सत्यमेव जयते

NITI Aayog

NITI Frontier Tech Hub

FUTURE FRONT:

QUARTERLY FRONTIER TECH INSIGHTS

March 2025

The Only Way to Predict the Future is to Create it...

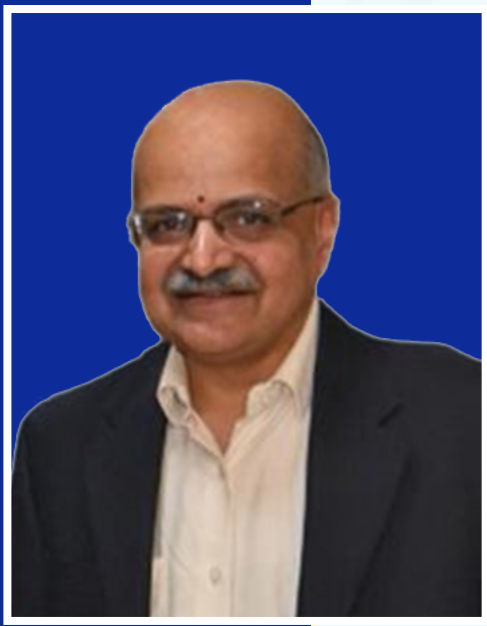
Issue-2

Quantum Computing:
National SecurityImplications & Strategic Preparedness

Knowledge Partner:
Data Security Council of India

PROMOTING DATA PROTECTION

Foreword



Our future success hinges on our ability to proactively harness transformative technologies for inclusive economic growth and national security. Among these, quantum computing stands as a revolutionary force—one that has the potential to fundamentally reshape problem-solving, cryptography, and strategic decision-making. As nations worldwide race to establish supremacy in this domain, India must not only participate in this revolution but take the lead—driving innovation, setting global standards, and ensuring our security in an increasingly complex geopolitical landscape.

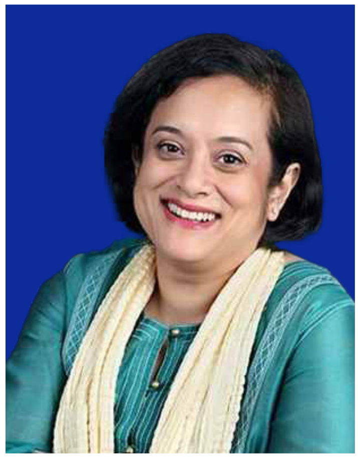
In this edition of NITI Frontier Tech Hub's Quarterly Insight, *Future Front®*, we explore the profound implications of quantum computing on national security and our collective mission to build an *Atmanirbhar Bharat*. Quantum technologies will play a defining role in securing critical infrastructure, strengthening defense capabilities, and safeguarding our digital sovereignty. However, leadership in this domain will require more than technological prowess—it demands a bold vision, strong policy frameworks, and an ecosystem that fosters cutting-edge research, talent development, and large-scale deployment.

By forging deep collaboration between government, industry, and academia, and by investing in indigenous capabilities, we can unlock the true potential of quantum computing and build a future that is secure, resilient, and inclusive for all.

Let us seize this opportunity with determination and foresight to shape the future of quantum technologies for both national security and global progress.

BVR Subrahmanyam
CEO, NITI Aayog

Quantum computing is becoming real much faster than we think—not in decades, but in years. Breakthroughs like Google's Willow and Microsoft's Majorana-1 prove that scalable quantum systems are on the horizon. This is not a distant future; it is unfolding now, and India must act today to stay ahead.



Quantum computing will redefine AI, cryptography, and national security, bringing both transformative opportunities and critical risks. As quantum capabilities accelerate, they challenge existing security frameworks while unlocking powerful new defense strategies. Nations that prepare today will shape the future; those that don't risk falling behind.

At the NITI Frontier Tech Hub, our mission is to position India as a Frontier Tech Nation. We actively engage with experts to build deep insights and accelerate India's readiness in emerging technologies—fostering innovation, driving adoption, and ensuring economic and societal progress.

We are proud to collaborate with the Data Security Council of India (DSCI) to present the second edition of Future Front, our Quarterly Frontier Tech Insights. This edition explores the profound implications of quantum computing on national security and resilience—providing strategic perspectives to help India navigate and lead in this transformative era.

Debjani Ghosh
Distinguished Fellow, NITI Aayog;
Chief Architect, NITI Frontier Tech Hub

Quantum computing technology ecosystem is now industrial in nature, and the supply chain is building formidably. Quantum technologies are already demonstrating practical benefits in fields such as optimization, materials science, and cryptography. The confidence in quantum technologies can be witnessed in the increasing private investment in the area. Although some doubts still persist, the acceleration of quantum technology, especially promising million-qubits, would have profound impact on national security. While cyber security preparedness needs urgent national response, the geopolitics associated with quantum advancements, their possible role in intelligence gathering and processing, and their potential to transform military preparedness demands holistic national security understanding. Data Security Council of India is glad to partner with NITI Frontier Tech Hub in this effort.

