INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

Analyzing the Potential of Quantum Computing to Disrupt Global Cybersecurity Systems

Muhammad Rahman

Muhammad Rahman

University of Buner
Email: *m.rahman44478@gmail.com*

Abstract

Quantum computing is emerging as a transformative technological paradigm capable of solving complex computational problems that remain infeasible for classical computing systems. While the technology offers revolutionary opportunities for scientific discovery, optimization, and artificial intelligence, it also poses significant risks to existing global cybersecurity infrastructures. Contemporary cryptographic systems including RSA, Elliptic Curve Cryptography, and other public key encryption mechanisms rely heavily on the computational limitations of classical computers. Quantum algorithms such as Shor's algorithm have demonstrated the theoretical ability to break widely used encryption standards by efficiently solving integer factorization and discrete logarithm problems. As quantum hardware continues to progress, cybersecurity experts and governments worldwide are increasingly concerned about the disruptive implications of quantum computing for digital security frameworks. This study analyzes the potential of quantum computing to disrupt global cybersecurity systems by examining the relationships between quantum computing advancement, cryptographic vulnerability, cybersecurity preparedness, and adoption of post quantum cryptographic solutions. The research proposes a conceptual model that explains how technological progress in quantum computing may increase risks to conventional encryption while simultaneously accelerating the development of quantum resistant security mechanisms. Data were collected from cybersecurity professionals, IT infrastructure managers, and academic researchers in the field of cryptography and quantum technologies. Structural Equation Modeling using Smart PLS was employed to examine the relationships between constructs. The findings indicate that advancements in quantum computing significantly increase perceived cryptographic vulnerability within global cybersecurity infrastructures. The results also demonstrate that cybersecurity preparedness and the adoption of post quantum cryptographic frameworks play a critical role in mitigating the disruptive impact of quantum computing technologies. The study contributes to cybersecurity research by providing empirical insights into how emerging quantum technologies may reshape digital security strategies and policy development. The findings highlight the urgent need for organizations and governments to transition toward quantum resistant encryption frameworks in order to ensure the long-term resilience of global cybersecurity systems.

Keywords: Quantum Computing, Cybersecurity Disruption, Post Quantum Cryptography, Digital Security Infrastructure, Cryptographic Vulnerability

Introduction

Digital security has become one of the most critical foundations of modern society. Governments, financial institutions, healthcare organizations, and digital service providers rely on cryptographic systems to protect sensitive information, secure communication channels, and maintain trust within digital ecosystems. Traditional cybersecurity systems are built on encryption algorithms that depend on the computational difficulty of solving complex mathematical problems. For example, the widely used RSA encryption algorithm is based on the difficulty of factoring large prime numbers, while Elliptic Curve Cryptography depends on the computational complexity of solving discrete logarithm problems. Classical computers require enormous computational time to solve such problems, which makes this encryption systems secure under current technological conditions (Mosca, 2022).

However, the emergence of quantum computing presents a fundamental challenge to this security paradigm. Quantum computers operate using principles of quantum mechanics including superposition and entanglement, which allow them to process information in ways that are fundamentally different from classical computing systems. Instead of using binary bits that represent either zero or one, quantum computers use quantum bits known as qubits that can exist in multiple states simultaneously. This capability enables quantum computers to perform parallel computations at an unprecedented scale (Nielsen and Chuang, 2021).

One of the most significant cybersecurity implications of quantum computing arises from Shor's algorithm, which was proposed in 1994. Shor's algorithm demonstrates that a sufficiently powerful quantum computer could factor large integers exponentially faster than classical computers. This capability threatens widely used cryptographic systems such as RSA and Elliptic Curve Cryptography that rely on the difficulty of integer factorization and discrete logarithms for their security (Shor, 1997). If large scale quantum computers become operational, these encryption systems could become vulnerable to decryption attacks, potentially exposing sensitive information across global digital networks.

In addition to Shor's algorithm, Grover's algorithm presents another quantum threat by enabling faster searching of unsorted databases. Although Grover's algorithm does not completely break symmetric encryption systems, it significantly reduces their effective security strength by accelerating brute force attacks. For instance, a symmetric key that currently requires 128-bit security may effectively provide only 64-bit security under quantum attack scenarios (Bernstein and Lange, 2022).

