



UPSC &amp; STATE PCS CURRENT AFFAIRS · UJIYARI.COM

**DAILY CURRENT AFFAIRS**

# National Quantum Mission – India's Bet on Quantum Technology

13 January 2026

SUBJECTS COVERED

SCIENCE &amp; TECH

ECONOMY

CURATED &amp; WRITTEN BY

**Bharat Choudhary**

UPSC Educator &amp; Content Creator •

[linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)

Free UPSC &amp; State PCS Resources

[ujiyari.com](http://ujiyari.com)

# National Quantum Mission — India's Bet on Quantum Technology

13 January 2026

## WHY IN NEWS

India's National Quantum Mission (NQM), launched in April 2023 with Rs 6,003 crore, reported early milestones in January 2026: quantum dot single photon sources demonstrated at TIFR Mumbai and superconducting qubit progress at IISc Bengaluru — as India works toward its target of a 50-qubit quantum computer prototype by 2028 and positions itself in the global race for quantum supremacy.

## WHAT IS QUANTUM COMPUTING?

**Quantum computing** leverages the principles of quantum mechanics — superposition, entanglement, and quantum interference — to process information in ways that classical computers fundamentally cannot.

### Classical vs Quantum computing:

Feature	Classical Computer	Quantum Computer
Basic unit	Bit (0 or 1)	<b>Qubit</b> (can be 0, 1, or both simultaneously — superposition)
Operations	Sequential logic gates	Quantum gates; parallel computation through superposition
Entanglement	Not used	Two qubits can be <b>entangled</b> — measuring one instantly affects the other
Interference	Not applicable	Quantum interference amplifies correct answers, cancels wrong ones
Best use cases	General computing; word processing; web	Cryptography cracking; drug discovery; optimisation; materials simulation

### Qubit systems currently available:

**IBM Quantum:** 127-qubit Eagle processor (2021); 433-qubit Osprey (2022); 1,000-qubit Condor (2023)

**Google:** 72-qubit Bristlecone; demonstrated quantum supremacy (2019, 200-second task that would take classical supercomputer 10,000 years)

**China:** 66-qubit Zuchongzhi processor (2021); 100+ qubit systems

**India's target:** 50-qubit by 2028; 1,000-qubit by 2031

## NATIONAL QUANTUM MISSION (NQM) — ARCHITECTURE

**Launched:** April 19, 2023, by the Union Cabinet **Ministry:** Department of Science and Technology (DST), Ministry of Science and Technology **Budget:** Rs 6,003 crore over 8 years (2023–2031) **Nodal body:** Office of the Principal Scientific Adviser (PSA) to the Government of India

### Four Technology Hubs (T-Hubs)

NQM establishes four specialised technology hubs at premier research institutions:

Hub	Host Institution	Focus
<b>QSim Hub</b>	IIT Madras	Quantum simulation; quantum materials
<b>QCom Hub</b>	C-DOT (Centre for Development of Telematics)	Quantum communication; QKD networks
<b>QSense Hub</b>	IIT Bombay	Quantum sensing; quantum metrology
<b>QComp Hub</b>	IISc Bengaluru + TIFR Mumbai	Quantum computing hardware

### Key Targets Under NQM

Milestone	Timeline
50–1,000 qubit physical quantum computer	2028–2031
Quantum Key Distribution (QKD) satellite links	2028
Ground-based QKD over 2,000 km	2031
Quantum sensing for geodesy, healthcare, navigation	2026–2028
Atomically precise manufacturing using quantum dots	2028

## WHY QUANTUM TECHNOLOGY MATTERS STRATEGICALLY

### Quantum Computing and Cryptography

The most immediate strategic threat of quantum computing is **breaking public-key cryptography**. The RSA and ECC (Elliptic Curve Cryptography) encryption algorithms that protect banking, government communications, and military networks are based on the mathematical difficulty of factoring large numbers — a task that a sufficiently powerful quantum computer can perform using **Shor's algorithm**.

A quantum computer with ~4,000 error-corrected qubits could crack RSA-2048 encryption — the gold standard today

This would render all current encrypted communications retroactively readable (adversaries can store encrypted data now and decrypt later — **“harvest now, decrypt later” threat**)

India’s banking system, UIDAI/Aadhaar databases, defence communication networks, and nuclear command infrastructure all rely on current cryptographic standards

**Post-quantum cryptography (PQC):** The US NIST standardised 4 post-quantum cryptographic algorithms in 2024. India’s DoT, CERT-In, and DST are working on a roadmap for migrating India’s critical infrastructure to PQC standards.

## Quantum Communication — Quantum Key Distribution (QKD)

**QKD** (Quantum Key Distribution) uses the quantum properties of photons to create cryptographic keys that are physically impossible to intercept without being detected. Any eavesdropper disturbs the quantum state — alerting both parties.