Vinayak Godse
CEO, Data Security Council of India

NITI FRONTIER TECH HUB INSIGHTS

Quantum computing is evolving rapidly, posing both opportunities and challenges for national security. This paper explores the global quantum race, latest technological breakthroughs and the potential impact on National Security. It also provides recommendations for enhancing India's preparedness.

While there are ongoing scepticisms about the exact timeline for cryptographically relevant quantum computers (CRQCs), it is essential to recognize the significant forces accelerating their development. Recent breakthroughs challenge our previous assumptions, making it imperative to reassess our expectations. The profound implications of CRQCs—particularly for national security—demand our attention.

Tangible progress is being made in areas that were once considered formidable roadblocks. Qubit coherence and control are advancing, error mitigation and correction techniques are becoming more robust, and novel quantum algorithms are emerging. Researchers are also making strides across multiple qubit modalities, expanding the possibilities for scalable quantum computing.

These advancements are not occurring in isolation. A mature ecosystem and supply chains are rapidly taking shape, supported by increasing public and private investments. This convergence—of technological breakthroughs and ecosystem maturation—suggests that the timeline for achieving fault-tolerant, cryptographically relevant quantum computers may be shorter than previously anticipated.

In the 2nd NITI Frontier Tech Hub Insights, we explore the intersection of quantum technology breakthroughs, the shifting landscape of quantum geopolitics, and their far-reaching implications for national security.

QUANTUM TECHNOLOGY: ADVANCEMENTS AND BREAKTHROUGH

1. **Longer Qubit Coherence - Core Component for Quantum Stability**: Qubits are the fundamental building blocks of quantum computers, and their stability is crucial for harnessing quantum states for computation. One of the primary challenges in quantum computing has been qubit coherence—the duration for which qubits can maintain their delicate quantum state before decoherence sets in. Achieving longer qubit coherence is a critical milestone in making quantum computers more robust, scalable, and capable of solving complex problems.

   Recent advancements by **Atom Computing** and **ColdQuanta** have demonstrated significantly longer coherence times using innovative **neutral atom qubit architectures**. These breakthroughs mark a crucial step forward, as extended coherence enables more sophisticated quantum circuits, enhancing computational potential and bringing us closer to practical, fault-tolerant quantum computing.

2. **Enhanced Qubit Control and Fidelity – Enabling More Accurate Operations**: Beyond qubit stability, precise control over qubits is essential for minimizing errors and ensuring reliable quantum computations. Higher fidelity in qubit operations means that the actual

quantum state closely aligns with the intended target state, reducing computational noise and increasing accuracy. Since quantum gates serve as the fundamental building blocks of quantum operations, improving their fidelity directly enhances the overall performance and dependability of quantum computers.

Recent advancements highlight significant progress in this area. IBM continues to refine superconducting qubit technology, while Quantinuum has demonstrated exceptionally high-fidelity gate operations using trapped-ion qubits. These breakthroughs allow quantum computers to be programmed with greater accuracy and confidence, making them more reliable for tackling complex real-world problems.

3. **Error Correction Progress – Paving the way towards Fault-Tolerant Quantum Computing:** Qubits are inherently susceptible to noise and errors. Error correction is essential for building machines capable of complex, reliable computation. Compelling breakthroughs in this vital area were witnessed in the recent past.

   Google's Willow Chip: One of the most notable advancements comes from Google's Quantum chip named Willow. Designed to explore and demonstrate hardware-based error correction techniques, Willow enables multiple physical qubits to work together to store a single unit of quantum information, creating a built-in self-checking mechanism that detects and corrects errors in real time. This redundancy improves computational stability and is a key enabler of fault-tolerant quantum computing. Google has projected that, theoretically, quantum computers could one day shrink 100-million-year problems down to mere minutes—a transformative leap with profound implications for fields such as cryptography and materials science.

   Global Efforts in Quantum Error Correction (QEC): Beyond Google, diverse institutions are tackling the error correction challenge from multiple angles:

   i. **Hardware Innovations:**

      - IBM & UCSB – Focused on implementing and experimentally validating surface codes, a leading QEC technique.
      - PsiQuantum – A startup pursuing a scalable, photonics-based approach to fault-tolerant quantum computing.
      - Microsoft – Building Majorana 1 is the world's first Quantum Processing Unit (QPU) powered by a Topological Core to make it more fault-tolerant.
      - Atom Computing – Uses neutral atoms, which are atoms without an electrical charge, as qubits. They are preparing second-generation systems with over 1,000 qubits for commercial introduction as Quantum Computing as a service.

   ii. **Theoretical and Algorithmic Research:**

      - ETH Zurich & University of Toronto – Advancing the mathematical foundations and algorithmic strategies for robust QEC.
      - USTC & Zhejiang University (China) – Contributing significantly to both experimental and theoretical breakthroughs in QEC.

