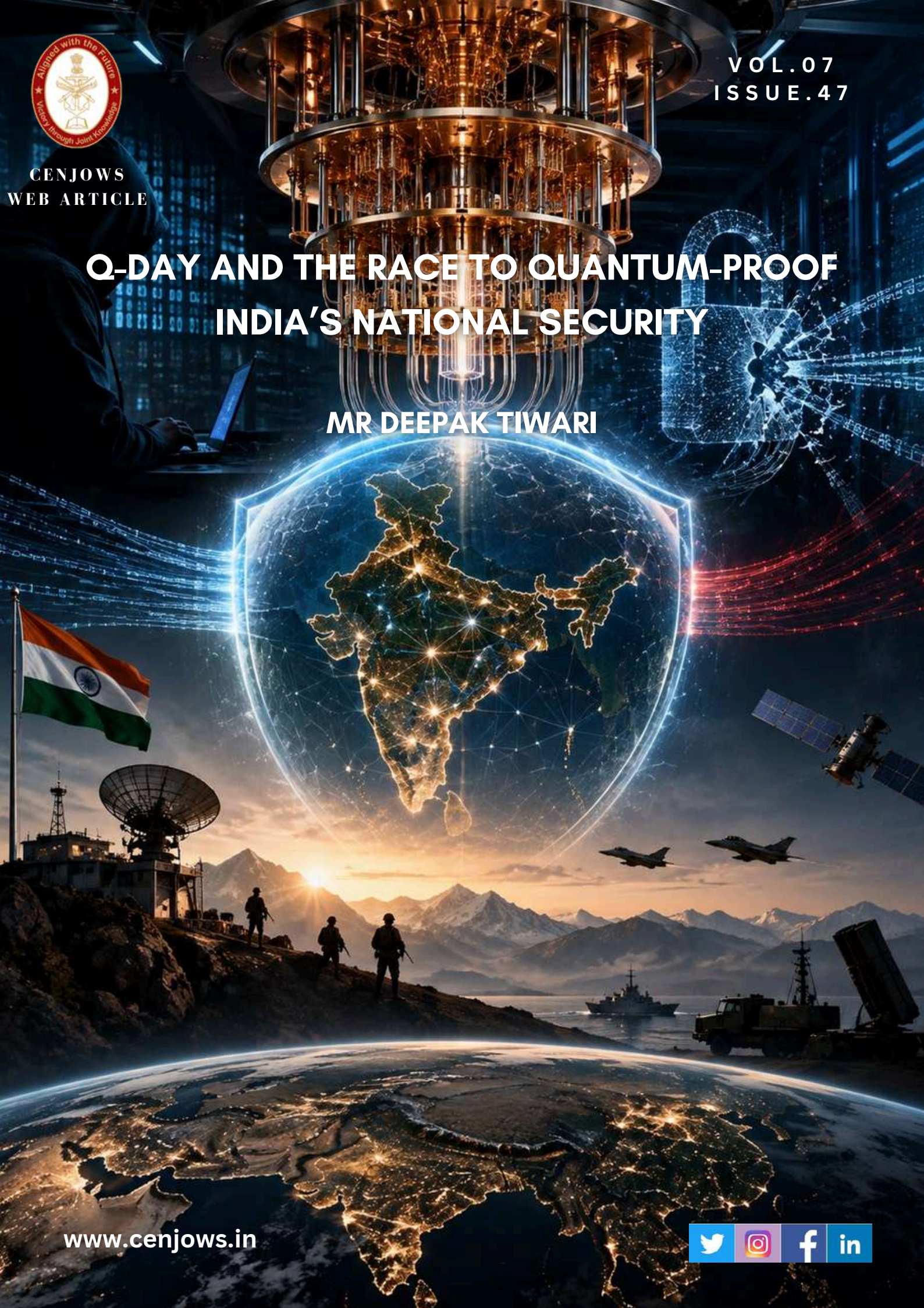
CENJOWS
WEB ARTICLE

VOL.07
ISSUE.47

Q-DAY AND THE RACE TO QUANTUM-PROOF INDIA'S NATIONAL SECURITY

MR DEEPAK TIWARI



www.cenjows.in

CENJOWS WEB ARTICLE

Volume 07 Issue 47 SEP 2026

CENJOWS

(Established: 2007)

Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan,
CGO Complex, Lodhi Road
New Delhi –110003 (INDIA)
Telephone Nos: 011-24364881, 24366485
Fax: 011-24366484
Website: www.cenjows.in
E-mail: cenjows@cenjows.in

