

# Quantum-Resistant Cryptography in Critical Infrastructure: A Strategic Framework for Transition Readiness in National Defense

TIM ABDIUKOV

*NTS Netzwerk Telekom Service AG, Australia.*

*Abstract: The repercussions of a crack in classical cryptographic systems, presented alongside the quantum computer, are immense, as they compromise the national infrastructure and communications essential to national security. As the quantum function is developed, encryption systems, such as RSA and ECC, that are still in use will become obsolete because they will be vulnerable to quantum methods, e.g., Shor's. This paper examines the transition to quantum-resistant cryptography (QRC) in national defense systems and the implications of such a move. It identifies a model-based integration as the risk assessment, policies, and technological adaptation, as well as the phased migration strategies, become integrated systematically within the critical infrastructure sectors. Following recent developments in the area of post-quantum cryptography (PQC), the framework focuses on aspects such as pre-intentional planning, compatibility with current frameworks, and consideration of emerging global standards, including those from NIST. Another issue identified in the paper as a major implementation challenge is the limitation of resources, technological inertia, and coordination across agencies. Conclusively, this paper emphasizes the necessity of initiating a quantum-safe migration of cryptography to ensure resilience, continuity of business, and continued delivery of national security in the current period of quantum breakthroughs.*

*Index Terms: Quantum-resistant cryptography, post-quantum cryptography, critical infrastructure, national defense, cryptographic transition*

## I. INTRODUCTION

### 1.1 Background on Quantum Computing and Its Implications for Classical Cryptography

Quantum computing represents a revolutionary shift in computational capacity, enabling the resolution of issues that were previously deemed intractable using traditional computing systems. In addition to offering revolutionary opportunities in fields such as pharmaceuticals and materials science, this presents a significant challenge to existing cryptographic systems. Traditional schemes of public-key cryptography, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), are based on the complexity of solving specific mathematical functions, particularly the factorization of an integer and the discrete logarithm. Such problems can be efficiently solved (when these systems are in use) with quantum algorithms such as Shor, and these systems will then be rendered obsolete when cryptanalytically relevant quantum computers (CRQCs) are available (Bishwas & Sen, 2024). Bishwas and Sen stress that the mathematical foundation of modern cryptography is irreconcilably incompatible with the quantum capabilities of computation and suggest making immediate plans in the industry to transition to a future cryptography.

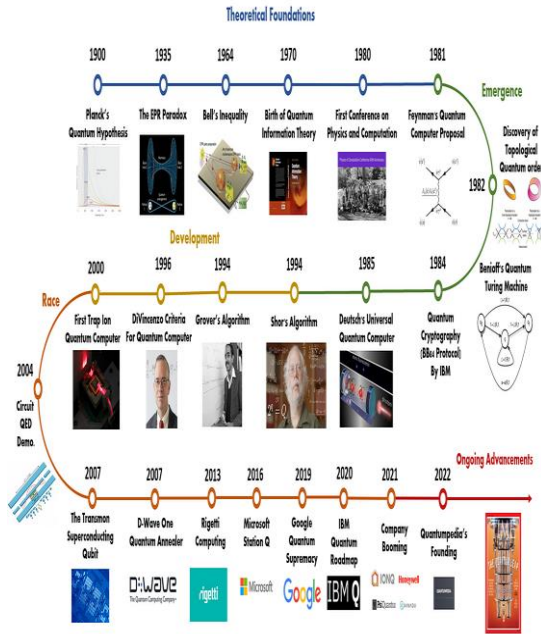


Figure 1: A Brief History of Quantum Computing

### 1.2 Importance of Cryptographic Security in National Defense and Critical Infrastructure

The underpinning of the confidentiality, the integrity, and the authenticity of information in terms of national defense systems and critical infrastructure relies on cryptography. The energy, telecommunications, and transportation industries are increasingly being digitalized and networked, making them highly reliant on secure communications and resilient cyber infrastructure. Asimiyu (2024) highlights the lack of resilience of national defense architecture against quantum threats and warns that the failure of a single cryptography level would be a catastrophic event, leading to the downfall of an entire network of interconnected systems. Cryptographic protection is crucial for the security of command-and-control structures, satellite systems, and intelligence exchange systems, which are highly critical to national sovereignty and operational preparedness.

