JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 41

The Security implications of Quantum Computing for Encryption Policy

Snehasree Parida, Centurion University

Recommended Citation:

Parida (2026) "The Security implications of Quantum Computing for Encryption Policy" Journal of Cyber Governance and Intellectual Property, Vol. 1, Article 41. (DOI)

ABSTRACT

One of the most significant and emerging technological advancements in the 21st century is "quantum computing". It has the potential to disrupt encryption and cyber security systems all across the world. Pertinently, cryptographic methods available as of now such as Elliptic Curve Cryptography (ECC), RSA and the Diffie-Hellman key exchange protocol place reliance on mathematical problems which are computationally infeasible for traditional computers but which may be solved by the quantum computers efficiently using principle such as entanglement and superposition. The paper examines the impact of "quantum computing" on the existing framework of encryption and seek to evaluate whether the current domestic and international legal regime are adequate to address the emerging cyber security risks revolving around quantum computing. It also seeks to analyze the transition towards post quantum cryptography, specifically referencing the standard developed by NIST - National Institute of Standards and Technology. By using a comparative and doctrine research methodology, the paper categorizes significant policy and regulatory gaps, with a special focus on existing encryption framework in India. It reaches the conclusion that policy makers and government must seek adoption of proactive technological and legal measures for addressing the emerging risks concerning quantum computing.

KEYWORDS

Quantum Computing, Post-Quantum Cryptography, Cybersecurity Law, Encryption Policy, NIST Standards, Information Technology Act

INTRODUCTION

In 2019, a quantum processor by the name of Sycamore was announced by Google. It completed the computational task given to it in 200 seconds, contrary to the allegedly 10,000 years that the world's most powerful classical supercomputer would take to perform the same.[1] This claim was widely debated within the scientific community but at the same time, this particular announcement marked the significant milestone towards the development of quantum computing. It demonstrated the rapid advancement of quantum technologies. However, this development has raised pertinent concerns in the cyber security domain and encryption systems specially those which operate digitally and presently secure government databases, financial transactions as well as critical infrastructure.

The modern cryptographic systems place reliance on mathematical problems which are infeasible for classical computers to solve efficiently. These systems have given way to a foundational secure communication across the world for many years. However, what poses a serious challenge to this framework is "quantum computing". Through principles such as entanglement and superposition, quantum computers would have the requisite capability to execute the algorithms, specifically Shor's Algorithm. This algorithm can easily break the public encryption systems at an exemplary speed, which is practically not attainable by classical computers. Consequently, the data which is secure as of today due to the encryption systems installed in our computers, could become vulnerable in the near future.

The paper seeks to examine this very emergence in light of security implications for encryption policies through a legal lens. The research problem is whether the current domestic and international legal regime is adequate to respond to the risks implicit in the cyber security world due to the quantum computing era. Specific attention has been given to the transition towards post quantum cryptography (PQC), which includes the efforts of generalization led by the National Institute of Standards and Technology (NIST) as well as India's preparedness towards addressing the potential quantum threats through its encryption policies.

[1] Frank Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 NATURE 505 2019.

The paper adopts a doctrinal and comparative research methodology and draws upon policy documents, statues, academic literature as well as international standards. The paper argues that existing regulatory and legal frameworks remain limited to the assumptions of classic computers and systems revolving around it. Therefore, the present framework is not sufficient to address the disrupting capabilities of quantum computing. It is further contended that the threat blooming due to quantum computing is not futuristic or speculative, especially in light of the "harvest now, decrypt later" strategy. Pertinently, this strategy is generally employed by state actors for storing the encrypted data for future decryption.[2]

The paper is divided into six sections. Following this introduction, Section II reviews the relevant literature on quantum computing and cryptographic vulnerability. Section III outlines the research methodology. Section IV analyses the impact of quantum computing on current encryption systems and examines international and Indian policy responses. Section V discusses policy recommendations and proposes a future-oriented legal framework. Finally, Section VI concludes with the key findings and the need for urgent legislative and regulatory reform.