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Starting Year : 2020

Year of Publication : 2026

Frequency : Weekly

Language : English

Publisher : Maj Gen (Dr) Ashok Kumar, VSM (Retd) Director General, CENJOWS

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003

Editor : Maj Gen (Dr) Ashok Kumar, VSM (Retd) (dg@cenjows.in)

Deputy Editor : Dr Ulupi Borah, Distinguished Fellow (distinguishedfellow1@cenjows.in)

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS) 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484 e-mails:
cenjows@cenjows.in / cenjows@yahoo.com Website: http://cenjows.in

Price: Rs 150/- INR

Q-DAY AND THE RACE TO QUANTUM-PROOF INDIA'S NATIONAL SECURITY

CONTENTS

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Q-Day and the Race to Quantum-Proof India's National Security

Mr Deepak Tiwari is a Technical Research Assistant at CENJOWS

Why a Future Event Already Demands Action in Present

Somewhere in the next decade, a machine will exist that can do something no computer has ever done, i.e., read the world's secrets. Not by stealing passwords or exploiting software bugs, but by solving the mathematics that our entire digital trust system is built on. Cryptographers have given this moment a name, "Q-Day", the day a quantum computer becomes powerful enough to break the encryption that currently protects everything from bank transfers to military orders.[1]

No one can say precisely when Q-Day will arrive. Most experts think it will happen sometime in the 2030s, and very few expect it before 2030. The US National Institute of Standards and Technology (NIST) has already set 2030 as the point where it begins retiring vulnerable algorithms and 2035 as the deadline for removing them entirely.[2] But the uncertainty around the date is precisely what makes this dangerous. This is not a

threat that gives advance warning. A senior quantum scientist at Booz Allen Hamilton recently noted that most industry roadmaps expect quantum computers to threaten current encryption within about five years and that both hardware and algorithmic progress keep pulling that estimate closer, not further away.[3] Every few months brings a new research paper that shaves zeros off the number of qubits. Studies published in January 2026 suggested that breaking widely used encryption might require only around 10,000 qubits, a dramatic drop from the millions once assumed necessary, and this reduction has visibly sped up the whole conversation around Q-Day. Google's own Quantum AI team has since suggested that elliptic curve cryptography, the kind of encryption protecting most banking and government transactions worldwide, could theoretically be broken using roughly twenty times fewer physical qubits than earlier estimates assumed, prompting the company to set 2029 as its own internal migration deadline.[4]

The reason this matters right now, and not in 2032, is a concept security professionals call “harvest now, decrypt later.” An adversary does not need a working quantum computer today to benefit from one tomorrow.[5] It simply needs to steal and store encrypted data now and wait for the day it can be unlocked. Information that needs to stay secret for years or decades, such as troop deployment plans, weapons designs, intelligence sources, treaty negotiations, satellite architectures, etc., is now already highly vulnerable, and every day of delay adds another year of data sitting somewhere in a server, waiting.

Sorting Fact from Hype

Given the stakes, it is worth being honest about what has actually been proven and what has not. Chinese research groups have repeatedly generated global headlines by claiming to have used quantum computers to crack encryption. In 2024, a Shanghai University team published a paper describing an attack on RSA (Rivest, Shamir, and Adleman encryption) using a D-Wave quantum annealer, and headlines ran with phrases like “military-grade encryption broken.” A closer look showed the team had actually factored a 50-bit number using a hybrid quantum-classical method, a genuine research

milestone, but nowhere close to threatening real-world RSA keys, which typically run to 2048 bits.[6] The same group returned in April 2025 with a slightly larger 90-bit factorisation, still the largest of its kind, but again far short of anything used in practice. A separate paper with the eye-catching title “A First Successful Factorization of RSA-2048” turned out, on inspection, to have used a special, easy-to-factor class of numbers rather than a genuine RSA-2048 key.[7] These episodes are worth remembering not because the threat is exaggerated but because they show how quickly claims outrun capability in this field and why India's own planning needs to be grounded in engineering reality rather than headlines.