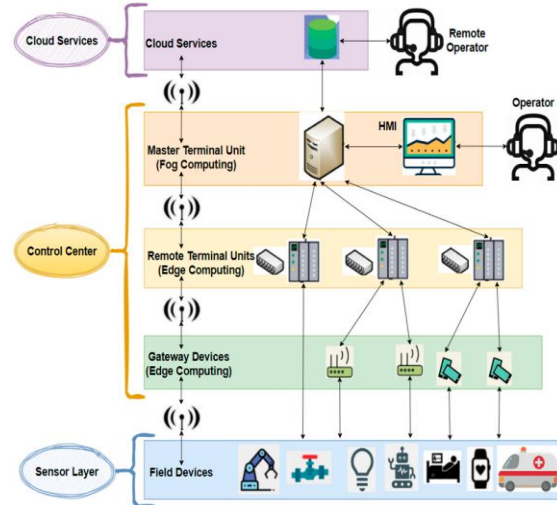


Figure 2: Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures

### 1.3 Emerging Urgency of Transition Planning Due to Anticipated Quantum Breakthroughs

How soon robust, scalable quantum computers will be possible to use to break existing cryptographic protocols is unclear. However, the consensus among experts is that the move towards quantum resistance is imminent. Solutions have to happen now. Geremew and Mohammad (2024) also explain that, after the long lifecycle of critical systems and the challenges associated with removing embedded cryptographic entities, transition planning should be taken into consideration. In the absence of prior planning, defense agencies may fail to respond promptly to quantum breakthroughs, leading to security lapses that adversaries can exploit.

### 1.4 Problem Statement

The rise of quantum computing poses an impending and unique threat to the security of major infrastructure and nationwide security networks that rely on conventional cryptography algorithms. These encryption algorithms (used today), like RSA, ECC, and Diffie-Hellman, which form the basis of secure communications, data matching, and system authentication in the military, intelligence, and infrastructure networks, are mathematically insecure against quantum algorithms such as Shor and Grover. With the pace of cryptanalytically relevant quantum computing accelerating worldwide, the imminent

obsolescence of the current cryptographic environment looms, threatening to expose classified knowledge, disrupt command and control systems, and compromise key national assets. Although there is an increasing number of studies on post-quantum cryptography (PQC), and a standardization process is underway among government agencies like NIST, national defense systems are generally not yet ready to implement the transition. The existing infrastructure employs outdated cryptographic protocols, which are neither flexible nor easily updated.

Furthermore, the absence of a coherent strategic plan in evaluating risk, articulating policy on the one hand, and technology migration on the other, has left critical areas lacking care in response. In the event of quantum-empowered attackers, the inability to develop a proactive and integrated transition plan places the national defense entities at risk of operational and cybersecurity breaches. This paper addresses the need for a developed strategic plan that enables stakeholders to ensure the secure and timely transition of national defense and critical infrastructure to quantum-resistant cryptographic systems. It is not only a technical issue but also an organizational and geopolitical one, which needs cross-sectoral teamwork, solid governance, and sustainable resource management. A wait in action would be disastrous, leaving the most important defense processes vulnerable to the post-quantum world.

### 1.5 Purpose and Scope of the Paper

This paper proposes a detailed strategic plan to achieve quantum-resistant cryptography preparedness in national security, with a focus on key infrastructure sectors. This aims to bridge the gap between the development of theoretical post-quantum cryptography (PQC) systems and practical implementation planning in critical, large-scale, and high-assurance systems. Thus, this paper will identify key risks, explain technological and policy transitions, and provide concrete recommendations to defense planners, infrastructure managers, and national cybersecurity stakeholders, enabling them to prepare efficiently in the post-quantum world.

