Quantum Diplomacy, Data Security, and India's Digital Future

Nitin Bayal*
Senior Researcher, Department of Computing, Faculty of Technology, University of Turku, Finland
E-mail: nitin.bayal@protonmail.com

India is living through a digital revolution at a scale few countries have attempted. From Aadhaar-enabled identity services and UPI-based real-time payments to National Health Systems Resources, telecom networks, and advanced biomedical research, data has become the invisible infrastructure of governance, science, and the economy. India's digital public infrastructure is advancing from the classical to the quantum era. Its four strategic pillars: communication, sensing, computing, and cryptography promise transformative benefits in various sectors, i.e., pharmaceuticals, finance, artificial intelligence (AI), logistics, space exploration, and energy. However, the same leap in computing power introduces a profound risk for data security systems.[1-3] As new technologies advance, widely used encryption and digital signature methods will become vulnerable. Many critical data types, such as identity records, healthcare data, financial archives, and scientific repositories, must remain confidential. India will therefore need a shift to post-quantum cryptography (PQC), a new generation of data security systems designed to resist attacks from powerful quantum computers.[4] PQC should be the immediate imperative because of the 'harvest now, decrypt later' threat, i.e., data encrypted today can be collected and decrypted later once sufficiently capable quantum capabilities evolve. In other words, while quantum risks may take years to hit, the countdown has already begun.[1-3]

Science Diplomacy and Quantum Risks

Science diplomacy is often described in terms of scientific alliances, collaborations, and large mega science projects. In the quantum era, diplomacy also plays an important role in coordinating transition timelines to quantum-safe data security, setting technology standards, managing critical digital infrastructure, and ensuring that systems remain interoperable, mitigating quantum risks. This matters because India's digital ecosystem is deeply connected to the world. If countries adopt different security baselines at significantly different paces, interoperability can weaken, and trust can erode. In practical terms, stalled or uneven upgrades can translate into greater friction in sensitive international exchanges: more audits, tougher compliance requirements, delayed partnerships, and reputational 'trust deficits' that affect finance, research collaboration, and digital governance.[5-6]

The Missing Strategy in India's Quantum Ambitions

India has formally acknowledged the strategic importance of quantum technologies through the National Quantum Mission, under the Government of India (GoI). Defence Research and Development Organisation

* Views in the article are of the author and do not belong to the organisation they represent.

(DRDO) and Indian Space Research Organisation (ISRO) have demonstrated their competence in secure communication methods for defence and space applications. These achievements show that India is not starting from scratch, and quantum-safe communication is already a strategic priority in sensitive domains.[7-8] The Indian Computer Emergency Response Team (CERT-In) and the Ministry of Electronics and Information Technology (MeitY), along with industry partners, have begun promoting 'quantum cyber readiness' through advisories and whitepapers, including joint reports with firms such as SISA.[9] These documents have already speculated that future quantum computers could compromise today's data security approaches. They rarely address public digital systems and integrate the scientific, policy, and long-term societal risk dimensions for nationwide PQC transition. Upgrading to deeply embedded and often legacy cryptographic components of the digital ecosystem will require careful planning and coordinated action at scale.[4] Without crypto-agility – the ability to update encryption without rebuilding entire systems – future upgrades will be slow, expensive, and difficult to manage. The key science diplomacy risk here is asymmetry, or a quantum divide, which is not only about who has quantum computers first; it is about who can operate secure, interoperable infrastructure across borders and who becomes dependent on someone else's stack.[5-6]

Diplomatic Arena for Quantum-Safe Standards

In science diplomacy, technical standards often function as geopolitical infrastructure. One of the prime examples is the ongoing global effort to standardize PQC, led by the U.S. National Institute of Standards and Technology (NIST).[4] The de facto standards or monopoly can create geopolitical vulnerability. The stakes are immense for India and imply that PQC readiness is not only about algorithms, but also about platforms that run them. If global standards converge, cross-border services and data flows become seamless and secure. However, if the world fragments into incompatible cryptographic zones, securing international finance, trade, and research will become fraught with friction. This transforms PQC from a simple transition plan into a strategic imperative for participation in global security governance.

The European Commission is also encouraging EU member states for a coordinated PQC transition, supported by the European Union Agency for Cybersecurity (ENISA) assessments.[5-6] Within this landscape, Finland stands out for translating the quantum threat into practical national governance through its preparedness framework, most notably 'Data Security Impacts of Quantum Computing – Preparedness Recommended', prepared by the National Emergency Supply Organisation's Digipool and VTT Technical Research Centre of Finland Ltd.[10] Also, Finland's National Cyber Security Centre (NCSC-FI) has issued operational guidance on PQC transition complemented by policy briefs from VTT, 'Kvanttiturvalliset salausmenetelmät Suomessa' summarising Finland's PQC capability-building and preparedness work.