LITERATURE REVIEW

The technical literature on the topic begins in 1994 through Peter Shor, which demonstrates that a sufficiently and significantly advanced quantum computer could factor "large integers in polynomial time".[3] This finding establishes that public encryption systems such as RSA are most likely vulnerable to quantum attacks. Subsequently, Lov Grover in 1996 put forth an algorithm showing that database searches could be significantly accelerated through quantum computing, leading to reduction in effective security of encryption systems of symmetric nature such as AES.[4] Both these works form the technical basis for concerns regarding the security implications of quantum computing for encryption policy. Consequently these works have led to further

[2] U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) & National Institute of Standards and Technology (NIST), *Quantum-Readiness: Migration to Post-Quantum Cryptography* (2023), https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography (last visited, Jun. 7, 2026).

[3] Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science 124 (1994).

[4] L.K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on Theory of Computing 212 (1996)

extensive research on "quantum-resistant" cryptographic systems. Subsequently, attention of the leading scholars shifted towards the post quantum cryptography (PQC). Researchers such as Tanja Lange and Daniel J. Bernstein made extensive contributions to the mathematical development of hash-based and lattice-based cryptographic models which are intended to resist quantum attacks.[5]

Pertinently, much of the literature on the topic remains highly complex and technical as well as insufficient as far as legal and policy aspects are concerned. When it comes to policy oriented and institutional scholarship, the same has largely emerged through the work of the National Institute of Standards and Technology (NIST). In 2016, NIST initiated its "Post-Quantum Cryptography Standardisation Project" in order to evaluate and standardise the quantum-resistant encryption algorithms. This led to the release of the first PQC standards in 2024.[6] This significant initiative has set the benchmark for quantum cybersecurity preparedness globally and has also influenced significant policy responses in many countries. Similar to this initiative, in 2022, the United States National Security Agency (NSA) has also issued guidance on this aspect, whereby it recommended the ongoing migration of national security systems towards the quantum-resistant cryptographic standards.[7]

A broader framework for assessing the quantum technology related risk has also been introduced by various policy scholars. For instance, "Mosca Theorem" conceptualized by Michele Mosca seeks to provide a way of assessing the quantum risk through the relationship between the time required for migration to secure systems, the lifespan of encrypted information and the expected advent of cryptographic sound quantum computers.[8] This framework highlights the immediate need for preparation. Further, as per "harvest now, decrypt later" (HNDL) strategy, the fraudsters might collect the encrypted data available today with an intention of decrypting it as soon as

[5] Daniel J. Bernstein & Tanja Lange, "Post-quantum cryptography," 549 Nature 188, 2017.
[6] National Institute of Standards and Technology, *Post-Quantum Cryptography Standardization*, https://csrc.nist.gov/projects/post-quantum-cryptography (last visited Jun. 7, 2026).
[7] National Security Agency, *Cybersecurity Advisory: Quantum Computing and Post-Quantum Cryptography* (2022), https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF (Last visited Jun. 7, 2026).
[8] Michele Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, 16 IEEE Security & Privacy 38, 2018.

quantum computing capabilities mature.[9] Thus, there is imminent risk for private as well as public shareholders, however, the legal aspects are still underdeveloped.

When it comes to India, the literature on encryption policy is largely centered under the Information Technology Act, 2000 and corresponding rules as far as the academic commentary is concerned. However, in the Indian landscape, minimal attention has been devoted towards the impact of quantum computing on encryption systems. Consequently, debates and discussions still revolve around the "assumptions of classical computing".

Therefore, the existing literature reveals two major gaps. Firstly, an imbalance still exists between extensive technical literature and policy and legal analysis on quantum computing. Moreover, the comparative analysis from legal lens as to how different jurisdictions are currently responding to this quantum transition remains underdeveloped. For instance, the approach of the European Union, towards quantum risk through the NIS2 Directive and the Cyber Resilience Act and the United Kingdom's National Cyber Security Centre's publication on the guidance on PQC migration. Secondly, there is almost no jurisdiction specific research on how the developing economies including India should develop policy and legal frameworks for the transition to post-quantum cryptography. This paper makes an attempt to address these two gaps by doing a comparative legal analysis of quantum-related cybersecurity risks and proposing a future-oriented framework for India's encryption policy in the quantum era.

