quantum Key Distribution (QKD) and PQC algorithms in this network. This multifaceted approach aims to accelerate the transition of PQC from theory to practice.

Other national strategies are also contributing to this global race. The **National Cyber Security Centre (NCSC)** in the **UK** has published detailed roadmaps for the PQC transition. The NCSC's guidance provides a concrete timeline, aiming for organizations to inventory their current cryptographic assets by 2028, prepare the most critical systems for transition by 2031, and complete a full PQC transition in all systems by 2035 [7,8].

The Communications Security Establishment (CSE) in **Canada** is also providing guidance for a transition aligned with NIST standards. Countries like **Japan** and **Australia** are also developing their own PQC strategies through national and international collaborations. For example, in Japan, institutions like the National Energy and Industrial Technology Development Organization (NEDO) are carrying out projects for the integration of PQC into the national supply chain [16].

Meanwhile, **China** is also making notable progress in the PQC field. China is moving towards creating its own national cryptographic standards independently of the US-led standards. The Chinese Academy of Sciences and related research institutes are working intensively on PQC algorithms and developing their own commercial cryptography standards (ICCS) [9,17]. This indicates that PQC has become part of technological competition and national security, and that multiple ecosystems could emerge on a global scale.

4. The Academic Research Ecosystem

The development and evaluation of post-quantum cryptography are fundamentally based on academic research. Many leading universities and research centers worldwide are working intensively on the mathematical foundations of PQC algorithms. For example, the theoretical security analysis and performance optimization of next-generation algorithms like lattice-based, code-based, and multivariate cryptography are the main agenda for researchers at these centers [2,10].

Institutions such as the **University of Waterloo (Canada)**, the **Massachusetts Institute of Technology (MIT - USA)**, and **KU Leuven (Belgium)** are taking on leading roles in quantum computing and cryptography. These universities are not only discovering new algorithms but also conducting critical studies to identify their potential vulnerabilities. This process is vital for standardization initiatives like the NIST PQC competition; because peer review and cryptanalysis in the academic world are the most important ways to prove an algorithm's reliability.

Beyond PQC algorithms, academic research also covers other quantum security technologies like **quantum random number generators (QRNG)** and **quantum key distribution (QKD)** [11]. QKD aims to provide secure key sharing using the laws of quantum mechanics, and countries like China have made significant progress in this area by testing this technology via satellites.

Finally, collaboration mechanisms between academia, industry, and government institutions are also an important part of this ecosystem. For example, many of the algorithms submitted to the NIST competition were developed through the joint efforts of academics and industrial cryptographers. This collaboration is crucial for translating theoretical knowledge into practical applications and creating a common front against the quantum threat. The dynamic role of academia will continue to shape the future of quantum readiness.

 doi:10.20944/preprints202509.1146.v1

5. Sectoral Implementation and Cybersecurity Dynamics

The materialization of the quantum threat has led to significant activity in the cybersecurity sector beyond theoretical research. Critical sectors, especially **finance, telecommunications, and defense**, are the ones taking the most urgent measures against this threat. These sectors are actively planning their PQC transition strategies due to their long-term data privacy requirements (the "harvest now, decrypt later" threat).

Cybersecurity product and service providers are developing new solutions for PQC compliance. Software and hardware that can replace existing encryption modules with PQC algorithms or offer multi-layered hybrid approaches are being launched [12]. These products include **quantum-safe VPNs**, **key management systems** that use PQC algorithms during data transfer, and **data protection solutions** that make critical data resilient to the post-quantum era.

One of the most important concepts in this transition process is **crypto-agility**. Crypto-agility refers to an organization's ability to quickly and seamlessly adapt its existing cryptographic infrastructure to new algorithms (like PQC). This requires a transition from old systems, where encryption algorithms are tightly embedded in the code, to modular architectures where algorithms can be easily swapped out. Crypto-agility is not only a mandatory part of the PQC transition but also provides flexibility against other cryptographic threats that may emerge in the future.

Major technology companies are leading the PQC transition. For example, Google has conducted PQC tests in its Chrome browser, and IBM has started offering PQC-enabled solutions in its cloud services [13]. Such pioneering steps serve as motivation for other players in the sector. However, this process presents a major challenge, especially for legacy systems. The hardware and software dependencies in old systems show that the PQC transition can be costly and complex. To overcome these challenges, close collaboration between industry leaders, academics, and governments is essential.

6. Future Predictions and Recommendations

While the future of quantum computing is uncertain, it is only a matter of time until quantum computers reach a level capable of breaking current encryption (often referred to as "Y2Q"). This requires organizations and countries to act proactively. In the future, with the widespread adoption of PQC, new challenges will also emerge. One of these is the burden on network performance due to the larger key and signature sizes of PQC algorithms. This may necessitate updates to telecommunication infrastructures and internet protocols.

