ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

EDITORIAL ANALYSIS

India's Quantum Mission — Technology Sovereignty in the Post-Classical Era

THE HINDU

13 January 2026

SUBJECTS COVERED

SCIENCE & TECH SECURITY & DEFENCE

GS PAPERS

GS3

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator •
linkedin.com/in/epicbharat

ujiyari

India's Quantum Mission — Technology Sovereignty in the Post-Classical Era

The Hindu 13 January 2026 GS3

TH The Hindu | MAINS RELEVANCE: GS Paper 3

INTERVIEW ANGLE

"India approved the National Quantum Mission in 2023. How does quantum computing threaten national security, and is India's response adequate?"

WHY IN NEWS

The National Quantum Mission (NQM) reported early milestones in January 2026 — quantum dot single photon sources demonstrated at TIFR Mumbai and superconducting qubit progress at IISc Bengaluru — as India benchmarks itself against the global quantum race ahead of its 2028 targets.

THE QUANTUM RUPTURE: WHY THIS TECHNOLOGY IS DIFFERENT

Every decade or so, a technology arrives that does not merely improve existing systems but makes entire categories of existing security architecture obsolete. Quantum computing is that technology for the 2030s.

The reason demands precision. The global internet, banking system, diplomatic communications, nuclear command and control, and intelligence architecture are all secured by **public-key cryptography** — specifically RSA and Elliptic Curve Cryptography. These algorithms rest on a mathematical guarantee: factoring the product of two large prime numbers is computationally intractable for any classical computer in reasonable time. A 2,048-bit RSA key would take a classical supercomputer longer than the age of the universe to crack by brute force.

Peter Shor's 1994 algorithm dissolved that guarantee in theory. A quantum computer — using superposition to evaluate all possible factorisations simultaneously, and quantum interference to amplify the correct answer — can factor RSA-2048 in hours, not eons. The US National Institute of Standards and Technology (NIST), which spent eight years evaluating alternatives, standardised four post-quantum cryptographic algorithms in August 2024 precisely because the threat horizon is no longer theoretical. China's quantum hardware programme, the US National Quantum Initiative, and the EU Quantum Flagship are all operating on the assumption that quantum-capable adversaries will exist within 10–15 years.

The strategic implication India must absorb: **a sufficiently powerful quantum computer does not only break future communications — it breaks everything already stored**. The "harvest now, decrypt later" doctrine means adversaries are already archiving encrypted Indian diplomatic cables, defence procurement files, and UIDAI backend communications today, against the day when decryption becomes feasible. India is not building quantum defences for a future threat; it is already behind on protecting the present.

WHAT THE NATIONAL QUANTUM MISSION ACTUALLY DELIVERS

The Union Cabinet approved the NQM on April 19, 2023, under the Department of Science and Technology (DST), with a budget of Rs 6,003 crore over eight years (2023–2031). The mission's architecture is sensible: four specialised Technology Hubs distributed across India's premier research institutions — QSim (IIT Madras), QCom (C-DOT), QSense (IIT Bombay), and QComp (IISc Bengaluru with TIFR Mumbai) — each targeting a distinct quantum domain.

The targets are ambitious on paper. A 50-to-1,000-qubit quantum computer by 2028–2031. Satellite-based Quantum Key Distribution (QKD) by 2028. A 2,000-km ground-based QKD network by 2031. Quantum sensing applications — gravimeters, atomic clocks, medical imaging — by 2026–2028.

Yet three structural problems constrain the mission's delivery.

First: the hardware gap is large and widening. IBM's Condor processor reached 1,121 qubits in December 2023. Google demonstrated quantum supremacy in 2019 with a 72-qubit processor solving a task that would take a classical supercomputer 10,000 years. China's Zuchongzhi exceeded 66 qubits in 2021 and has since advanced further. India's target of 50 qubits by 2028 is not trivially achievable — it requires solving hard engineering problems in cryogenic refrigeration, qubit coherence times, and error correction. The T-Hub architecture distributes effort across institutions, but quantum hardware development requires sustained, concentrated capital investment that India's academic research culture is not historically structured for.

Second: the budget is meaningful but insufficient at scale. Rs 6,003 crore over eight years (~$720 million) compares poorly to China's estimated $15 billion public investment, the US National Quantum Initiative's multi-billion dollar allocation, and the EU Quantum Flagship's €1 billion. More critically, India's quantum budget must cover hardware, software, talent, and communication infrastructure simultaneously. The US and China have specialised quantum hardware companies (IBM, Google, IonQ, Baidu, Origin Quantum) absorbing private capital at scale; India's quantum startup ecosystem is nascent. Government funding cannot substitute for a missing private-sector quantum industry.

Third: the post-quantum cryptography migration is the more urgent problem. Building a quantum computer is a decade-long project. Migrating India's critical infrastructure to quantum-resistant cryptography is a shorter-term, equally urgent task — and it has received less policy attention than the

hardware ambitions. CERT-In, the Department of Telecommunications, the Reserve Bank of India, and UIDAI each govern large encrypted systems. A coordinated national PQC migration roadmap — analogous to NIST's systematic approach — does not yet exist in India at the institutional level required.

WHAT A CREDIBLE QUANTUM STRATEGY REQUIRES

Quantum sensing before quantum computing. India's near-term, deployable quantum advantage is in sensing, not computing. Quantum gravimeters can detect underground structures, submarines, and geophysical anomalies. Quantum-enhanced atomic clocks can provide GPS-independent navigation for military platforms — directly relevant to India's stated goal of NavIC self-reliance. Quantum sensors do not require 1,000-qubit processors; they are achievable with current technology. The NQM's QSense hub at IIT Bombay should be the near-term priority, not the QComp hub's moonshot targets.