METHODOLOGY

The paper primarily adopts a doctrinal research methodology and undertakes a comparative legal analysis of frameworks adopted by different jurisdictions and their approach towards emerging threats of quantum computing. The doctrinal approach includes a detailed examination of various case laws, statutes, policies, regulatory frameworks as well as international standards concerning cyber security and encryption for the evaluation of adequacy of existing legal framework to address the challenges that may arise due to the emergence of quantum computing. The primary

[9] Cybersecurity and Infrastructure Security Agency (CISA), *Preparing for Post-Quantum Cryptography* (2021), https://www.cisa.gov/sites/default/files/publications/cisa-insight_post-quantum-cryptography_508.pdf (Last visited Jun. 8, 2026).

domestic sources include the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Information Technology (Amendment) Act, 2008.

The international sources include the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardisation Project and the standards issued thereunder, (including FIPS 203, 204 and 205). Additionally, policy guidance issued by several international institutions such as the European Union Agency for Cybersecurity (ENISA), the United Kingdom's National Cyber Security Centre (NCSC) and the United States National Security Agency (NSA) have also been studied.

Furthermore, a comparative analysis has been employed in order to analyze how various jurisdictions are approaching the emerging challenges of the quantum related cyber security risk and the corresponding transition towards post-quantum cryptographic standards. This exercise has been done in order to identify the best practices for India and evaluate their relevance to India's emerging quantum and cybersecurity framework, particularly in light of the National Quantum Mission launched in 2023. It is important to note that the doctrinal approach comes with a significant limitation that the reliance has been placed mostly on publicly available information.

THE TECHNICAL ASPECTS OF QUANTUM COMPUTING VIS-A-VIS CLASSICAL ENCRYPTION

While classical computers process information in "binary bits" where in each bit is either 1 or 0, the quantum computers use "quantum bits" or "qubits" that can exist in a superposition of 1 and 0 simultaneously. This property of quantum computing combined with quantum interference and entanglement allows the quantum computing to be exponentially faster than classical machines.

Shor's Algorithm is the most important quantum issue to the basic encryption system. This algorithm was provided by Peter Shor in 1994 and enables factoring in large integers in polynomial time, in comparison to which the best standard classical solution is sub-exponential but super-polynomial in time.[10] Thus, a sufficiently capable quantum computer running Shor's

[10] Shor, *supra* note 3, at 126.

Algorithm could be capable of defeating the extensive applied public key encryption standard in a couple of hours/days, while classical machines need billions of years. Further, Grover's Algorithm, although comparatively less exciting in its effect, is still a considerable challenge to symmetric encryption. This algorithm offers a quadratic speed up when searching unsorted databases. This lowers the security of a symmetric key of length N bits to N/2 against a quantum attack.[11] Therefore AES-128, that has its security that is safe against current classical attacks, would have 64-bit security vs. a quantum computer, considered inadequate. AES-256, on the other hand, would have 128-bit quantum security which is acceptable for the current threat models.

Accordingly, the critical policy question is: when will a cryptographically relevant quantum computer (CRQC), a computer capable of executing Shor's Algorithm against public key encryption standard or equivalent, come to exist. Current estimates are wide ranging. IBM's quantum roadmap anticipates the potential for systems with thousands of logical qubits to exist by the late 2020s, despite error correction overhead required for cryptographically relevant computations indicating the need for millions of physical qubits.[12] The expert consensus is that the availability of a CRQC will fall in the time period of 2030-2040, though some assessments suggest the period could potentially be sooner. The fact that it is unknown when a CRQC will become available is a policy problem itself: the transition to quantum-resistant cryptography is a multi-year, complex process, and holding off while waiting for certainty about the threat before initiating a transition is not a strategy that should be pursued.

HARVEST NOW, DECRYPT LATER (HNDL)

Perhaps the most pressing and underappreciated aspect of the quantum threat is the HNDL threat strategy. Presently, intelligence agencies and highly capable adversaries can, and do, intercept encrypted communications and keep these data points forever. The advent of a CRQC will allow this stored ciphertext to be decrypted retroactively. As a result, important data such as diplomatic communications, financial records, health data, and classified government information is already vulnerable to future exposure.