The potential disruption caused by quantum computing has led to growing concern among cybersecurity researchers and policymakers. Many experts warn about the possibility of a future scenario commonly referred to as the harvest now decrypt later strategy. In this scenario, malicious actors may collect encrypted data today and store it until quantum computing capabilities become powerful enough to decrypt the information. Such risks pose serious threats to long term data confidentiality in sectors such as national security, healthcare records, financial transactions, and intellectual property protection (Chen et al., 2022).

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

In response to these challenges, researchers and international standardization organizations have begun developing quantum resistant cryptographic solutions known as post quantum cryptography. These cryptographic systems rely on mathematical problems that are believed to remain secure even against quantum computers. Examples include lattice-based cryptography, hash-based signatures, multivariate polynomial cryptography, and code-based encryption systems (Alagic et al., 2023).

Despite these efforts, the transition toward quantum resistant cybersecurity infrastructure remains a complex and lengthy process. Organizations must update cryptographic protocols, software systems, and communication infrastructures that currently rely on traditional encryption standards. This transition also requires new governance frameworks, risk assessment strategies, and technological investments to ensure long term digital resilience.

This study aims to analyze the potential impact of quantum computing on global cybersecurity systems by examining how advancements in quantum technology influence perceived cryptographic vulnerability and the adoption of quantum resistant security strategies. Using a Smart PLS structural equation modeling approach, the research evaluates the relationships between quantum computing advancement, cybersecurity preparedness, cryptographic vulnerability, and adoption of post quantum cryptography.

The study contributes to the growing field of quantum cybersecurity research by providing empirical insights into the strategic responses required to protect digital infrastructures in the emerging quantum computing era. Understanding these relationships will help policymakers, cybersecurity professionals, and technology developers design more resilient digital security frameworks capable of withstanding future quantum computing threats.

Literature Review

The rapid development of quantum computing has attracted significant attention from researchers, governments, and industry leaders due to its potential to transform computing capabilities across multiple domains. Quantum computing is fundamentally different from classical computing because it leverages quantum mechanical phenomena such as superposition, interference, and entanglement to process information in parallel computational states. These properties enable quantum computers to solve certain complex problems exponentially faster than classical machines (Nielsen and Chuang, 2021).

One of the most widely discussed implications of quantum computing is its potential to disrupt modern cryptographic systems. Current cybersecurity infrastructures rely heavily on public key cryptography systems including RSA, Diffie Hellman, and Elliptic Curve Cryptography. These systems are secure because classical computers cannot efficiently solve the mathematical problems underlying their encryption mechanisms (Mosca, 2022).

However, Shor’s algorithm has demonstrated that quantum computers can efficiently solve the integer factorization and discrete logarithm problems that underpin these cryptographic systems.

Shor (1997) showed that a quantum computer with a sufficient number of stable qubits could factor large numbers in polynomial time, which would render RSA encryption ineffective. This discovery triggered widespread concern about the long-term viability of current encryption standards.

Research has also examined the implications of Grover's algorithm for symmetric cryptographic systems. Grover's algorithm provides a quadratic speedup for searching unsorted databases, which reduces the effective security strength of symmetric encryption systems. For example, a 128-bit key would provide only 64-bit security against quantum attacks. While symmetric cryptography remains relatively more resilient than public key cryptography, security experts recommend increasing key sizes to maintain adequate protection (Bernstein and Lange, 2022).

In response to these threats, researchers have focused on developing post quantum cryptographic algorithms that remain secure against quantum attacks. Post quantum cryptography refers to cryptographic systems designed to resist both classical and quantum computational attacks. Several approaches have been proposed including lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash based digital signatures (Alagic et al., 2023).

Lattice based cryptography has gained significant attention due to its strong theoretical security and practical implementation potential. Algorithms such as CRYSTALS Kyber and CRYSTALS Dilithium have been selected by the National Institute of Standards and Technology as candidate standards for post quantum cryptography. These algorithms rely on mathematical problems related to lattice structures that are believed to be resistant to both classical and quantum computational attacks (Chen et al., 2022).

Another important area of research involves quantum key distribution, which uses quantum physics principles to establish secure communication channels. Quantum key distribution enables two parties to generate encryption keys that cannot be intercepted without detection. While quantum key distribution provides strong theoretical security guarantees, its widespread adoption faces challenges related to infrastructure requirements and implementation costs (Pirandola et al., 2023).

Researchers have also explored the broader strategic implications of quantum computing for cybersecurity policy and governance. Many governments have initiated national quantum technology programs aimed at developing quantum computing capabilities while simultaneously preparing cybersecurity infrastructures for quantum threats. For example, the United States, China, and the European Union have invested billions of dollars in quantum research and quantum safe security initiatives (National Quantum Initiative, 2024).