As these global efforts continue to push the boundaries of error correction, the vision of fault-tolerant quantum computing is moving from theory to reality. These advances will enable quantum computers to tackle high-impact problems, from breaking current encryption standards to designing revolutionary new materials and accelerating scientific discovery.

3. **Diversity of Qubit Modalities – A "Multi-Horse Race":** Quantum computing is not a one-size-fits-all technology. Instead, it is evolving as a multi-horse race, with multiple competing qubit modalities being actively pursued worldwide. The leading contenders include superconducting circuits, trapped ions, photonic systems, neutral atoms, silicon spin qubits, and topological qubits.

   This diversity fosters a dynamic ecosystem where breakthroughs in one modality often benefit others, accelerating overall progress in the field. While the suitability of a qubit type depends on the specific application, having multiple viable approaches reduces dependency on any single technology or player, increasing resilience and innovation in the quantum landscape.

4. **Continued Pursuit of Topological Qubits – A Potential Game Changer:** Topological qubits have the potential to revolutionize quantum computing by achieving fault tolerance at the hardware level. Unlike conventional qubits, which rely on individual particles like ions, electrons, or photons, topological qubits encode information within a topological state or phase of matter. This makes them inherently more stable and resistant to errors, significantly reducing the need for complex error correction mechanisms.

   Although still in the early stages of development, any significant breakthrough in topological qubits could be transformative. By fundamentally simplifying error correction, they could leapfrog existing quantum computing approaches, accelerating the path to scalable, fault-tolerant systems faster than previously anticipated.

   In this context, topology refers to a branch of mathematics dealing with properties that remain unchanged under continuous deformations, such as stretching or twisting. This principle enables topological qubits to store information in a way that is inherently protected from external disturbances—unlike traditional qubits, which are highly sensitive to environmental noise and decoherence.

   Topological qubits are envisioned to rely on exotic quasiparticles known as Majorana Zero Modes (MZMs)—which are their own antiparticles and can exist at the ends of specially engineered nanowires. Quantum information is stored across pairs of these MZMs, making it more robust against errors. Indium arsenide nanowires coated with aluminium are commonly used as topoconductors to facilitate this process.

   A key feature of MZMs is their braiding property, where the movement of these quasiparticles around each other encodes quantum information. Unlike conventional logical qubits—where maintaining stability requires hundreds or even thousands of physical qubits—topological qubit technology could drastically reduce this requirement, making large-scale quantum computing more feasible.

   Microsoft's recent announcement of Majorana-1, an eight-qubit system, provides strong evidence of MZMs, a topological energy gap, and improved qubit coherence times. However, some scientists remain cautious, emphasizing the need for robust validation of braiding operations before declaring definitive success.

The combination of nanowire-based architecture, braiding operations immune to timing and positioning errors, and semiconductor materials like indium arsenide and aluminium could pave the way for scaling topological qubits to millions of qubits. Recognizing its potential, DARPA has selected Microsoft's topological qubit approach as one of two key methods for developing an industrially viable quantum computer.

5. **Software and Algorithmic Innovation – Unlocking Quantum Potential:** Advancements in software and algorithmic innovation are essential for efficiently harnessing quantum power, transforming raw hardware potential into practical capabilities. Companies and institutions are making significant strides in optimizing quantum circuits and enhancing computational efficiency. IBM is refining quantum circuits to run faster with fewer quantum gates, ensuring useful results before decoherence disrupts computations. Oxford University is focused on reducing 'gate counts' in algorithms, simplifying quantum programs and minimizing errors. Microsoft is pushing the boundaries of fault-tolerant quantum computing through concatenated codes and improved protocols to create robust logical qubits from noisy physical ones. Additionally, Quantum Machine Learning (QML), Quantum Simulation for applications like drug discovery, and Quantum Optimization are expanding the possibilities of quantum computing. The field is also witnessing rapid advancements in programming languages and compilers, with growing expertise in high-level quantum programming languages such as Q#, Cirq, Qiskit, and PennyLane. These innovations collectively drive the efficient application of quantum computing, bringing us closer to unlocking its full potential.

MATURING TECHNOLOGY ECOSYSTEM AND SUPPLY CHAIN

The evolution of a robust technology ecosystem and supply chain is critical for transforming lab-based quantum breakthroughs into real-world, scalable systems. Recent developments indicate significant progress in this direction, with key advancements across supporting industries, specialized materials, manufacturing capabilities, and workforce development.