[11] Grover, *supra* note 4.
[12] IBM Quantum, *IBM Quantum Development Roadmap* (2023), https://www.ibm.com/quantum/roadmap (Last visited Jun. 8, 2026).

The legal ramifications of HNDL are profound. Under the Digital Personal Data Protection Act, 2023 (DPDPA), data fiduciaries are required to undertake "reasonable security safeguards" to guard against personal "data breaches".[13] If it is known that the encryption standard being used to protect personal data is vulnerable to a foreseeable quantum attack, the question arises whether a failure to migrate away from this standard counts as a failure of the "reasonable security safeguard" obligation. Similarly, under the 2000 IT Act, Section 43A creates liability for body corporates that negligently handle sensitive personal data.[14] The HNDL threat arguably invades this responsibility regime by placing quantum vulnerability within the purview of these pre-existing obligations, even if no CRQC has the maturity to exist.

INTERNATIONAL POLICY RESPONSES: THE NIST POST- QUANTUM CRYPTOGRAPHY STANDARDS

Allegedly, the most significant international policymaking response to the quantum threat is the NIST Post-Quantum Cryptography Standardisation Project. Launched in 2016, this project solicited candidate post-quantum cryptographic algorithms from cryptographers across the world. The first set of finalised PQC standards in August 2024 are:

(i) FIPS 203 (ML-KEM): Based on the CRYSTALS-Kyber algorithm, FIP S203 offers a key encapsulation mechanism resistant to quantum attacks capable of replacing RSA and ECC in key exchange protocols.[15]

(ii) FIPS 204 (ML-DSA): Based on the CRYSTALS-Dilithium algorithm, FIPS 204 offers a quantum attack-resistant digital signature scheme.[16]

(iii) FIPS 205 (SLH-DSA): Based on the SPHINCS+ algorithm, FIPS 205 offers a stateless hashbased digital signature scheme in lieu of lattice-based alternatives.[17]

[13] Digital Personal Data Protection Act, 2023, § 8(5) (India).
[14] Information Technology Act, 2000, § 43A (India)
[15] National Institute of Standards and Technology, *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard* (2024).
[16] National Institute of Standards and Technology, *FIPS 204: Module-Lattice-Based Digital Signature Standard* (2024).
[17] National Institute of Standards and Technology, *FIPS 205: Stateless Hash-Based Digital Signature Standard* (2024).

Pertinently, the United States has called for federal agencies to start migrating to these standards and the NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) provides timelines for staggered migration for different categories of national security systems: software and firmware signing should prefer CNSA 2.0 algorithms by 2025, should completely transition exclusively by 2030, web browsers and cloud services by 2033, and all national security systems should fully transition by 2035.[18]

The European Union has taken a similar stance on the quantum threat. ENISA issued its report on post-quantum cryptography in 2021, advocating for a "crypto-agility" design strategy, making systems capable of rapid cryptographic algorithm replacement as a critical principle for handling the quantum transition.[19] The EU has impliedly and potentially taken a step to legislate the Quantum Transition Response in the form of its Cyber Resilient Act [Regulation (EU) 2024/2847)] and the NIS2 Directive [Directive (EU) 2022/2555]. Both establish terms that create a plausible legal basis for adopting quantum-resistant security measures in the absence of any explicit call to adopt PQC.[20] The NIS2's Article 21 compels operators of essential services to undertake "state of the art" technical measures in relation to their cybersecurity risk management responsibilities; as quantum threats become more specific, national competent authorities may plausibly interpret continuing to use classical encryption as not satisfying this standard. Likewise, the Cyber Resilience Act establishes "security-by-design" obligations for makers of connected products encompassing their whole lifecycle, an obligation that is inherently an anticipatory process potentially embracing PQC integration as quantum timelines become more defined. The EU's involvement captures a form of technology-agnostic future-proofing: instead of specifying a particular algorithm the EU develops a legal structure in which mandates for PQC adoption can take shape within a phase-honed and structured regulatory guidance in response to the improving quantum timeline.

