PRIMUS PARTNERS®

Published in Tech Circle
December 22, 2025

Building a Quantum Safe India: An Idea where action is needed Now

Authored by Devroop Dhar

Read on: https://www.techcircle.in/2025/12/22/building-a-quantum-safe-india-an-idea-where-action-is-needed-now/

Article Content:

The buzz around Quantum Computing has been growing steadily over the years. Many experts are of the view that Y2Q (Years to Quantum) is just around the corner, probably within the next 5 years or so. Which means, very soon, there would be quantum computers that can run algorithms to break even the most complex public key encryptions that safeguard critical systems today. Infact, the Harvest Now Decrypt Later (HNDL) threat becomes even more severe with the impending Y2Q.

While countries like the USA and China have been leading the quantum race, India has also joined the move with the launch of the National Quantum Mission (NQM), which aims at investing USD 1 billion into Quantum Computing in India. States such as Andhra Pradesh and Karnataka have followed suit and are taking a lead in developing the Quantum computing ecosystem in India. While the quantum computing industry is expected to be more than $100 billion within the next decade, its importance is much

beyond the economic value. Quantum computing would play a key role in defining the sovereignty of nations, with countries investing in quantum being in a much better position to safeguard their critical assets and systems from getting compromised.

Today, critical systems such as defence, communications, energy, and banking are all secured through encryption, which can't be easily compromised even by brute force. However, with algorithms being run on quantum computers in the future, it may be possible to decrypt such data at a later date, unless it is secured before that. Therefore, as a country, India needs to budget for and plan to implement Post Quantum Cryptography (PQC) solutions across all critical systems.

The National Quantum Mission, along with the State Governments, need to focus on the implementation of PQC solutions over the next 3-4 years. While SEBI has taken a lead by announcing that its regulated entities would be adopting Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) solutions by 2028-2029, other organizations within the Government needs to follow. Countries such as Singapore have already laid out their plan and roadmap, and India needs to fast track the same as well.

Transitioning to Quantum Safe India would need a dedicated effort, much like the Y2K initiative across the globe to safeguard IT systems at the turn of the century. All Government organizations and critical sectors such as defence, aerospace, banking, financial services, healthcare need to move into a Quantum Safe environment within the next 3 years. Organizations can adopt a 3-step approach. Step 1 being to assess and prepare a cryptography inventory, identify gaps and gauge quantum readiness. Step 2 would involve implementation of quantum overlay solutions to safeguard critical data without the need for full scale system migration. Step 3 would involve the most critical stage wherein PQC solutions can be embedded into firmware, software and hardware.

Budget 2026 can be an opportunity for Government of India to lay clear directions and roadmap for Quantum Safe India. It would need Government support and public private partnership to take India on this journey. Start-ups and private sector companies may be encouraged to design and develop an Indian solution to cater to the need of the country. The Budget should clearly lay the timeline for achieving Quantum Safe India and drive it in a mission-mode. After all, it is for the safety, security and sovereignty of the country.