INTERNATIONAL JOURNAL OF NETWORKS AND SECURITY
(ISSN: 2693-3608)
VOL.06 ISSUE02 (2026)

Research Article

Post-Quantum Cryptography for Critical Infrastructure: A National Security Framework for Secure Digital Transformation

Dr. Nguyen Minh Khoa [1]

[1]Department of National Security Studies, Vietnam Institute for Strategic Security Research, Hanoi, Vietnam

Received: 12 May 2026
Revised: 2 June 2026
Accepted: 20 July 2026
Published: 28 August 2026
Doi:10.55640/ijns-06-02-02
Page No: 14-21

Abstract

The emergence of cryptographically relevant quantum computing presents a strategic challenge to critical infrastructure because conventional public-key cryptographic mechanisms may become vulnerable to sufficiently capable quantum computers. This paper develops a national security framework for post-quantum cryptography (PQC) adoption across critical infrastructure, emphasizing policy coordination, cryptographic migration, risk prioritization, governance, and long-term digital resilience. The study adopts a conceptual research-and-review methodology based strictly on the references supplied by the author, with particular emphasis on the provided work addressing quantum-resistant cryptography and national security. Because most of the supplied empirical references concern intrauterine-device knowledge, attitudes, counseling, and healthcare behavior rather than cybersecurity or cryptography, their direct applicability to PQC is limited. This evidence mismatch itself constitutes an important methodological limitation and demonstrates the necessity of domain-specific evidence when developing national cybersecurity frameworks. The proposed framework therefore positions PQC migration as a socio-technical national security program rather than a simple algorithm replacement exercise. It integrates asset classification, cryptographic inventory, quantum-risk assessment, algorithm selection, hybrid deployment, governance, workforce preparation, supply-chain coordination, and continuous assurance. The analysis suggests that successful PQC transformation requires early migration planning, centralized policy direction, interoperability testing, lifecycle management, and protection of long-lived sensitive information. The paper contributes a structured conceptual roadmap for governments and critical-infrastructure operators seeking to reduce quantum-related systemic risk while maintaining operational continuity during cryptographic transition.

Keywords: Post-Quantum Cryptography, Critical Infrastructure, National Security, Quantum Computing, Cybersecurity, Cryptographic Migration, Digital Transformation, Risk Management, Cyber Resilience.

INTRODUCTION

Critical infrastructure increasingly depends on interconnected digital systems for energy distribution, telecommunications, transportation, healthcare, finance, water management, public administration, and industrial operations. These systems rely on cryptography to provide confidentiality, authentication, integrity, identity assurance, secure communications, and trusted transactions. Consequently, a fundamental change in the security assumptions underlying public-key cryptography can become a national security concern rather than merely a technical information-security problem.

Post-quantum cryptography addresses this challenge by developing cryptographic

mechanisms intended to remain secure against adversaries possessing quantum computing capabilities. The strategic issue is not limited to the hypothetical future availability of powerful quantum computers. Sensitive information can have a long operational lifetime, meaning information intercepted today may remain valuable when stronger computational capabilities become available. Similarly, critical infrastructure frequently contains legacy systems that cannot be rapidly replaced because of safety requirements, certification constraints, procurement cycles, or operational dependencies.

Ahmed (2024) frames quantum-resistant cryptography as a national-security and policy implementation problem rather than exclusively as an algorithmic research problem. This perspective is particularly important for critical infrastructure, where technological change must coexist with continuity, regulatory compliance, economic constraints, and institutional accountability. A national PQC strategy must therefore address not only which cryptographic algorithms should be adopted, but also where they should be deployed, when migration should occur, who should be responsible, and how security can be maintained throughout the transition.

The objective of this paper is to develop a conceptual national-security framework for PQC-enabled digital transformation of critical infrastructure. The framework focuses on five central questions: how quantum risk should be identified, how cryptographic dependencies should be inventoried, how migration should be prioritized, how hybrid security architectures can reduce transition risk, and how national governance can coordinate public and private infrastructure operators.

The significance of the research lies in treating cryptographic modernization as infrastructure resilience. Rather than waiting for quantum computing capabilities to mature, organizations can establish inventories, governance mechanisms, procurement requirements, testing programs, and migration priorities in advance. However, the evidence base supplied for this review contains a substantial domain mismatch. Most of the provided studies address reproductive-health knowledge, attitudes, counseling, and contraceptive adoption rather than cryptography or cybersecurity. Accordingly, these references cannot substantively validate technical PQC claims. The paper explicitly recognizes this limitation rather than attributing cybersecurity findings to unrelated healthcare studies.