---

[18] National Security Agency, *Commercial National Security Algorithm Suite 2.0*, Cybersecurity Advisory (Sept. 2022), https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF. (Last visited Jun. 10, 2026).

[19] European Union Agency for Cybersecurity (ENISA), *Post-Quantum Cryptography: Current State and Quantum Mitigation* (2021), https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. (Last visited Jun.10, 2026).

[20] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive), Art. 21; Regulation (EU) 2024/2847 (Cyber Resilience Act).

The NCSC in the United Kingdom has issued guidance to indicate that organisations must begin preparing for their transition to PQC. It also emphasises a sense of urgency for systems that secure data with long-term sensitivity.[21] The strategy of the UK involves guidance rather than a requirement to migrate; however, the NCSC has suggested that PQC timelines will steadily be made finer for critical national infrastructure operators.

ASSESSMENT OF INDIA'S ENCRYPTION POLICY FRAMEWORK

India's legal infrastructure for encryption is completely ill-equipped to handle the quantum era. The Information Technology Act, 2000 empowers the Central Government under Section 84A to prescribe encryption modes and methods as part of securing electronic records and communications. However, this power has rarely been exercised and an all-encompassing national encryption policy has yet never been framed and implemented.

Pertinently, a draft of a National Encryption Policy was released by the Ministry of Electronics and Information Technology (MeitY) in 2015 but was withdrawn within a few weeks of its release, due to criticism on its provisions, specifically which directs the citizens to maintain plaintext copies of encrypted communications in storage for 90 days.[22] Even after ten-years from this withdrawal, no substitute policy for a replacement encryption policy has been put forward. Consequently, this creates a vacuum in this regulatory framework by which encryption standards within India are essentially a product of market practice and international standards as opposed to national policies or frameworks.

The National Quantum Mission (NQM), authorized by the Union Cabinet in April 2023, with a budgetary allocation of Rs. 6003.65 crores constitute India's largest policy commitment towards quantum in terms of its financial magnitude.[23] The objective of NQM is the creation of intermediate-scale quantum computers, quantum communication networks and quantum-safe cryptography facilities. However, NQM is essentially a research and development initiative

[21] National Cyber Security Centre (UK), *Preparing for Quantum-Safe Cryptography* (2020), https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography. (Last visited Jun. 11, 2026).
[22] Ministry of Electronics and Information Technology, *Draft National Encryption Policy* (2015) (withdrawn).
[23] Press Information Bureau, *Cabinet Approves National Quantum Mission*, Government of India (April 19, 2023), https://pib.gov.in/PressReleasePage.aspx?PRID=1917855. (Last visited Jun. 12, 2026).

which does not create any legal obligation to migrate to quantum-resistant encrypted standards in government agencies and private sector firms.

Notably, while the Digital Personal Data Protection Act, 2023 is a significant evolution in India's data protection framework, it alludes to no quantum-computing or post-quantum cryptography issues. Further, the "reasonable security safeguards" within the DPDA is completely technology-neutral, creating an issue of adaptability but a lack of clarity on what to require as the quantum threat becomes more imminent in the near future.

Thus, there is a dearth in policy considerations and India has no laws or guidelines in place for mandating government agencies or critical infrastructure operators to evaluate their vulnerability status, create migration plans and adopt quantum-resistant cryptographic standards. This almost complete absence is especially worrisome as India's digital infrastructure [including the Unified Payments Interface (UPI), the Aadhaar biometric database and government e-governance platforms] is heavily dependent on classical encryption standards, making it all susceptible to quantum attack.

DISCUSSION

The analysis shows a significant unevenness between the pace at which quantum computing technology is developing and the pace at which legal and policy frameworks are being considered. This indicates that the technical aspects of the threats of the emerging quantum computing have been responded to by the scientific community rapidly and with great severity. For instance, the NIST PQC standards signify that an intensive research on cryptographic methods has been done for over a decade and they also represent reliable solutions to the quantum threat while also discussing the corresponding technical aspect. In contrast, the policy and legal community has been far slower to respond. Most pertinently, when it comes to India, one would presently find no engagement, discussions or deliberations on the issues.