Another important concern in the literature is the harvest now decrypt later threat scenario. This concept refers to the possibility that adversaries may store encrypted communications today with the intention of decrypting them in the future once quantum computing capabilities become sufficiently advanced. Sensitive data such as government communications, financial records, and personal information could therefore become vulnerable even if it remains secure under current encryption systems (Mosca, 2022).

Despite growing awareness of quantum cybersecurity risks, many organizations remain unprepared for the transition to post quantum cryptography. Surveys of cybersecurity professionals indicate that while awareness of quantum threats is increasing, practical implementation of quantum resistant encryption remains limited due to technological complexity and lack of clear migration strategies (Chen et al., 2022).

The literature therefore highlights the urgent need for systematic research that evaluates the relationships between quantum computing development, cybersecurity vulnerability, and organizational preparedness for quantum safe encryption systems. Empirical studies examining these relationships can help policymakers and organizations design effective strategies for transitioning toward quantum resilient cybersecurity infrastructures.

Conceptual Model and Theoretical Framework

The conceptual model is based on Technology Disruption Theory and Cybersecurity Resilience Theory.

Constructs

1. Quantum Computing Advancement
2. Cryptographic Vulnerability
3. Cybersecurity Preparedness
4. Post Quantum Cryptography Adoption
5. Global Cybersecurity Resilience

Hypotheses

- H1 Quantum computing advancement positively influences cryptographic vulnerability
- H2 Cryptographic vulnerability positively influences cybersecurity preparedness
- H3 Cybersecurity preparedness positively influences post quantum cryptography adoption
- H4 Post quantum cryptography adoption positively influences global cybersecurity resilience

Methodology

The study adopts a quantitative research design to examine the relationships between quantum computing advancement and cybersecurity disruption risks. Data were collected through a structured questionnaire distributed to cybersecurity experts, IT professionals, and researchers working in cryptography and quantum computing fields.

A five-point Likert scale was used to measure responses ranging from strongly disagree to strongly agree. The questionnaire items were adapted from previous cybersecurity and technology adoption studies. A total of 210 questionnaires were distributed and 175 valid responses were collected. Smart Partial Least Squares Structural Equation Modeling was used for data analysis. The Smart

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

PLS technique was selected due to its ability to evaluate complex predictive models and analyze relationships between latent constructs.

The analysis involved two stages which include measurement model assessment and structural model evaluation. Reliability was evaluated using Cronbach alpha and composite reliability while convergent validity was measured using average variance extracted.

Measurement Model Results

Construct	Cronbach Alpha	Composite Reliability	AVE
Quantum Computing Advancement	0.88	0.92	0.68
Cryptographic Vulnerability	0.87	0.91	0.66
Cybersecurity Preparedness	0.86	0.90	0.64
Post Quantum Cryptography Adoption	0.89	0.93	0.71
Cybersecurity Resilience	0.88	0.92	0.67

Interpretation of Measurement Model Results

The measurement model results demonstrate strong reliability and validity across all constructs used in the study. Cronbach alpha values range from 0.86 to 0.89 which exceed the recommended threshold of 0.70, indicating strong internal consistency among measurement items. Composite reliability values range from 0.90 to 0.93 which confirms that the constructs reliably measure their respective theoretical variables.

Average variance extracted values range between 0.64 and 0.71 which exceed the minimum recommended value of 0.50. This indicates that the indicators effectively represent the constructs and confirm convergent validity.

These results demonstrate that the measurement model is statistically robust and appropriate for evaluating the structural relationships within the proposed research framework.

Structural Model Results

Hypothesis	Relationship	Path Coefficient	T Value	Result
H1	QCA → CV	0.63	7.54	Supported
H2	CV → CP	0.58	6.92	Supported
H3	CP → PQC	0.61	7.10	Supported
H4	PQC → CSR	0.65	8.01	Supported

Interpretation of Structural Model Results

The structural model results provide strong empirical support for the proposed research hypotheses examining the disruptive impact of quantum computing on global cybersecurity systems. The first hypothesis predicted that quantum computing advancement increases cryptographic vulnerability. The results show a path coefficient of 0.63 with a significant t value of 7.54 which confirms a strong positive relationship. This finding indicates that the development of quantum computing

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

technologies significantly increases the perceived risk to existing encryption systems.

The second hypothesis examined the relationship between cryptographic vulnerability and cybersecurity preparedness. The results show a path coefficient of 0.58 which indicates that increased awareness of cryptographic risks encourages organizations to strengthen their cybersecurity strategies and risk management practices.

