Q→NU

Defence & Aerospace Quantum Threat Intelligence Report | August 2025

Global Quantum Preparedness and Landscape

- **$40B** is committed to quantum tech globally for military & strategic systems. (Source: Deloitte Insights)
- **50%** of federal US IT leaders are moving to post-quantum cryptography. (Source: Quantum Zeitgeist)
- Quantum computers can efficiently factor large numbers using algorithms such as Shor's, threatening conventional encryption systems like RSA and ECC that currently protect sensitive data and military communications.
- SIPRI highlights that technological advances in quantum and AI are reshaping deterrence, cyber capabilities, and increasing the risk of miscalculation or escalation in military affairs.
- A collaborative approach involving government, CERT-In (the national computer emergency response team), and security firms like SISA is essential for upgrading systems and ensuring quantum cyber readiness.
- India's Ministry of Defence recognises the national security risk posed by quantum-enabled attacks and is proactively investing in quantum key technologies and post-quantum cryptography for protection.
- Initiatives like the quantum-secure satellite project and strategic roadmaps are specifically designed to harden space infrastructure and digital assets against future quantum threats, ensuring sovereignty and mission integrity.

Global Quantum Landscape

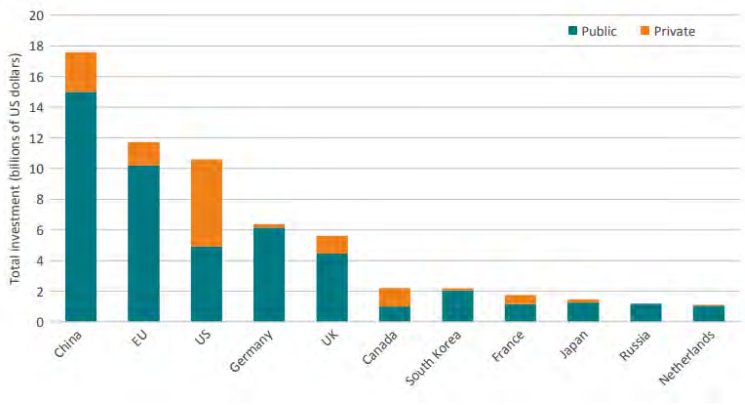
- **NATO**
  Focusing on Quantum as a strategic defence.
- **US**
  NSA and CISA mandated PQC adoption timelines.
- **UK NCSC**
  A clear migration roadmap has been established. Early adopters are from the defence sector.
- **China**
  Invested billions into quantum research and demonstrated intercontinental QKD.
- **Russia**
  The country is developing home-built PQC research with a special focus on secure communications for military operations.

- **Australia**
  ASD advised post-quantum planning from 2023.

- **EU**
  Building EuroQCI (Quantum Communication Infrastructure) as a multi-nation secure backbone.

- **India**
  NQM has been set up to drive self-reliance in Defence by India in alignment with Atmanirbharta. With National Quantum Mission (NQM) funding, entanglement trials, showcasing 500 Km longest QKD, and now building 2000 Km longest QKD networks and quantum satellite experiments.

- Global public investments in quantum technology have already surpassed $40 billion.



Source: ECIPE

- It is shown that India is not among the top 10 investors. However, with a strong foundation in government initiatives such as Startup India, Digital India, Atal Innovation Mission, Make in India, and NQM, India's quantum efforts are promising and well-received globally.

Why It's Important Now?

- **Harvest Now, Decrypt Later (HNDL)**
  Cyber adversaries have already begun their attack using HNDL strategies: collecting encrypted data today, with the expectation that it can be decrypted in the future when sufficiently powerful quantum computers become available. So, the data classified as secret today could be catastrophically exposed a decade from now.

- 1-in-7 Chance that public-key crypto will be broken by 2026.

- 1-in-2 Chance that it will be broken by 2031 by quantum computers. (Source: Ultimaco)

- **Migration Timeline**
  Quantum migration will also take considerable time and resources anywhere between 2 to 10 years.

- **Long lifecycle of military systems**
  Unlike commercial IT systems, which typically refresh every 3 to 5 years, defence platforms often remain in service for 20 to 30 years. An operational military system deployed today will likely remain operational when quantum computers mature.

- **Global peers are moving fast**
  NATO, the US DoD, China, and the EU are embedding quantum security into defence architectures. India and other countries must move in parallel to avoid a strategic disadvantage.

- **SIPRI has identified 162 states as recipients of major arms in 2020–24.** The five largest arms recipients were **Ukraine, India, Qatar, Saudi Arabia and Pakistan.**
- **SIPRI and Indian government reports urge early adoption of quantum-resistant algorithms to mitigate systemic vulnerabilities before quantum computers become mainstream and can break current encryption standards.**

Recent Quantum Tech Innovation and Preparedness Across India

Indian Army Terrier Cyber Quest 2025 focused on emerging technologies like AI, ML, Quantum and predictive threat intelligence.

Recent innovations from IIT Delhi + DRDO demonstrated entanglement-based free space QKD of 1 KM, meaning without fibre optic cables, achieving a secure key rate of nearly 240 bits per second and a Quantum Bit Error Rate (QBER) below 7%.

Military-Specific Vulnerabilities

- **Communication Systems**
  Secure military communications using current encryption
- **Weapons Systems**
  C4ISR networks controlling defense operations
- **Intelligence Data**
  Classified information repositories and databases
- **Satellite Communications**
  ISRO and defence satellite networks
- **Border Security**
  Surveillance and reconnaissance system data integrity

Business Impact

- **National Defence**
  Military readiness compromised by quantum-vulnerable communications
- **Strategic Secrets**
  Defence research and weapons development data exposed
- **Allied Relations**
  Information sharing with international partners at risk
- **Defence Exports**
  ₹76,000 crore defence export target threatened without quantum security

Timeline Urgency

- **Quantum Arms Race**
  Major powers accelerating military quantum capabilities
- **Border Security**
  Immediate need for quantum-safe communication with China/Pakistan tensions
- **Defense Indigenisation**
  Atmanirbhar defence requiring quantum-secure supply chains

Key Statistics

- **₹5.25 trillion** defence budget with 70% systems quantum-vulnerable
- **23 defence PSUs** requiring immediate quantum security upgrades
- **156** critical defence installations needing quantum-safe communications

Immediate Actions Required

- **Military Communications**
  Upgrade C4ISR systems with quantum-safe protocols
- **Intelligence Protection**
  Secure classified data repositories immediately
- **R&D Collaboration**
  Expand DRDO-IIT quantum security research partnerships
- **Allied Coordination**
  Develop quantum-safe information sharing protocols

Sources

- Indian Army Terrier Cyber Quest 2025 Documentation
- DRDO-IIT Delhi Quantum Communication Research (Drishti IAS)
- Global Security Defence Technology Reports
- Centre for International Governance Innovation Quantum Defence Analysis

Q→NU
Proactively™
Quantum

Tomorrow's Quantum Security, Today.

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary Building, 2nd Floor, East Wing, #28 MG Road Bengaluru - 560025

CIN: U72900KA2016PTC096629

India USA Australia Global