Pertinently, several policy implications flow from this analysis. Firstly, India should adopt the principle of "crypto-agility" in the encryption policy. Crypto-agility is the ability of quickly adapting to new "cryptographic standards" with the advent of technology. Thus, laws in place

must ensure enough flexibility for replacing the vulnerable or outdated algorithms without needing to rebuild the entire infrastructure.

Secondly, the policy makers must remain alert due to the HNDL threat and accordingly, the shift to post quantum cryptography (PQC) must begin immediately. Notably, sensitive data such as financial information, health records, and correspondence with the government must be encrypted using the standards which are "quantum resistant". This must be done as soon as possible. Moreover, "reasonable security safeguard" obligation under DPDPA should be interpreted to include quantum risk assessments, especially for organizations handling the sensitive personal data.

Thirdly, India must implement an act specifically dedicated to "Quantum-Safe Cryptography Transition". Otherwise, it must amend the IT Act to include a specific mandate for quantum-resistant encryption in critical sectors. Therein, the provisions could require the government to undertake a complete quantum vulnerability assessment, establishment of an advisory council for quantum cryptography and requirement imposed on organizations to disclose data breaches concerning quantum technology under the DPDPA framework.

Fourthly, India must make active efforts to participate in international discussions on developing post quantum cryptography standards including those revolving around National Institute of Standards and Technology (NIST) and ISO/IEC. This will help in ensuring that the global standard includes the regulatory and technological needs of India into account. Moreover, the involvement of India in the NQM places it in a powerful and secure position for it to contribute meaningfully through the development of the concerned standards.

Notably, the current law being the IT Act was drafted in 2000 which contains the classical encryption provisions. These provisions were drafted for a world in which quantum computing was just a looming thought and a futuristic possibility. Consequently, the policy makers are in a challenging position to overcome the slow pace of quantum cryptography discussions and consequently, to finally be prepared to counter the quantum threats that might emerge sooner than we think.

CONCLUSION

Quantum computing poses "an existential threat" to the classical encryption systems, which at present, acts as the primary security system for digital infrastructure across the world. However, it is evident from the above discussion and analysis that India is not ready to address this threat as far as the existing policy and legal framework is concerned. The analysis, especially the HNDL strategy, indicates that the threat is not merely prospective and that the threat is imminent as attackers are already storing the encrypted information for decrypting the same in future using quantum technology.

Internationally, the situation is such that the NIST PQC standards published in 2024 provide a reliable technical foundation for the transition to quantum-resistant cryptography. Prominent countries such as the United States, the United Kingdom and the European Union have started the process of encouraging or mandating this transition. However, India does not have a comprehensive encryption policy adaptable to the emerging quantum technology, has no legal mandate for adoption of PQC and has not adopted the key ambitions of the National Quantum Mission (NQM) into concrete regulatory obligations.

The central contributions of the paper specifically include the theoretic inclusion of Shor's Algorithm and Grover's Algorithm to elicit the imminent quantum threat to public-key encryption, with the projection of a cryptographic quantum computer likely in the range of 2030-2040 i.e., roughly four-14 years ahead of present day.[24] Further, the HNDL threat indicates that legal duties of data fiduciaries under the DPDPA and the IT Act ought to be interpreted to encompass quantum-risk assessments and planning for migration. Lastly, India requires urgent legislative reform through amendment to the IT Act or the creation of specific quantum-safe cryptography legislations, in order to enforce a structured and time-bound movement toward a post-quantum cryptographic standard.

Accordingly, the time for proactive policy intervention is running. The movement towards PQC is a complex, multi-year endeavor that spans the substitution of cryptographic libraries in millions of systems, re- training of technical staff members, and re-negotiation of technology procurement standards. Every year of delay is a year in which sensitive data is vulnerable to

[24] Michele Mosca & Mark Mulholland, *2023 Quantum Threat Timeline Report*, Global Risk Institute, https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/. (Last visited Jun. 14, 2026).

harvest-and-decrypt attacks. Thus, it is highly recommended that India must treat quantum-safe cryptography not as a future aspiration, but as an urgent legislative one.