That said, the underlying technical direction is not in doubt. In August 2024, NIST finalised the world's first three post-quantum cryptography standards: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) for encrypting data in transit, Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures, and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) as a backup signature scheme built on a different mathematical foundation, followed by the selection of a fourth algorithm, Hamming Quasi-Cyclic (HQC), in 2025.[8] These are not experimental proposals; they are the algorithms that governments and companies worldwide are now expected to build into their systems. The US National Security Agency has already told its national security systems that any new acquisition must be quantum-safe by January 2027, and other allies have set their own deadlines.[9]

India's Exposure and Its Stakes

India's vulnerability here is not abstract. The country has built, in less than a decade, one of the largest digital public infrastructures on earth, and almost all of it rests on the same classical cryptography that quantum computing threatens. Digital payments crossed roughly 22,000 crore transactions in 2024 - 25, with UPI (Unified Payments Interface) making up the overwhelming share and running as the largest real-time payment system in the world.[10] Moreover, Aadhaar has issued over 1.3 billion identities with authentication requests running into billions every month. IBM Research India's director has pointed out plainly that platforms like Aadhaar and UPI depend on encryption that quantum computing

could eventually defeat and that data being harvested today could be unlocked once quantum capability catches up.[11] Add to this India's defence communications, satellite links, and intelligence networks, and the exposure spans nearly every layer of the state.

But India also holds real cards. Its scale in software and mathematics talent, a functioning National Quantum Mission, and a strategic culture that increasingly treats technological self-reliance as a security imperative give it a genuine chance to build indigenous quantum-safe capability. The challenge is one of speed and coordination rather than raw capacity. In that context, India has to move at the pace the threat demands, across a state apparatus that does not always move quickly.

What India Has Actually Done

To its credit, India has moved with greater purpose on this front than is commonly recognised. The Union Cabinet approved the National Quantum Mission in April 2023 with an outlay of ₹6,003.65 crore for the period 2023-24 to 2030-31, and the mission has set up four thematic hubs: quantum computing at IISc Bengaluru, quantum communication at IIT Madras with C-DOT, quantum sensing at IIT Bombay, and quantum materials at IIT Delhi, connecting over 150 researchers across 43 institutions in 17 states.[12]

On the defensive side specifically, the Department of Science and Technology (DST) released a report in May 2026 titled the Roadmap to Quantum Resiliency, setting out a dual-track approach. These two tracks are broad post-quantum cryptography deployment across the wider digital ecosystem, combined with quantum key distribution for the most sensitive strategic links.[13] This built on an earlier February 2026 report, “Implementation of Quantum Safe Ecosystem in India,” produced by a dedicated task force under the National Quantum Mission, which called for accelerated adoption timelines in defence, telecom, and energy, mandatory cryptographic inventories, and a tiered national testing and certification framework for quantum-safe products. Under this roadmap, critical information infrastructure, the systems whose failure would cripple defence, telecom, or power, is being pushed toward full post-quantum adoption by 2029, with broader enterprise adoption targeted by 2033.[14]

On the harder engineering side, DRDO has been building real, tested capability. In June 2025, DRDO and IIT Delhi successfully demonstrated free-space quantum secure communication using entangled photons over more than a kilometre in the IIT Delhi campus. In this experiment, they achieved a secure key rate of around 240 bits per second with a quantum bit error rate under 7 percent.[15] It was a follow-on to an earlier intercity quantum communication link demonstrated between Vindhyachal and Prayagraj in 2022 and a 100-kilometre quantum key distribution trial over telecom-grade optical fibre. Importantly, the entire system was developed indigenously, without imported hardware, which matters as much strategically as it does technically, since a quantum-safe communication system built on foreign components defeats much of its own purpose.

The financial sector has also begun to stir. In May 2026, the Reserve Bank of India set up an eight-member expert committee under its Quantum Secure and Adaptive Financial Ecosystem, or Q-SAFE, initiative, led by Professor Anil Prabhakar of IIT Madras.[16] This committee had representatives from the Department of Science & Technology (DST), State Bank of India (SBI), the National Payments Corporation of India (NPCI), and the Ministry of Electronics and Information Technology (MeitY).[17] The committee has been asked to build a Cryptography Bill of Materials for the financial sector, assess how easily institutions could switch to quantum-safe algorithms, and recommend a roadmap for securing India's financial system, with a report due within six months of its first meeting.[18] Alongside this, the telecom sector's own research arm, Centre for Development of Telematics (C-DOT), has developed quantum key distribution systems, post-quantum cryptography solutions, and quantum-secure video IP phones for government and defence use.[19] On the hardware front, quantum computing itself is advancing in parallel; a Bengaluru startup, QpiAI, released India's first full-stack 25-qubit superconducting quantum computer in April 2025. The Amaravati Quantum Valley, opened in February 2026, houses an IBM Quantum System Two, anchored alongside Tata Consultancy Services and L&T.[20]