LITERATURE REVIEW

The supplied literature presents two substantially different bodies of material. The first and directly relevant body consists of the provided work by Ahmed (2024), which explicitly concerns quantum-resistant cryptography, national security, policy, and implementation. This reference provides the conceptual foundation for positioning PQC as a strategic policy and implementation issue. Its relevance supports an approach in which cryptographic modernization is integrated into national security planning rather than treated as an isolated information-technology upgrade (Ahmed, 2024).

The remaining supplied studies predominantly concern healthcare and reproductive-health behavior. For example, Venturin et al. (2024), Okud et al. (2023), Pratiwi (2024), Wulandari and Nimah (2024), Purwati et al. (2024), and Kurniawati et al. (2024) examine knowledge, attitudes, perceptions, or experiences associated with healthcare and contraceptive decisions. Stone et al. (2021), Tounkara et al. (2022), Mvandal et al. (2020), and Zulfitriani et al. (2021) similarly investigate healthcare-provider behavior, counseling, knowledge, and adoption factors. Other supplied references address related healthcare contexts, including Ardanti and Dewi (2023), Azizah et al. (2023), Gustika et al. (2024), Arjuna and Santoso (2023), Via and Cusmarih (2024), and Kerja et al. (2023).

From a methodological perspective, these studies cannot be used as empirical evidence for quantum-resistant algorithms, cryptographic security, critical-infrastructure architectures, or national cybersecurity policy. Their inclusion nevertheless reveals an important research-design issue: a rigorous literature review requires alignment between the research question and the evidence base. Transferring conclusions from healthcare behavioral studies to cryptographic engineering would produce unsupported claims.

The principal literature gap is therefore clear. The supplied reference set provides insufficient domain-specific empirical evidence concerning PQC implementation in critical infrastructure. There is a need for studies examining cryptographic inventories, migration costs, algorithm interoperability, hybrid cryptographic architectures, legacy-system constraints, procurement policies, quantum-risk models, and national governance mechanisms. Ahmed (2024) supplies a policy-oriented starting point, but a comprehensive implementation framework requires additional technical and empirical research.

The theoretical positioning adopted in this paper consequently treats PQC migration as a socio-technical transformation. Cryptographic security depends on algorithms, protocols, hardware, software, identities, certificates, vendors, operational processes, governance, and human expertise. A national framework must integrate these dimensions rather than assuming that replacing one cryptographic algorithm automatically establishes quantum resilience.

METHODOLOGY

3.1 Research Design

This study uses a conceptual research-and-review methodology. The approach synthesizes the directly relevant supplied literature and develops a framework for national PQC implementation. The methodology does not claim experimental validation, benchmarking, or field testing. Instead, it constructs an analytically grounded model linking quantum risk, infrastructure dependency, migration governance, and operational resilience.

The methodological foundation follows the policy-oriented perspective that quantum-resistant cryptography should be addressed through coordinated national implementation rather than isolated technical adoption (Ahmed, 2024). Because the majority of supplied references are outside the cybersecurity domain, they are treated as evidence of the limitations of the available reference corpus rather than as technical support for PQC claims.

3.2 National Critical-Infrastructure Cryptographic Inventory

The first framework component is a national cryptographic inventory. Government agencies and critical-infrastructure operators should identify where public-key cryptography is used across applications, networks, devices, certificates, authentication systems, secure communications, software libraries, cloud services, operational-technology environments, and third-party platforms.

The inventory should record the cryptographic mechanism, implementation location, data sensitivity, system owner, vendor dependency, certificate lifecycle, replacement difficulty, and expected system lifetime. Such an inventory provides the foundation for migration prioritization. Without it, organizations cannot determine which systems are most exposed or which dependencies could prevent timely migration.

3.3 Quantum-Risk Prioritization

Not every cryptographic asset requires identical migration urgency. A national framework should therefore evaluate risk through multiple dimensions: sensitivity of protected information, expected information lifetime, infrastructure criticality, cryptographic exposure, replacement complexity, and dependency on external vendors.

A useful conceptual model is:

Quantum Migration Priority = Criticality × Data Lifetime × Cryptographic Exposure × Migration Complexity

This model is not intended as a universal mathematical risk standard but as a decision-support mechanism. A system protecting highly sensitive national information for several decades would receive a higher migration priority than a low-impact application containing short-lived information.

3.4 Hybrid Cryptographic Transition

Immediate replacement of every conventional cryptographic mechanism may create operational risks. A more practical transition strategy can employ hybrid mechanisms in which classical and post-quantum approaches operate together during a migration period. Such an architecture can provide resilience against uncertainty surrounding implementation maturity while organizations validate interoperability and performance.