## II. UNDERSTANDING THE QUANTUM THREAT LANDSCAPE

Quantum computing is poised to revolutionize information processing, as it can perform highly complex calculations with time efficiencies that have never been achieved before. However, quantum computers differ in that they are based on quantum bits (qubits), which behave in a superposition and entangled state, rather than being considered 0 or 1, as is the case with classical computers based on binary bits. This allows for potentially advantageous increased speeds when evaluating particular classes of problems. Although there are great potential implications of this technology in applications such as drug discovery and optimization procedures, its most significant implication is that the technology may compromise encryption systems currently used to protect global communications, monetary transfers, and national militaries (Ferreira, Lipiäinen, & Polito, 2023).

Classical cryptographic systems, and in particular the public-key algorithms used in them, including RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), rely on the difficulty of computational problems such as discrete log, integer factorization, and related problems as the basis of their security. These schemes are said to be secure because they would require a prohibitively long time (in terms of the computer's processing power; see asymptotic complexity) to solve these mathematical problems on a classical computer. Quantum algorithms, however, are threatening these foundations. In particular, the algorithm proposed by Shor enables the efficient factorization of large numbers and calculation of discrete logarithms, which renders RSA and ECC completely susceptible to a total compromise as soon as a sufficiently large quantum computer is constructed (Mashatan & Heintzman, 2021; De Roure & Santos, 2023).



Figure 3: What is Quantum Computing

Even though Grover is less devastating than Shor, it does provide a quadruple-speedup on brute-force attacks on symmetric-key systems, thus necessitating a doubling of the key sizes to achieve similar levels of security. This further imposes a calculation burden on restricted systems, such as embedded systems, which are prevalent in the military (Kubecka, 2024). The impact of such deployment of cryptographic protocols which have not been designed to anticipate these quantum capabilities, cannot be understated: encrypted military communications, command-and-control systems, secure infrastructure channels, and secure communication channels could all be retroactively and prospectively read even after the deployment of such cryptographic protocols, posing existential threats to national sovereignty and operational integrity. Researchers are still uncertain about when cryptanalytically powerful quantum computers (CRQCs) will become a reality, devices that can exploit quantum effects to crack many of the cryptographic schemes currently in use. While there are projections that this feasibility may take 15 to 20 years, other proponents believe it could emerge within 10 years or less, given that quantum hardware is developing at an accelerating rate and with both government and corporate funding being invested (Aydeger et al., 2024). The lack of certainty regarding when quantum preparedness will occur makes strategic planning more difficult, yet that does not diminish the urgency of action. The ambiguity is a strong argument for preemptive action. A rather alarming strategy that has developed in anticipation of CRQCs is the 'harvest-now, decrypt-later' approach.

According to Aydeger et al. (2024), state actors and non-state actors can actively intercept and store encrypted sensitive information or data, including diplomatic communications, military plans, and national infrastructure designs, without decrypting it, with the hope of decrypting it when quantum capabilities become feasible. This latent threat suggests that the cryptographically secured data of today may be compromised and hacked in the future, despite being secure at the time of its creation. The consequences are particularly disastrous in areas involved in national defense, where long-term secrecy and integrity are most valued, and where a single incident can trigger strategic repercussions.

### Quantum Algorithms

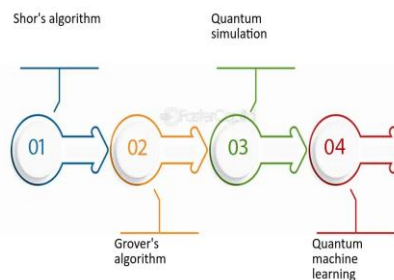


Figure 4: Key Quantum Algorithms

Akhai and Kumar (2024) note that there is a need to initiate the quantum transition process now, given the long lifecycle of military and critical infrastructure systems. Defense systems could be in use for decades, unlike consumer software, which may be updated at any time, making updates a very rapid process. Such systems are often made of highly embedded cryptographic modules, and upgrades are thus slow, expensive, and complicated. Additionally, most existing defense systems lack cryptographic agility, meaning they cannot easily shift between or improve cryptographic protocols. In the future, this will be critical in integrating post-quantum cryptographic (PQC) algorithms.