India’s NQM targets:

**Intra-city QKD** networks in major metros (Phase I — 2026)

**Inter-city QKD** links (Delhi-Mumbai-Bengaluru — 2028)

**Satellite-based QKD** (quantum communication satellite — 2028)

**Strategic use:** QKD can protect communications between India’s nuclear command and control infrastructure, diplomatic channels, and defence operations centres — creating **“unhackable” communication links**.

## Quantum Sensing

Quantum sensors exploit quantum effects to measure physical quantities — gravity, time, electromagnetic fields — with extreme precision:

**Atomic clocks** accurate to  $10^{-18}$  seconds — enabling GPS-independent navigation

**Quantum gravimeters** that can detect submarines, underground tunnels, or oil reservoirs

**Medical imaging** using nitrogen-vacancy centres in diamonds (quantum MRI)

**Navigation without GPS** — critical for India’s military platforms in GPS-denied environments

## INDIA’S POSITION IN THE GLOBAL QUANTUM RACE

**US:** Quantum computing leadership (IBM, Google, Honeywell); NIST PQC standards; National Quantum Initiative (\$1.2 billion, 2018) **China:** Largest government investment (~\$15 billion); demonstrated satellite QKD (Micius satellite, 2016); aggressive qubit development **EU:** Quantum Flagship programme (€1 billion,

2018–2028) **India (NQM):** Rs 6,003 crore (~\$720 million) — a meaningful investment, though lower than US/China. However, India has strong fundamentals: AMU (Aligarh Muslim University) quantum group, IISc, TIFR, and IIT-Madras have produced world-class quantum research.

**The advantage gap:** India is 5–7 years behind US and China in quantum hardware. The NQM’s goal is to close this gap through focused investment, international collaboration (particularly with the EU, Japan, and Australia under Quad science partnerships), and leveraging India’s large pool of physics and engineering talent.

## UPSC RELEVANCE

### Prelims:

NQM: launch April 19, 2023; DST; Rs 6,003 crore; 8 years (2023-2031)

Targets: 50-qubit (2028); 1,000-qubit (2031); satellite QKD (2028); 2,000 km ground QKD (2031)

Four T-Hubs: QSim (IIT Madras), QCom (C-DOT), QSense (IIT Bombay), QComp (IISc/TIFR)

Qubit: quantum bit; can exist in superposition (0, 1, or both)

Shor’s algorithm: quantum algorithm that can break RSA/ECC encryption

QKD: Quantum Key Distribution; eavesdropping-proof; uses quantum photon properties

Post-quantum cryptography (PQC): NIST standardised 4 algorithms (2024); India migrating

**Mains GS-3:** National Quantum Mission — strategic rationale; quantum computing threats to cryptography; harvest-now-decrypt-later; QKD for national security; India’s position in quantum technology race.

## ★ FACTS CORNER — KNOWLEDGEPEDIA

### NATIONAL QUANTUM MISSION (NQM):

Launch: April 19, 2023; Cabinet approval

Budget: Rs 6,003 crore; 2023-2031 (8 years)

Ministry: Department of Science and Technology (DST)

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

Four T-Hubs: QSim at IIT Madras; QCom at C-DOT; QSense at IIT Bombay; QComp at IISc+TIFR

### QUANTUM TARGETS:

50-qubit quantum computer: 2028

1,000-qubit quantum computer: 2031

Satellite-based QKD: 2028

2,000 km ground QKD network: 2031

### QUANTUM COMPUTING BASICS:

Qubit: quantum bit; superposition (0, 1, or both)

Entanglement: qubits correlated regardless of distance

Quantum supremacy: task impossible for classical computer in reasonable time

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

### GLOBAL LEADERS:

IBM: Eagle (127 qubit, 2021), Condor (1,000+ qubit, 2023)

Google: quantum supremacy demonstration 2019 (72-qubit Sycamore)

China: Micius QKD satellite (2016); Zuchongzhi (66 qubit, 2021)

India: 50-qubit target 2028; NQM Rs 6,003 crore

### CRYPTOGRAPHY CONTEXT:

RSA-2048: current encryption standard; secure against classical computers

Post-quantum cryptography (PQC): NIST standardised 4 algorithms in 2024

“Harvest now, decrypt later”: adversaries store encrypted data now to decrypt once quantum computers are powerful enough

### OTHER RELEVANT FACTS:

C-DOT: Centre for Development of Telematics; under DoT; national telecom R&D institution

Quad science cooperation: India-US-Australia-Japan; quantum, semiconductors, AI

Critical and Emerging Technologies (iCET): India-US framework (2023) covering quantum, AI, semiconductors, space

Sources: DST, PIB, The Hindu

---

CURATED & WRITTEN BY

# Bharat Choudhary

UPSC Educator & Content Creator

 [linkedin.com/in/epicbharat](https://www.linkedin.com/in/epicbharat)

---

Published on [ujiyari.com](http://ujiyari.com) · Free UPSC & State PCS Current Affairs