Hybrid deployment should be accompanied by rigorous testing because combining mechanisms can increase protocol complexity. Critical infrastructure requires particular caution because authentication or key-establishment failures can interrupt essential services. The migration objective should therefore be cryptographic resilience without compromising availability.

3.5 Governance and Institutional Coordination

A national PQC program requires centralized policy direction combined with decentralized implementation. A national authority can establish minimum requirements, transition deadlines, procurement standards, reporting requirements, assurance mechanisms, and risk classifications, while individual infrastructure operators maintain responsibility for system-specific migration.

This governance structure addresses a fundamental coordination problem. A telecommunications operator, financial institution, electricity provider, and government agency may use different vendors and technologies while depending on interconnected identity and communication systems. Fragmented migration can therefore create systemic vulnerabilities.

Ahmed (2024) emphasizes the policy dimension of quantum-resistant cryptography, supporting the proposition that national-level coordination should accompany technical modernization.

3.6 Supply-Chain and Procurement Integration

PQC migration should become part of procurement and vendor-management processes. New infrastructure contracts should require cryptographic agility, documented cryptographic dependencies, upgrade mechanisms, and support for approved quantum-resistant approaches.

Cryptographic agility is particularly significant because security standards and implementation practices can evolve. Systems designed around rigid cryptographic assumptions may require expensive replacement when algorithms or protocols change.

By contrast, systems capable of replacing cryptographic components through controlled software or hardware updates can reduce future migration costs.

3.7 Workforce and Operational Readiness

Technical migration also requires trained personnel. Security architects, software engineers, system administrators, procurement officers, auditors, and policy officials need sufficient understanding of PQC risks and migration procedures. A shortage of expertise can transform a theoretically secure algorithm into an insecure operational implementation.

Training should therefore cover cryptographic inventory, certificate management, secure implementation, protocol configuration, vulnerability assessment, incident response, and lifecycle management. National programs should also establish testing environments in which organizations can experiment with PQC migration without disrupting production infrastructure.

3.8 Continuous Assurance

PQC migration should be treated as a lifecycle rather than a one-time project. Continuous monitoring should evaluate algorithm status, implementation vulnerabilities, vendor support, system dependencies, performance, certificate lifetimes, and emerging quantum-risk assessments.

This lifecycle model reflects the broader policy orientation of quantum-resistant security: national resilience depends on sustained implementation capacity rather than simply announcing an algorithm-selection policy (Ahmed, 2024).

RESULTS

The conceptual analysis produces five principal findings.

First, PQC migration is fundamentally a governance problem as well as a cryptographic problem. Algorithms alone cannot provide national resilience when legacy systems, procurement structures, vendors, operational technology, and institutional responsibilities remain uncoordinated.

Second, cryptographic inventory is the critical first operational capability. Organizations cannot prioritize quantum migration without knowing where vulnerable cryptographic mechanisms exist. Consequently, national programs should establish standardized inventory requirements before imposing universal replacement deadlines.

Third, critical infrastructure requires risk-based sequencing rather than uniform migration. Systems protecting long-lived sensitive information and essential national functions should receive earlier attention. Less critical systems can migrate according to longer transition schedules. This reduces the probability that rushed migration introduces availability or interoperability failures.

Fourth, cryptographic agility is a strategic resilience capability. Systems designed to accommodate controlled cryptographic replacement can respond more effectively to changes in algorithms, standards, vulnerabilities, and technological conditions. This reduces dependence on repeated large-scale infrastructure replacement.

Fifth, the available literature reveals a major evidence gap. The supplied healthcare-oriented studies cannot substantiate claims about PQC engineering or cybersecurity. Their subject matter includes knowledge, attitudes, counseling, healthcare-provider practices, and contraceptive adoption rather than quantum-resistant cryptography.

Therefore, the proposed framework should be considered conceptual and policy-oriented rather than empirically validated.

The strongest directly relevant evidence supplied is Ahmed (2024), which supports framing quantum-resistant cryptography within national-security policy and implementation planning. The results consequently indicate that future research must supplement policy analysis with technical benchmarking, infrastructure case studies, migration-cost analysis, and empirical evaluations.

DISCUSSION

The findings suggest that the central strategic mistake in PQC planning would be to define migration simply as an algorithm-substitution exercise. Critical infrastructure is characterized by long system lifecycles, complex dependencies, heterogeneous technologies, and stringent availability requirements. A technically secure algorithm can still generate operational risk if implemented without appropriate testing, certificate management, interoperability validation, or fallback procedures.