### III. ROLE OF CRYPTOGRAPHY IN CRITICAL INFRASTRUCTURE AND NATIONAL DEFENSE

The modern digital age is witnessing cryptography as a foundation for establishing the security operations of critical infrastructures and national defense systems. Critical infrastructure. Many elements of critical infrastructure (energy grids, water systems, financial services, transportation networks, healthcare services, and defense facilities) are heavily dependent on cryptographic algorithms to provide confidentiality, integrity, and authenticity of data transmitted and stored. The sectors are highly interdependent and even less dependent on secure communication standards, authentication procedures, and data protection technologies (Baseri, Chouhan, & Ghorbani, 2024). Within the national defense context, cryptographic systems are the foundation of communication, intelligence, command, and control (C4I) systems. These systems handle all aspects of real-time communications with satellites, encrypted battlefield messages, surveillance transmission, and chain of command structures. The single-point failure of any of the C4I layers may cause a game over in the situation awareness, mission accomplishment, or even self-defense systems. Akhai and Kumar (2024) highlight the strategic need for cryptographically secured systems in defense, noting that distributed systems of trust (such as blockchain-bolstered communications) rely on their integrity being fully dependent on resilient cryptographic processes.

The essence of the strategic importance of cryptography consists in its ability to ensure the integrity, confidentiality, and authenticity of the information. Integrity: Makes sure that important information, e.g., target coordinates or system commands, is not altered; confidentiality: Ensures sensitive operations are not subject to an adversary surveillance operation; authenticity: Verifies that a legitimate source issued a message or command. Such are not abstract principles, but rather the practical realities in the world of defense. Split seconds and reliability in information could mean the difference between mission failure and success. According to Syed (2023), the destabilization of these properties by

quantum-empowered actors may cripple defense operations and subject state assets to espionage, sabotage, or even digital warfare. Quantum threat increases national security risks on a large scale. An adversary capable of working with quantum technology may infiltrate defense networks and crack previously encrypted sensitive communications, or replicate a more reliable recipient of a superior command network. According to Csenkey and Bindel (2023), such a threat is not only technological but also geopolitical, thereby posing a threat to various deterrence plans, alliances, and international diplomacy. Strategic advantage and a country's global status depend on its ability to provide secure digital sovereignty in the post-quantum world. De Roure and Santos (2023) emphasize that the necessity of safe cryptographic solutions covers not only classic encryption but also avenues of innovation (such as quantum key distribution (QKD) and post-quantum cryptographic algorithms endorsed by NIST). The technologies are designed to eliminate instances of weaknesses presented by classical systems, such as proposing mathematically unfeasible key exchange protocols or being physically vulnerable. Nonetheless, until national defense infrastructures are flooded with such systems, these systems will still face the threat of emerging challenges.

### IV. POST-QUANTUM CRYPTOGRAPHY (PQC): TECHNOLOGIES AND STANDARDS

4.1 Overview of PQC Approaches (Lattice-Based, Code-Based, Multivariate, Hash-Based, etc.)

Post-quantum cryptography (PQC) is a broad class of algorithms that strive to prevent attacks using both classical computers and quantum computers. In contrast to quantum cryptography (e.g., quantum key distribution), PQC is still based on classical concepts of computation but attempts to resist quantum computers, also using problems thought to be intractable by mechanical means.

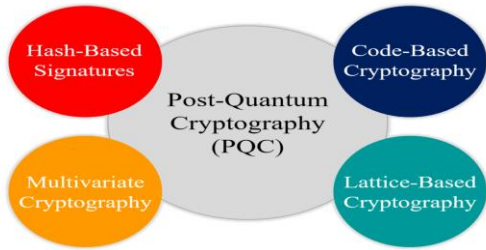


Figure 5: Post-Quantum cryptography

Most prominent families include:

- Lattice-based cryptography is currently the most studied and popular because it strikes a balance between adequacy and performance. The problems used to create these algorithms are quantum-resistant conjectures, such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE).
- Cryptography based on hard problems in decoding random linear codes, e.g., the McEliece encryption scheme. These are characterized by great security but have large keys.
- Multivariate cryptography is based on the hardness of solving systems of multivariate polynomials over finite fields. This family offers the promise of efficient signature schemes but is vulnerable to certain algebraic attacks unless carefully designed and implemented.
- Hash-based cryptography: Hash-based cryptography, particularly in digital signature schemes, relies solely on the security of cryptographic hash functions. The level of their security is very high, but their use is frequently limited due to the stateless Nature of their signing and the insufficiency of their scalability (Bishwas & Sen, 2024; Asimiyu, 2024).