To overcome these challenges and ensure quantum readiness, several steps can be recommended:

1. **Technology Assessment and Inventory Management**: Organizations should identify which of their data needs long-term protection and which systems most require a PQC transition [14]. This requires adopting a risk-based approach.
2. **Collaboration and Training**: The public and private sectors must maintain a continuous dialogue with academics. Training a workforce specialized in cryptography and quantum security is of critical importance.
3. **Hybrid Approaches**: Before a full PQC transition, hybrid solutions that use a combination of existing encryption algorithms and PQC algorithms can provide a gradual and secure transition [15].
4. **Updating Policies and Standards**: Governments and international organizations should accelerate the determination of PQC standards and create policies that encourage compliance.

This article emphasizes that quantum readiness is not just a technological transformation but also a strategic security matter. The future will be shaped by those who can manage the challenges and opportunities brought by the quantum era.

7. Conclusion

The rise of quantum computing presents both a transformative potential and an unprecedented threat to the world of cybersecurity. This review article has examined the concept of **quantum readiness**

 doi:10.20944/preprints202509.1146.v1

across a broad spectrum, from fundamental theoretical threats (Shor's and Grover's algorithms) to global standardization efforts and sectoral implementation dynamics. The findings show that the quantum era is not just a theoretical topic of discussion but a strategic issue that requires concrete, proactive, and coordinated action among states, academics, and industry leaders.

International collaborations, such as the NIST PQC competition, play a critical role in overcoming this global challenge. The different approaches to PQC in the US, EU, China, and other countries highlight the geopolitical importance of this topic. PQC algorithms, nourished by academia, are converging with industry solutions around concepts like **crypto-agility**. These dynamics not only create a defense mechanism against the quantum threat but also lay the groundwork for building secure digital infrastructures for the future.

The analysis presented in the article reveals that quantum readiness is a journey, and this journey must be supported by ongoing research, education, collaboration, and continuously updated policies. In particular, the "harvest now, decrypt later" threat is forcing organizations to take action today. In conclusion, quantum readiness is not just a technical necessity but a strategic vision that will shape the future of cybersecurity. This vision will secure our cryptographic infrastructures and enable a safe transition into the quantum era.

References

1. National Academies of Sciences, Engineering, and Medicine, *Quantum Computing and the Cybersecurity Threat* (The National Academies Press, 2019).
2. D. J. Bernstein and T. Lange, *Post-Quantum Cryptography*, 2nd ed. (Springer, 2017).
3. PwC, *Preparing for the Quantum Computing Era*, 2021, https://www.pwc.com/gx/en/issues/cybersecurity/preparing-for-the-quantum-computing-era.html.
4. National Institute of Standards and Technology (NIST), *Report on Post-Quantum Cryptography*, NISTIR 8105 (NIST, 2016).
5. National Institute of Standards and Technology (NIST), FIPS 203, FIPS 204, and FIPS 205: Three Post-Quantum Cryptography Standards Approved, 2024.
6. European Commission, The European Quantum Flagship, 2020, https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies.
7. National Cyber Security Centre (NCSC), *Guidance on migrating to Post-Quantum Cryptography* (NCSC, 2022).
8. National Cyber Security Centre (NCSC), Timelines for migration to post-quantum cryptography, 2025.
9. J. Zhao and Q. Guo, Chinese Journal of Cryptography **3**, 123 (2021).
10. M. Albrecht, S. Bai, L. Ducas, and et al., Cryptology ePrint Archive, Report 2016/483, 2016.
11. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
12. Microsoft, Quantum computing and cybersecurity, 2023, whitepaper, https://www.microsoft.com/en-us/research/whitepaper/quantum-computing-and-cybersecurity/.
13. IBM, IBM Quantum Safe, 2023, product documentation, https://www.ibm.com/quantum/quantum-safe-cryptography/.
14. J. Boogert and et al., *Preparing for the Quantum Transition: A Guide for Organizations* (Deloitte, 2022).
15. ETSI, *Quantum-Safe Cryptography: An ETSI White Paper* (ETSI, 2019).
16. The Quantum Insider, PQShield Participating in NEDO Program to Implement Post-Quantum Cryptography Across Japan, 2025.
17. Merics, China's long view on quantum tech has the US and EU playing catch-up, 2024, https://merics.org/en/commentary/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch.
18. E. M. Alagoz and S. K. Gunes, IEEE Access **11**, 100 (2023).
19. P. Schwabe and L. H. P. de Lacerda, in *NIST PQC Workshop* (2022).
20. M. K. K. S. M. K. P. R. P. D. S. J. C. R. S. V. D. S. S. A. G. S. G. P. D. A. H. R. J. D. S. S. A. A. S. C. S. A. A. C. S. V. K. T. A. T. B., J. Cybersecurity Privacy **3**, 89 (2023).