The proposed framework therefore extends the policy perspective of Ahmed (2024) by organizing migration into a sequence of inventory, risk prioritization, architecture, governance, implementation, and assurance. This approach recognizes that national security depends on the reliability of the entire cryptographic ecosystem rather than the security properties of an individual primitive.

A major trade-off concerns migration speed. Rapid migration can reduce exposure to future quantum threats, but rushed implementation may introduce configuration errors, interoperability problems, performance degradation, or unexpected dependencies. Slow migration allows organizations to test and mature their implementations but increases exposure to the risk that sensitive information remains protected by vulnerable mechanisms for too long. A risk-based strategy provides a means of balancing these competing objectives.

Another trade-off concerns centralized versus decentralized governance. Strong central standards can improve consistency and accountability, but excessively rigid requirements may be difficult to apply across heterogeneous sectors. Conversely, complete organizational autonomy can produce inconsistent security levels and create weak links across interconnected infrastructure. A layered governance model is therefore preferable: national authorities define minimum requirements and assurance expectations, while infrastructure operators determine technically appropriate implementation pathways.

The literature mismatch also has important implications. Although the supplied healthcare studies may demonstrate how knowledge, attitudes, counseling, and institutional practices influence adoption in their respective domains, they cannot legitimately be interpreted as evidence for cryptographic migration behavior. For example, findings concerning contraceptive knowledge or healthcare-provider attitudes should not be transformed into claims about cybersecurity awareness. Doing so would undermine the validity of the literature review. Their presence in the supplied corpus instead demonstrates why domain alignment is essential for publication-quality research.

The proposed framework also has limitations. It has not been tested against a real national infrastructure environment, and the risk equation is conceptual rather than empirically calibrated. No quantitative migration-cost dataset was provided, and the supplied references do not provide technical benchmarks for PQC algorithms, hardware acceleration, latency, bandwidth consumption, or implementation vulnerabilities.

Consequently, the framework should be viewed as a strategic architecture requiring subsequent empirical validation.

Nevertheless, the framework has practical value because it establishes a structured decision process. Governments can use it to identify critical cryptographic dependencies, prioritize high-consequence systems, incorporate PQC requirements into procurement, develop workforce capabilities, and establish continuous assurance. This transforms quantum preparedness from a future-oriented concern into a present-day digital-resilience program.

CONCLUSION

Post-quantum cryptography should be approached as a national critical-infrastructure transformation rather than a narrow cryptographic upgrade. The transition requires visibility into existing cryptographic dependencies, systematic risk prioritization, cryptographic agility, hybrid migration strategies, coordinated governance, procurement reform, workforce development, and continuous assurance.

The principal research contribution is the integration of cryptographic migration with national-security governance and infrastructure resilience. The analysis also identifies an important evidence limitation: most references supplied for this paper concern reproductive-health research and are not directly relevant to PQC. Therefore, the framework cannot be presented as empirically validated by those studies. Future research should incorporate domain-specific technical literature, real-world infrastructure case studies, quantitative migration-cost models, algorithm-performance evaluations, and empirical assessments of organizational readiness.

Ultimately, quantum preparedness is most effective when treated as a continuous capability. Organizations that establish cryptographic visibility, agility, governance, and migration processes before quantum threats become operationally decisive will be better positioned to preserve confidentiality, authentication, integrity, and national infrastructure resilience during the transition to a post-quantum security environment (Ahmed, 2024).

REFERENCES

1. Adger, AB Venturin et al., “Open-Access Women's Experiences with the Post-Placental Intrauterine Device: A Qualitative Study,” Brazilian Journal of Gynecology and Obstetrics, pp. 1-9, 2024.

2. Amira Okud et al., “Knowledge, Attitudes, and Practice About Emergency Contraception Among Saudi Women of Childbearing Age of Eastern Region in Saudi Arabia,” Cureus, vol. 15, no. 11, pp. 1-14, 2023.

3. Asti Inka Pratiwi, “Overview of Knowledge of Women of Fertile Age About Iud Contraception in Grand Vienna Housing Complex, Kenali Asam Village, Kota Baru District,” Midwifery Health Journal, vol. 9, no. 1, pp. 137-140, 2024.

4. Fetty Chandra Wulandari, and Kenly Zubdatan Nimah, Overview of Knowledge of Women of Fertilizing Age (Wus) About Pregnancy Over the Age of 35 Years In Baledono Village Krajan Purworejo District Purworejo District,” Journal of Health Communication, vol. 15, no. 1, pp. 9-15, 2024.