Such varied methods address various cryptographic functions, including encryption, key exchange, and digital signature use, and are fundamental to an infrastructure based on quantum-resistant cryptography.

#### 4.2 Current Research and Standardization Efforts (e.g., NIST PQC Project)

Due to the increasing threat it poses, the quantum threat has led to a world of competition, as noted by the National Institute of Standards and Technology

(NIST) in 2016, which standardizes post-quantum cryptographic algorithms. This undertaking has invited the participation of researchers from around the world, resulting in the selection of numerous finalists and substitute candidates in the evaluation of encryption and digital signatures. As of 2024, NIST has standardized Kyber (lattice-based) for key encapsulation and Dilithium (also lattice-based) for digital signatures, with SPHINCS+ (hash-based) and FALCON (lattice-based) as alternative options. Such algorithms have been chosen due to the painstaking estimations of security, work efficiency, implementation cost, and resistance to side-channel attacks (Geremew & Mohammad, 2024).

#### 4.3 Evaluation of Candidate Algorithms and Their Suitability for Defense Systems

The appropriateness of PQC algorithms for use in national defense systems depends on several factors, including their performance under limited hardware constraints, resistance to side-channel and fault-injection attacks, and compatibility with existing protocols. The Kyber and Dilithium are also regarded as unique cryptographies for use in defense settings, primarily due to their efficiency and sufficient cryptographic strength. These schemes have small key sizes, low computational complexity, and minimal bandwidth requirements, traits that are essential for military-grade communications and embedded systems. Some systems, such as drones, satellites, and tactical radios, where the available processing power and memory are limited, can be problematic even for the most efficient PQC algorithms.

#### 4.4 Challenges in PQC Algorithm Implementation (Efficiency, Bandwidth, Performance)

Although the field of PQC development has made significant progress, numerous implementation issues remain, particularly in challenging environments such as national security and critical infrastructure.

Performance: Not all PQC algorithms are efficient, as they often incur high computational overheads, particularly code-based and multivariate PQC, which cannot be implemented in real-time for defense responses.

**Performance:** Since PQC introduces performance overhead that may be significant in cryptographic processes with ultra-low latency requirements, e.g., missile guidance systems, battlefield decision-making systems, or low-latency sensor fusion systems, this may impact the functional performance of these systems.

**Interoperability with Legacy Systems:** Much existing military infrastructure was created using fixed-function crypto hardware, which is inflexible regarding the implementation of new algorithms. This problem requires cryptographic agility and long-term redesign of a system, as explained by Bishwas and Sen (2024); this is costly and complicated.

**Security Assurance and Trust:** Asimiyu (2024) notes that the theoretical quantum resistance of PQC algorithms does not guarantee their high level of security, as their implementation must be strictly tested to prevent leakage into side channels, poor implementation, or development due to reliance on vulnerable coding patterns.

## V. TRANSITION CHALLENGES AND READINESS GAPS

The idea of modernizing conventional cryptography to post-quantum cryptography (PQC) presents significant challenges, particularly in the fields of national security and critical infrastructure. The most immediate of these is the legacy component of legacy infrastructure, which, in most instances, contains embedded systems programmed decades ago, lacking modular cryptographic agility (Mashatan & Heintzman, 2021). Interoperability and integration are another example of a critical barrier. National defense networks comprise numerous interdependent networks between command, control, communications, and intelligence (C4I) systems and communications satellites, the majority of which have never undergone cryptographic changes in a network consisting of heterogeneous systems. As noted by Ferreira, Lipiainen, and Polito (2023), integrating PQC with distributed and typically proprietary systems is a challenging task that requires consistency and technically nuanced work. The threat of resource