The Gap Between the Roadmap and the Reality

For all this activity, the honest picture is of a country that has done the hard work of writing plans but still has an enormous distance to cover in execution. A detailed review of India's Post Quantum Cryptography (PQC) roadmap by the Observer Research Foundation noted that India could still learn from countries like the United States, where NIST has drawn technology vendors into formal cooperative agreements as “Technology Partners,” and that India's own roadmap, while ambitious, needs sharper distinctions between when to use post-quantum cryptography versus quantum key distribution.[21]

The financial sector illustrates the scale of the problem well. Experts have warned of a substantial “readiness gap” in Indian banking, where many institutions still rely on complex legacy systems built on older encryption, and where a lack of coordinated transition could leave smaller banks as weak links in the wider national financial network.[22] UPI alone connects more than 400 banks and payment service providers, meaning migration has to be choreographed carefully since a single participant that fails to upgrade in time creates a vulnerability for the entire network. Public sector banks, in particular, run decades-old core banking systems where simply identifying every place cryptography is used is, in the words of one industry analyst, “archaeological-level work”.[23]

There is also a talent and capacity problem that no policy document can wish away. India's spending on quantum technology, at roughly $0.73 billion, sits several orders of magnitude below China's reported outlay of around $15 billion, and the country's strength has historically been in applying deep technology rather than inventing it at the foundational layer.[24] Building indigenous, field-tested post-quantum systems at the scale UPI and Aadhaar require will need sustained funding, trained cryptographic engineers, and above all, patient follow-through over a decade, the kind of follow-through Indian institutions have not always managed once the initial policy announcement fades from the news cycle.[25]

Finally, there is a question of proportion that Indian planners will have to get right. Migrating everything to post-quantum cryptography at once, regardless of sensitivity,

would be wasteful and slow. As one recent strategic assessment argued, most day-to-day encrypted traffic, such as ordinary payments, routine communications etc., carries limited long-term value to an adversary, while the real risk sits in data that must stay secret for decades.[26] Such data encoded in the forms of strategic defence archives, intelligence records, diplomatic cables, and long-lived identity systems like Aadhaar can impart long-term devastation. Getting the sequencing right, protecting what genuinely needs protecting first without diverting scarce cryptographic talent into low-value migrations, will decide whether India's roadmap becomes a real shield or just another well-written document.[27]

The Bottom Line

Q-Day is not a science fiction scenario anymore, it is a planning horizon, and India has, to its credit, begun planning for it. The National Quantum Mission, the DST's quantum-safe roadmap, DRDO's indigenous Quantum Key Distribution (QKD) trials, and the RBI's Q-SAFE committee together show that the Indian state understands what is coming. What remains is the harder part is turning committee reports and pilot demonstrations into cryptography that actually runs inside Aadhaar servers, UPI switches, and military communication networks before an adversary, real or merely rumoured, gets there first. In a contest where the finish line is invisible and the starting gun has already fired, the nations that treat quantum-safety as an engineering project rather than a talking point will be the ones still standing when Q-Day finally arrives.