5. Lilis Purwati, Wijayanti, and Tresia Umarianti “Relationship Between Education Level And Perception Of Choosing Intra Uterine Device (Iud) Contraception In Iud Kb Acceptors At Karangpandan Community Health Center,” Al-Insyirah Midwifery: Journal of Midwifery Sciences, vol. 13, no. 2, pp. 105-110, 2024.

6. Lise Kurniawati, Rindu, and Ageng septa Rini, “Relationship between Knowledge, Attitude and Perception of Husbands with the Use of IUD Contraceptives in the Haurwangi Health Center Work Area, Cianjur Regency in

2023," Innovative: Journal of Social Science Research, vol. 4, no. 2, pp. 7706-7719, 2024.

7. Lucy Stone et al., "Assessing Knowledge, Attitudes, and Practice of Health Providers towards the Provision of Postpartum Intrauterine Devices in Nepal: A Two-Year Follow-Up," Reproductive Health, vol. 18, pp. 1-11, 2021.

8. Maria Wemrell, and Lena Gunnarsson, "Attitudes Toward the Copper IUD in Sweden: A Survey Study," Frontiers in Global Women's Health, vol. 3, pp. 1-15, 2022.

9. Mariama S. Tounkara et al., "A Mixed-Methods Study of Factors Influencing Postpartum Intrauterine Device Uptake After Family Planning Counseling among Women in Kigali, Rwanda," PLoS One, vol. 17, no. 11, pp. 1-15, 2022.

10. Nambalirwa Teddy et al., "IUD Contraceptive Use Among Women of Reproductive Age: Experiences, Motivators and barriers in a General Hospital, Uganda," Makerere University, pp. 1-12, 2020.

11. Ni Komang Junia Ardanti, and Ni Luh Made Asri Dewi, "Description of the Level of Knowledge of Couples of Fertilizing Age Concerning the Use of Iud Contraception Devices," Community of Publishing in Nursing, pp. 490-495, 2023.

12. Nur Azizah, Elvi Murniasih, and Mira Agusthia, "Factors Related to the Incidence of Hyperemesis Gravidarum in Pregnant Women at Tanjungpinang City Hospital," Jurnal Inovasi KesehatanAdaptif, vol. 5, no. 4, pp. 71-85, 2023.

13. S. Gustika, D. C. Yun, and Dan A. W. Nainggolan "Factors that Influence the Low Interest of Women of Childbearing Age in Choosing an IUD Contraceptive Device in Uring Village, Pegasing District, Southeast Aceh Regency, 2022," STIKes Ibnu Sina Ajibarang, vol. 2, no. 4, 2024.

14. Samson Peter Mvandal, Joseph Nhandi, and Godfrey Lupoly, "Knowledge and Attitude concerning use of Intrauterine Contraceptive Device among Women attending Family Planning at Makambako RCH in Njombe-Tanzania," Preprints, pp. 1-9, 2020.

15. Tony Arjuna, and Nindita Kumalawati Santoso, "Level of Knowledge of Women of Childbearing Age About IUD Contraceptive Devices at BPRB Bina Sehat Kasihan Bantu," Indonesian Journal of Nursing and Midwifery, vol. 1, no. 1, pp. 1–5, 2023.

16. Vika Chita Via, and Cusmarih Cusmarih, "The Relationship Between the Role of Health Workers, Knowledge and Husband's Support on the Selection of IUD KB Acceptors at the Keagungan Village Health Center in 2023," Formil Journal (Scientific Forum) of Respati Public Health, vol. 9, no. 1, pp. 76-86, 2024.

17. W. Kerja, P. M. B. Dewi, dan S. Keb, "The Effect of IUD Birth Control Counseling Using Sheet Media to Become a Postpartum Birth Control Birth Control Acceptor," hal, pp. 8–14, 2023.

18. Zulfitriani Zulfitriani et al., "Counseling to Increase Knowledge of Women of Childbearing Age (WUS) about IUD Contraceptives," Community Empowerment, vol. 6, no. 3, pp. 374-379, 2021.

19. Ahmed, F. (2024). Quantum-resistant cryptography for national security: A policy and implementation roadmap. Int J Multidisciplinary on Science and Management, 1(4), 54-65.

20. Ramamurthy, K. (2023). AI-Driven Test Automation Frameworks for the Modern Software Quality Engineering. International Journal of Emerging Trends in Computer Science and Information Technology, 4(4), 257-269.

21. Philip, P. G. (2024). Artificial Intelligence-Driven Project Risk Prediction Models: Enhancing Decision-Making Accuracy in Large-Scale Infrastructure Projects. American Journal of Technology, 3(1), 52–69. https://doi.org/10.58425/ajt.v3i1.571.