constraints against transition efforts also endangers it. The implementation plans may be slowed down or separated due to financial problems, particularly in underfunded military departments. Adoption is also hindered by operational limitations, including a scarcity of quantum-literate personnel, bandwidth challenges, and inadequate facilities for testing (Aydeger et al., 2024). The lack of a sufficient workforce and the inexistence of PQC expertise and cryptographic engineering skills, especially, aggravate this problem. According to Kubecka (2024), unless companies make strategic investments in quantum-competent human capital, they will find themselves vulnerable during a time when cryptographic insecurity is highly probable. Inertia of policy and resistance to transition would also arise within the organization. Some agencies and contractors cannot afford to deploy untested cryptographic models, particularly in mission-critical activities. The projection of risk aversion regarding the development of quantum-safe solutions, as mentioned by Syed (2023) and Akhai and Kumar (2024), characteristically causes the postponement of necessary upgrades when one believes such a move will lead to instability. Along with that, De Roure and Santos (2023) emphasize that, given the lack of mandates and general legislative incentives, national infrastructure provision companies may refuse to prioritize and invest in the integration of PQCs, leaving national security assets vulnerable to the potential threat of quantum-related attacks in the future.

## VI. PROPOSED STRATEGIC FRAMEWORK FOR TRANSITION READINESS

### 6.1 Risk Assessment and Prioritization

Identifying and prioritizing the most vulnerable systems and data flows to quantum-enabled attacks is the most basic step towards becoming ready to transition. The rational strategic risk assessment should be initiated by digital asset classification according to their criticality and exposure to longer-term confidentiality threats, especially in environments such as defense, wherein the 'harvest-now-decrypt-later' paradigm presents a significant future threat (Aydeger et al., 2024). The components

of national command, control, and surveillance activities should be categorized as high-risk and acted upon with the utmost urgency. Mashatan and Heintzman (2021) further note that it is essential to conduct a cryptographic inventory and map the lifecycle of vulnerable algorithms to understand the exposure an organization poses and develop an active mitigation roadmap.

#### 6.2 Policy and Governance Alignment

The policy and governing framework should be coherent in terms of harmonizing the cryptographic transition activities within the national defense institutions. Syed (2023) emphasizes that incoherent or inconsistent policy guidance among agencies has the potential to slow down the process and leaves the systemic vulnerabilities unsolved. International coordination and consistent standards and compliance benchmarks are key properties of quantum threat governance, as argued by Csenkey and Bindel (2023), who provide references to the interoperability standards set by NIST. Akhai and Kumar (2024) also emphasize the importance of cross-domain regulatory frameworks that encompass national and allied defense networks, ensuring coherence and accountability in cross-border settings.

#### 6.3 Technical Migration Pathways

The transition process toward full quantum resistance will be gradual and will require integrating hybrid cryptographic designs to ensure continuity in operations. De Roure and Santos (2023) argue that at this transitional stage, it is possible to employ a twin-algorithm strategy of classical/quantum-safe algorithms, allowing systems to achieve backward compatibility during the introduction of post-quantum counterparts. Another important enabler is cryptographic agility, which is facilitated by modular design architectures. Baseri, Chouhan, and Ghorbani (2024) advise re-engineering defense systems to enable dynamic switching of their algorithms, decrease the likelihood of aging, and facilitate fast adaptation in response to emerging standards.

#### 6.4 Capacity Building and Resource Mobilization

To successfully overcome this transformation, it is important to invest heavily in human capital and

technical capacity building. Among the most urgent readiness gaps is a lack of professionals who understand both quantum computing theory and cryptographic engineering (Kubecka, 2024). To address this, defense institutions should initiate targeted training programs, learning partnerships, and certifications. The need to allocate more funding for the research and development (R&D) of PQC implementation tools, hardware accelerators for complex algorithms, and quantum-resistant key management frameworks is also mentioned by Aydeger et al. (2024).