Declaration

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

ENDNOTES

[1] Barracuda Networks. "Q-Day Explained: How to Prepare for Post-Quantum Cyber Risk." Barracuda Networks Blog, June 2, 2026. https://blog.barracuda.com/2026/06/02/q-day-explained-post-quantum-cyber-risk.
[2] NIST Computer Security Resource Center. "Post-Quantum Cryptography." Accessed July 2, 2026. https://csrc.nist.gov/projects/post-quantum-cryptography.
[3] Palo Alto Networks. "What Is Q-Day? Quantum Computing and Cyber Risk." Accessed July 2, 2026. https://www.paloaltonetworks.com/cyberpedia/what-is-q-day.
[4] Babbush, Ryan, Adam Zalcman, Craig Gidney, et al. “Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations.” Version 2. Preprint, arXiv, 2026. https://doi.org/10.48550/ARXIV.2603.28846.
[5] Cloudflare. "NIST's First Post-Quantum Standards." Cloudflare Blog, October 24, 2025. https://blog.cloudflare.com/nists-first-post-quantum-standards/.
[6] HSToday. "No, Chinese Did Not Crack RSA with Quantum (Yet)." HSToday, July 2, 2025. https://www.hstoday.us/subject-matter-areas/cybersecurity/no-chinese-did-not-crack-rsa-with-quantum-yet/.
[7] Forbes. "Debunking Hype: China Hasn't Broken Military Encryption with Quantum." Forbes, October 16, 2024. https://www.forbes.com/sites/craigsmith/2024/10/16/department-of-anti-hype-no-china-hasnt-broken-military-encryption-with-quantum-computers/.
[8] Cloudflare. "NIST's First Post-Quantum Standards." Cloudflare Blog, October 24, 2025. https://blog.cloudflare.com/nists-first-post-quantum-standards/.
[9] NIST Computer Security Resource Center. "Post-Quantum Cryptography." Accessed July 2, 2026. https://csrc.nist.gov/projects/post-quantum-cryptography.
[10] The Pioneer. "India's Quantum Push Faces a Problem of Proof." The Pioneer, March 30, 2026. https://dailypioneer.com/news/india-s-quantum-push-faces-a-problem-of-proof.
[11] Newsbytes. "IBM Warns Quantum Computing Could Break Encryption, Endangering Aadhaar, UPI." Newsbytes, May 26, 2026. https://www.newsbytesapp.com/news/science/ibm-warns-quantum-computing-could-break-encryption-endangering-aadhaar-upi/tldr.
[12] Department of Science and Technology, Government of India. "National Quantum Mission (NQM)." Accessed July 2, 2026. https://dst.gov.in/national-quantum-mission-nqm.
[13] DST. Implementation of Quantum Safe Ecosystem in India. Report of the Task Force. Department of Science & Technology (DST), 2026. https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf .
[14] The Quantum Insider. "India Reveals National Plan for Quantum-Safe Security." The Quantum Insider, February 22, 2026. https://thequantuminsider.com/2026/02/09/india-reveals-national-plan-for-quantum-safe-security/.
[15] Evertiq. "DRDO, IIT Delhi Demonstrate Free-Space Quantum Secure Communication over 1 km." Evertiq, June 18, 2025. https://evertiq.com/news/2025-06-18-drdo-iit-delhi-demonstrate-free-space-quantum-secure-communication-over-1-km.
[16] MediaNama. "RBI Forms Q-SAFE Quantum Technology Committee." MediaNama, May 28, 2026. https://www.medianama.com/2026/05/223-rbi-forms-q-safe-quantum-technology-committee/.
[17] Whalesbook. "RBI Assembles Panel to Tackle Quantum Computing Threats to Banking Security." Whalesbook, May 26, 2026. https://www.whalesbook.com/news/English/bankingfinance/RBI-Assembles-Panel-to-Tackle-Quantum-Computing-Threats-to-Banking-Security/6a14e783b979113840cab662.
[18] Ibid

[19] The Geostrata. "India's Post-Quantum Roadmap and the New Geopolitics of Cryptographic Power." Accessed July 2, 2026. https://www.thegeostrata.com/post/india-s-post-quantum-roadmap-and-the-new-geopolitics-of-cryptographic-power.
[20] The Quantum Insider. "India Reveals National Plan for Quantum-Safe Security." The Quantum Insider, February 22, 2026. https://thequantuminsider.com/2026/02/09/india-reveals-national-plan-for-quantum-safe-security/.
[21] Observer Research Foundation. "Quantum Urgency without Panic: Calibrating India's Strategic Posture." ORF Expert Speak, February 24, 2026. https://www.orfonline.org/expert-speak/quantum-urgency-without-panic-calibrating-india-s-strategic-posture
[22] Newsbytes. "RBI Studies Quantum Computing Risks in Banking." Newsbytes, May 25, 2026. https://www.newsbytesapp.com/news/business/rbi-forms-expert-panel-on-quantum-tech-in-banking/story.
[23] NewKerala. "RBI Expert Committee on Quantum Tech Risks in Finance." NewKerala, May 25, 2026. https://www.newkerala.com/news/a/rbi-sets-up-expert-committee-prepare-indian-financial-117.htm.
[24] Dr. Elena Vasquez, Quantum Information Theorist. “India Approves New ₹6,000 Crore Quantum Technology Mission with Focus on Indigenous Hardware.” Article. Quantum Intelligence Network, June 13, 2026. https://quantumintelligencenetwork.com.
[25] The Geostrata. "India's Post-Quantum Roadmap and the New Geopolitics of Cryptographic Power." Accessed July 2, 2026. https://www.thegeostrata.com/post/india-s-post-quantum-roadmap-and-the-new-geopolitics-of-cryptographic-power.
[26] SecurityWeek. "Cyber Insights 2026: Quantum Computing and the Potential Synergy with Advanced AI." SecurityWeek, February 9, 2026. https://www.securityweek.com/cyber-insights-2026-quantum-computing-and-the-potential-synergy-with-advanced-ai/.
[27] World Economic Forum. "Building Security into India's Digital Public Infrastructure." WEF Stories, October 2025. https://www.weforum.org/stories/2025/10/security-by-design-india-digital-public-infrastructure/.