These assessments reveal that other organisations lack basic visibility into their own cryptographic practices. Awareness of the quantum threat is relatively high, but concrete action, such as planning for transition, allocating resources, or training personnel, is limited. Finland has one of the finest national level 'quantum preparedness' guides currently available, translating the quantum threat into a practical transition manual for organisations that run critical services, with an indicative timeline that starts with inventory work during 2024-2026, planning across 2025-2028, and transition execution through 2026-2030.[10]

India has now articulated a national quantum-safe security plan, but the real test will be implementation, sectoral coordination, certification capacity, vendor readiness, and international interoperability.[11] Adapting the Finnish approach would help India to strengthen both domestic resilience and international trust for their post-quantum strategic plans.

Table 1: Recommendations for different stakeholders in India

Stakeholders	Primary Focus	Key Actions
Government	Coordination and minimum requirements	• Mandate cryptographic inventories for critical sectors and digital public infrastructure. • Publish time-bound milestones. • Create a national coordination forum linking MeitY/DST, sector regulators, critical infrastructure operators, and cybersecurity experts.
Industry	Implementation and transparency	• Publish PQC transition timelines to enable coordination with partners. • Prioritise PQC transition for infrastructure components that issue, manage, and rely on digital certificates.
Academia	Capacity building and standards participation	• Expand training in Quantum technologies. • Encourage active participation in standards bodies and open technical forums that shape strategic positioning.
Individuals and SMEs	Risk assessment and basic preparedness	• Keep OS/browsers core systems updated (so that quantum-safe upgrades can be adopted quickly). • Prefer vendors that demonstrate crypto-agility. • Classify data by longevity and reduce retention of high-sensitivity data.

Conclusion: Data Security as Science Diplomacy

Quantum technologies introduce a diplomatic paradox: they demand collaboration to build interoperable, secure systems while also intensifying strategic competition. The PQC transition process will test stakeholders' strategic awareness and operational readiness.[12] Data security will increasingly become a diplomatic concern alongside a technical one. Trust in cross-border data flows and international research collaboration will depend on shared commitments to quantum-safe systems. In this context, standards coordination, interoperability, and preparedness will shape the reliability, credibility, and resilience of partnerships in digital governance and data-intensive science and technology programs.[13] India has the talent, ambition, and strategic incentives to lead its quantum capabilities into civilian readiness – through clear timelines, comprehensive inventories, prioritisation, and crypto-agile procurement – while simultaneously engaging internationally to help shape the standards and trust frameworks that will define the next era of digital governance. In the quantum era, data security will increasingly function as diplomacy, as the infrastructure of trust can be negotiated, standardised, and demonstrated.

References

1. Mosca M (2018) Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5): 38–41. https://doi.org/10.1109/MSP.2018.3761723
2. Shor PW (1994) Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), Los Alamitos, CA: IEEE. pp. 124–134. https://doi.org/10.1109/SFCS.1994.365700
3. Global Risk Institute (2023) Quantum Threat Timeline Report 2023. Ottawa: Global Risk Institute. https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
4. National Institute of Standards and Technology (NIST) (2024) Post-Quantum Cryptography Standardization Project. Gaithersburg, MD: NIST. https://csrc.nist.gov/projects/post-quantum-cryptography
5. European Commission (2025) A coordinated implementation roadmap for the transition to post-

quantum cryptography. Brussels: European Commission. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

6. European Commission (2024) Recommendation (EU) 2024/1101 on a coordinated implementation roadmap for the transition to post-quantum cryptography. Brussels: European Commission. https://eur-lex.europa.eu/eli/reco/2024/1101/oj
7. Defence Research and Development Organisation (DRDO) (2022) Quantum key distribution experiments and secure communication initiatives. New Delhi: Press Information Bureau (Government of India). https://www.pib.gov.in/PressReleasePage.aspx?PRID=1800648
8. Indian Space Research Organisation (ISRO) (2023) Free-space and satellite-relevant quantum communication experiments. Bengaluru: ISRO. https://www.isro.gov.in/Quantum%20Key%20Distribution%20%28QKD%29.html
9. CERT-In, SISA (2023) Quantum cyber readiness: Preparing India's digital infrastructure for the quantum era. New Delhi: Indian Computer Emergency Response Team (CERT-In) and SISA. https://www.sisainfosec.com/downloads/white-papers/transitioning-to-quantum-cyber-readiness-a-white-paper-by-cert-in-in-collaboration-with-sisa.pdf
10. National Emergency Supply Agency (2024) Data security impacts of quantum computing: Preparedness recommended. Helsinki: National Emergency Supply Agency. https://www.huoltovarmuuskeskus.fi/files/3a17a4fc1889b0c36cfe61b950d14b82a36e8a59/hvk-datasecurityimpactsofquantumcomputing-2024-saavutettava.pdf
11. Department of Science and Technology, GoI (2026) Implementation of Quantum Safe Ecosystem in India: Report of the Task Force (February 2026). New Delhi. https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf
12. Dekkaki KC, Tasic I, Cano MD (2024) Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies*, 12(12): 241. https://doi.org/10.3390/technologies12120241
13. Hasan KF, Simpson L, Baee MAR, Islam C, Rahman Z, Armstrong W, Gauravaram P, McKague M (2024) A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*, 12: 23427–23450. https://doi.org/10.1109/ACCESS.2024.3360412