#### 6.5 Testing, Simulation, and Pilot Deployment

PQC solutions should undergo rigorous testing in production defense settings prior to implementation. According to Mashatan and Heintzman (2021), we should apply sandbox environments and red-teaming exercises to evaluate the operational effects and performance of quantum-resistant protocols against hacking, which is simulated through cyberattacks. Real-time feedback can be introduced by having an alpha operation in one or two mission-critical areas before further iteratively perfecting the cryptographic modules. Such an adaptive loop is crucial because it enables defense agencies to respond to integration issues and develop threat intelligence that they could not have predicted earlier (Csenkey & Bindel, 2023).

## VII. CASE STUDIES OR GLOBAL BENCHMARKING

The transition to quantum-resistant infrastructure is already underway in the most advanced defense ecosystems, particularly those driven by NATO and the U.S. Department of Defense (DoD). Such institutions have recognized the strategic need to future-proof (quantum-proof) communication systems and data assets against quantum decryption capabilities. An example is the U.S. DoD, which has started adopting post-quantum cryptographic standards by incorporating them into its zero-trust architecture in the wider national efforts to upgrade cybersecurity. These further state that the holistic approach envisioned in the department can be seen in the Quantum Ready Architecture for Security and Risk Management (QUASAR) framework, which

comprises a combination of cryptographic agility, phased implementation rollout, and compatibility with existing defense platforms. The use of this layered approach will ensure that legacy systems are safe to interoperate with future-ready, quantum-safe algorithms and encourage modular upgrades when new and standardized tools emerge. Similarly, NATO has been proactive in emphasizing the importance of member states coordinating the adoption of post-quantum cryptography (PQC). According to Geremew and Mohammad (2024), NATO's efforts include risk modeling collaboration, asset prioritization, and secure communication architecture for allied defense systems. Early piloting of the PQC protocols in strategic communication and logistics systems has resulted from such multinational exercises. The early adopters, which include countries within the transatlantic region, such as some European and Asia-Pacific nations, are at different stages, commensurate with their progress in cybersecurity evolution. It summarizes how other countries, such as the United Kingdom and Japan, have already established national quantum security task forces that can connect state agencies, academia, and private sector R&D to speed up PQC readiness. Such countries have focused on cryptographic agility in the public infrastructure, quantum simulation environments, and talent development. When examining the national security sector as a whole, one observes common themes of strategic alignment during benchmarking activities. Asimiyu (2024) also notes the consistent Nature of successful early adopters in incorporating PQC into their digital transformation plans and roadmaps, in association with resilience planning, secure cloud migration, and adherence to emerging international standards. Bishwas and Sen (2024) continue to note that more systematic roadmaps, where the application of PQC is linked to pre-selected threat models and school performance measurements, also allow more transparent decision-making in defense settings with limited resources.

## VIII. RECOMMENDATIONS

### 8.1 Immediate Action Points for Defense Agencies

With the quantum threat posing a critical issue, defense departments should comprehensively audit all

their cryptographic techniques to identify weak protocols and extremely risky systems. As stated by Geremew and Mohammad (2024), the procrastination in inventorying and categorizing parts of critical infrastructure exposes one to greater threats in the post-quantum world. Specifically, systems based on RSA, ECC, or other weak platforms of public-key algorithms should be noted as needing improvement as soon as possible. Additionally, it is recommended that quantum-enabled malefactors be included in incident response plans. Although the risk of harvest-now-decrypt-later attacks exists today, and sensitive transmissions should be further encrypted, even though adversaries cannot currently break them on the fly (Tubecka, 2024).

### 8.2 Long-Term Strategic Goals for Quantum-Safe Infrastructure

It is imperative that long-term planning not only address technical preparedness, but also encompass policy, governance, and cross-agency coordination. An effective national PQC plan. Investments in research and development (R&D) should also be maintained. Ferreira et al. (2023) recommend establishing national quantum cybersecurity centers that can organize fundamental research, track progress worldwide, and evaluate new PQC solutions under conditions similar to those of military operations.