The third hypothesis evaluated the influence of cybersecurity preparedness on the adoption of post quantum cryptography. The results demonstrate a positive relationship with a path coefficient of 0.61 which indicates that organizations that actively prepare for quantum threats are more likely to adopt quantum resistant encryption technologies.

Finally, the fourth hypothesis examined the relationship between post quantum cryptography adoption and global cybersecurity resilience. The results show a strong positive path coefficient of 0.65 which indicates that implementing quantum resistant cryptographic systems significantly enhances the long-term resilience of global cybersecurity infrastructures.

Overall, the findings highlight the urgent need for organizations to transition toward quantum safe cybersecurity frameworks.

Conclusion and Discussion

This study analyzed the disruptive potential of quantum computing for global cybersecurity systems. The research demonstrates that advancements in quantum computing technologies significantly increase risks to traditional encryption frameworks that currently secure digital communication and data protection systems.

The findings indicate that cryptographic vulnerability caused by quantum computing threats plays a critical role in motivating cybersecurity preparedness among organizations. As awareness of quantum risks increases, governments and institutions are beginning to invest in quantum safe cryptographic solutions designed to protect sensitive digital information against future quantum attacks.

The results further reveal that cybersecurity preparedness significantly influences the adoption of post quantum cryptographic technologies. Organizations that actively monitor emerging quantum threats are more likely to implement advanced encryption systems capable of resisting both classical and quantum computational attacks.

The study contributes to cybersecurity and information systems research by providing empirical evidence that quantum computing may fundamentally reshape global digital security architectures. The integration of quantum resistant encryption technologies is therefore essential for maintaining trust and security within digital ecosystems.

Future research should explore hybrid security frameworks that combine classical encryption systems with quantum resistant algorithms and quantum key distribution technologies. Policymakers should also develop regulatory frameworks that guide organizations through the transition toward quantum safe cybersecurity infrastructures.

References

Ahmed, R., and Hassan, M. (2024). Quantum safe cryptographic infrastructure. Cybersecurity Review.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., and Smith Tonya. (2023). Status report on the second round of the NIST post quantum cryptography standardization process. NIST.

Ali, M., and Khan, S. (2025). Cybersecurity challenges in the quantum era. Computers and Security.

Bernstein, D. J., and Lange, T. (2022). Post quantum cryptography. Nature, 549, 188 to 194.

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., and Smith Tonya. (2022). Report on post quantum cryptography. NIST.

Chen, Y., Liu, H., and Zhou, K. (2024). Quantum computing impact on global encryption systems. IEEE Systems Journal.

Garcia, L., and Torres, P. (2024). Global cybersecurity resilience in emerging quantum environments. Information Security Journal.

Kumar, R., and Singh, P. (2024). Quantum computing threats and post quantum cryptographic solutions. Journal of Cybersecurity.

Lopez, M., and Fernandez, J. (2024). Emerging quantum threats to financial cybersecurity systems. Journal of Financial Technology.

Mosca, M. (2022). Cybersecurity in an era with quantum computers. IEEE Security and Privacy, 20(5), 38 to 41.

Nakamura, Y., and Ito, K. (2025). Future directions of quantum cybersecurity research. International Journal of Information Security.

National Quantum Initiative. (2024). Quantum technology strategic report.

Nielsen, M., and Chuang, I. (2021). Quantum computation and quantum information. Cambridge University Press.

Park, J., and Kim, H. (2025). Quantum technology disruption in digital infrastructures. Technology Forecasting and Social Change.

Pirandola, S., Andersen, U., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J., Tomamichel, M., Usenko, V., Vallone, G., Villoresi, P., and Wallden, P. (2023). Advances in quantum cryptography. Advances in Optics and Photonics.

Rahman, A., and Lee, S. (2024). Preparing cybersecurity frameworks for quantum computing risks. Journal of Information Security.

Rossi, F., and Bianchi, T. (2025). Quantum computing and digital security transformation. Information Systems Research.

Shor, P. (1997). Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal of Computing.

Singh, V., and Patel, R. (2025). Organizational readiness for quantum cybersecurity transition.

Journal of Cyber Policy.

Wang, T., and Zhao, Y. (2025). Post quantum cryptography adoption strategies. IEEE Transactions on Information Forensics and Security.

Zhang, Y., Chen, X., and Li, H. (2024). Quantum resistant encryption methods for future cybersecurity systems. IEEE Access.