QKD deployment for strategic corridors now. China demonstrated intercontinental QKD via its Micius satellite in 2016 — linking Beijing to Vienna with quantum-secured communication. India's satellite QKD target is 2028. The window to deploy intra-city QKD networks — Delhi to Mumbai to Bengaluru — using existing fibre infrastructure and mature QKD hardware (now commercially available from European and Japanese vendors) is open today. The NQM's C-DOT-led QCom hub should prioritise deployment over further research on already-solved QKD protocols. Nuclear command links, cabinet-level communications, and DRDO's classified networks are the priority corridors.

A national PQC transition authority. India needs a body — notionally the National Cyber Security Coordinator's office, with DST and CERT-In as technical arms — empowered to mandate and timeline PQC migration across all government and critical infrastructure systems. The four NIST-standardised algorithms (CRYSTALS-Kyber for key encapsulation, CRYSTALS-Dilithium for digital signatures, FALCON, and SPHINCS+) provide the technical basis. The gap is institutional authority and a binding migration schedule. Without this, banks, UIDAI, defence ministries, and state governments will each proceed at their own pace — or not at all.

Quad science partnerships for hardware. India cannot build the global quantum supply chain alone. The iCET (Initiative on Critical and Emerging Technologies) framework with the United States, and similar technology cooperation tracks with Japan and Australia under the Quad Science and Technology Working Group, provide pathways for joint quantum hardware research, talent exchange, and access to advanced cryogenic and photonic components that India does not currently manufacture. Strategic technology sovereignty does not mean technological autarky — it means assured access and the ability to absorb, adapt, and ultimately produce indigenously.

THE DEEPER QUESTION: TECHNOLOGICAL SOVEREIGNTY

India's quantum ambition is inseparable from a broader question about what technological sovereignty means for a middle power in the 2030s. The naive answer is domestic production of everything. The realistic answer is different: strategic independence requires the ability to produce, access, or deny adversaries access to the technologies that determine military and economic outcomes.

Quantum technology is now on that list. The NQM is India's acknowledgment of this fact. The mission's design — distributed T-Hubs, long timeline, ambitious targets — reflects genuine seriousness. But seriousness in framing does not automatically become competence in execution. India's semiconductor mission, launched with similar urgency, took three years to produce its first factory commitment. Quantum computing's hardware challenges are, if anything, harder.

The January 2026 milestones — photon sources at TIFR, superconducting qubits at IISc — are genuine scientific achievements by India's research community. They are also the beginning of a very long road. Whether the NQM becomes India's quantum inflection point or another well-intentioned mission that falls short of its hardware ambitions will depend on institutional continuity, private capital mobilisation, and the willingness to treat post-quantum cryptography migration — the defensive task — with the same urgency as the quantum computing offensive ambition.

The cryptographic clock does not wait for hardware readiness.

📌 FACTS CORNER — KNOWLEDGEPEDIA

NATIONAL QUANTUM MISSION (NQM):

Approved: April 19, 2023, Union Cabinet

Budget: Rs 6,003 crore over 8 years (2023–2031)

Nodal Ministry: Department of Science and Technology (DST)

Oversight: Principal Scientific Adviser (PSA) to Government of India

FOUR TECHNOLOGY HUBS:

QSim Hub: IIT Madras — quantum simulation and materials

QCom Hub: C-DOT (Centre for Development of Telematics) — Quantum Key Distribution

QSense Hub: IIT Bombay — quantum sensing and metrology

QComp Hub: IISc Bengaluru + TIFR Mumbai — quantum computing hardware

NQM TARGETS:

50-qubit quantum computer prototype: 2028

1,000-qubit quantum computer: 2031

Satellite-based QKD: 2028

Ground QKD network 2,000 km: 2031

Quantum sensing (atomic clocks, gravimeters): 2026–2028

GLOBAL QUANTUM LANDSCAPE:

US: IBM Condor (1,121 qubits, Dec 2023); National Quantum Initiative (~$1.2 billion, 2018)

China: ~$15 billion public investment; Micius QKD satellite (2016); Zuchongzhi 66+ qubits (2021)

EU: Quantum Flagship programme (€1 billion, 2018–2028)

India: ~$720 million (NQM); 50-qubit target 2028

CRYPTOGRAPHY CONTEXT:

RSA-2048: current global encryption standard for banking, diplomacy, defence

Shor's algorithm: quantum algorithm that factors large numbers exponentially faster than classical computers — breaks RSA

"Harvest now, decrypt later": adversaries archive encrypted data today; decrypt when quantum computers mature

NIST PQC standards (August 2024): CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+

QKD (QUANTUM KEY DISTRIBUTION):

Uses quantum properties of photons to share cryptographic keys

Quantum no-cloning theorem: any eavesdropping disturbs quantum state — immediately detectable

China's Micius satellite: demonstrated intercontinental QKD (Beijing–Vienna) in 2017

India's C-DOT: nodal agency for QKD network development under NQM

OTHER RELEVANT FACTS:

iCET: India-US Initiative on Critical and Emerging Technologies (2023) — covers quantum, AI, semiconductors, space

Quad Science & Technology Working Group: India-US-Japan-Australia quantum cooperation

CERT-In: Indian Computer Emergency Response Team — cybersecurity nodal body

> NavIC (Navigation with Indian Constellation): India's regional satellite navigation system — 7 satellites; quantum atomic clocks would enhance its precision and independence

Sources: DST, The Hindu, PIB

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Published on **ujiyari.com** · Free UPSC & State PCS Current Affairs