### 8.3 Encouraging Public-Private Collaboration and International Alignment

PPPs will play a crucial role in scaling PQC solutions across the complex defense supply chains. According to Aydeger et al. (2024), the creation of numerous cryptographic interventions will be in the private sector, mainly utilizing startups and multinational tech companies that are already involved in the development of quantum-safe algorithms. Government-based structures should therefore involve cooperative testbeds, collective repositories of reviewed tools, and accelerated certification schemes for PQC vendors. Across the globe, defense agencies should actively participate in multilateral efforts to harmonize PQC standards. According to Geremew and Mohammad (2024), the failure to adopt cryptographic standards may result in interoperability failures among allied forces and critical infrastructure

partners due to fragmented adoption or inconsistent apparatuses. There should be international collaboration among institutions such as NATO, the EU, and international standards bodies, including the ISO and NIST. Lastly, new crypto will require this crypto paradigm to achieve trusted validation, transparent benchmarking, and transparent risk communication (Mashatan & Heintzman, 2021). Governments must be at the forefront in developing such trust, creating a collaborative ecosystem that involves academia, industry, and civil society.

### CONCLUSION

To protect national security in the era of quantum transformation, it is insufficient to respond to technical threats merely; instead, a paradigm shift is needed in the conceptualization, planning, and execution of cybersecurity. The financial losses are the highest for national defense institutions, as the safe operation of such organizations relies on secure communication, classified information, and stable infrastructure (Baseri, Chouhan, and Ghorbani 2024). National systems may remain susceptible to existential-level breaches because of an inadequate or fragmented response to quantum risks. Thus, early investment in research, intersectoral cooperation, and international standardization should be given priority. As the quantum future dawns, countries that leave their future to be determined will be in the best position to protect their sovereignty and secure their long-term digital well-being, which involves developing efficient, future-proof cryptographic systems.

### REFERENCES

- [1] Bishwas, A. K., & Sen, M. (2024). Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat. arXiv preprint arXiv:2411.09995.
- [2] Asimiyu, Z. (2024). Quantum-Resistant Cybersecurity for Critical Infrastructure: Preparing for the Post-Quantum Era in National Defense.
- [3] Geremew, A., & 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(4), 338–365.
- [4] Ferreira, A., Lipiäinen, V., & Polito, C. (2023). Quantum technologies and cybersecurity.
- [5] Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024, October). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024, the 15th International Conference on Network of the Future (NoF)* (pp. 195–203). IEEE.
- [6] Kubecka, Chris. "Secrets From the Future: Hacking in a Post-Quantum Cryptography World: Implications for Cyber Security and National Defense." (2024).
- [7] Mashatan, A., & Heintzman, D. (2021). The Complex Path to Quantum Resistance: Is Your Organization Prepared? *Queue*, 19(2), 65–92.
- [8] Akhai, S., & Kumar, V. (2024). Quantum resilience and distributed trust: The promise of blockchain and quantum computing in defense. In *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications* (pp. 125–153). Singapore: Springer Nature Singapore.
- [9] De Roure, D., & Santos, O. (2023). NLP, the BB84 quantum cryptography protocol, and the NIST-approved Quantum-Resistant Cryptographic Algorithms. Authorea Preprints.
- [10] Syed, S. A. (2023). THE QUANTUM THREAT: PREPARING FOR THE IMPENDING IMPACT ON CYBER SECURITY. *International Journal of Engineering Technology Research & Management (IJETRM)*, 7(03).
- [11] Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity*, 9(1), tyad001.
- [12] Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. arXiv preprint arXiv:2404.10659.
- [13] Encyclopedia, Q.-. Q. (2023, April 3). A brief history of Quantum Computing - QUANTUMPEDIA - The Quantum Encyclopedia - medium. Medium. <https://quantumpedia.uk/a-brief-history-of-quantum-computing-e0bbd05893d0>

- [14]Engineering, N. K. V. (2024, May 6). What is Quantum Computing? A complete Guide. VLink. <https://vlinkinfo.com/blog/what-isquantumcomputing>
- [15]Quantum Algorithms - FasterCapital. (n.d.). FasterCapital.<https://fastercapital.com/topics/quantum-algorithms.html>
- [16]Gilbert, C., & Gilbert, M. (2024). The Role of Quantum Cryptography in Enhancing Cybersecurity.
- [17]Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT, 2(1), 71-91.