- **Emergence of Specialized Component Suppliers**

  Companies are increasingly focusing on producing ultra-high purity materials, cryogenic systems, specialized lasers, and control electronics tailored for quantum computing. Notable players in this space include Quantum Silicon, Materion, Sigma-Aldrich, American Elements, Kyocera, Oxford Instruments, Bluefors, Cryoconcept, Sumitomo Heavy Industries, Cryomech, Samtec, Lake Shore Cryotronics, Toptica Photonics, NKT Photonics, Zurich Instruments, Tektronix, and Quinstar Technology.

- **Dedicated Quantum Foundries and Manufacturing Efforts**

  While still in the early stages, there is a growing push to establish specialized fabrication facilities capable of manufacturing complex quantum chips and components. Leading efforts in this space include Seeqc, Rigetti Foundry Services, VTT, IQM, IMEC, CEA-Leti, AQT, QuiX Quantum, and LioniX International.

- **Expanding Quantum Workforce**

  Formal education and training programs are being developed to cultivate a skilled workforce of quantum engineers, physicists, software developers, and technicians, ensuring the industry has the talent required to sustain long-term growth.

These advancements collectively signal the maturing of the quantum technology ecosystem, paving the way for scalable and commercially viable quantum solutions.

INCREASED PRIVATE INVESTMENT AND COMMERCIALIZATION

Private investment in quantum technologies is surging, reflecting growing commercial confidence and accelerating the transition from research to real-world applications. Leading quantum companies such as PsiQuantum, Rigetti Computing, IonQ, D-Wave Systems, Quantinuum, IQM Quantum Computers, and PASQAL have each secured investments exceeding $100 million, underscoring strong market interest.

- **Public Sector Investment**

  Governments worldwide are also making substantial commitments to quantum development. The U.S. has invested $5 billion to date, while China leads with $15 billion, followed by Europe at $1.2 billion and India at $0.75 billion. In total, more than 30 governments have pledged over $40 billion to advance quantum technologies.

- **Growing Deal Activity**

  The quantum sector witnessed approximately 50 investment deals worth $1.5 billion in 2024—double the previous year's total—highlighting an accelerating funding landscape. The Indian government, in particular, has ramped up financial support for quantum startups, and this momentum is expected to intensify in 2025.

With increasing private capital and government backing, quantum commercialization is set to advance rapidly, bringing the industry closer to practical deployment and widespread adoption.

QUANTUM GEOPOLITICS

Quantum technology is more than a scientific race—it is a contest for future global power with profound implications for defense, intelligence, economic security, and national resilience.

- **United States**

  The U.S. quantum ecosystem thrives on strong government funding and a dynamic private sector, with tech giants like Google and IBM, alongside startups like PsiQuantum, advancing diverse quantum modalities. The National Quantum Initiative Act of 2018 laid the foundation for research, workforce development, and industrial growth, while also emphasizing national security through Post-Quantum Cryptography (PQC) to counter future cyber threats. White House directives have reinforced quantum as a national priority, advocating a whole-of-government approach to maintain leadership and mitigate risks.

- **China**

  Following its centralized, state-driven model, China has made massive investments in quantum research, with institutions like USTC and Zhejiang University leading breakthroughs. The country's ambition for quantum supremacy is evident in its large-scale programs and military-intelligence integration efforts, aiming for rapid deployment of quantum capabilities. Researchers at Peking University demonstrated large scale quantum entanglement on an optical chip, heating up with Quantum race globally.

- **Europe**

  The EU pursues regional collaboration and strategic autonomy through initiatives like the Quantum Flagship and national programs in Germany, France, Belgium, and Switzerland. Europe is fostering strong academic research while also developing a robust quantum supply chain to reduce dependencies on external players.

- **Other Key Geographies**

  Countries like Canada, Japan, and Australia are making strategic investments in niche areas—quantum software (Canada), specialized quantum hardware (Japan), and quantum sensors (Australia).

Export control: As quantum technologies become critical to national security, export restrictions are tightening on components like Arbitrary Waveform Generators (AWGs), Digital-to-Analog Converters (DACs), Microwave Components, specialized lasers, and cryogenic dilution refrigerators. In January 2025, Europe initiated a review of outward Foreign Direct Investments (FDI) in critical security technologies, with quantum among the top three areas under scrutiny. Export controls on quantum are expected to intensify, shaping global supply chains and strategic alliances.

INDIA'S QUANTUM JOURNEY AND THE NATIONAL QUANTUM MISSION

India's quantum efforts have historically been led by individual researchers and academic institutions, with a strong focus on fundamental science rather than technology development and commercialization. With a rich legacy in theoretical physics, leading universities and research institutes have long engaged in quantum information science, quantum computation, and related areas, with over 170 professors actively working in quantum technology domains.

In recent years, start-up activity has emerged, particularly in quantum software, algorithms, and quantum-safe cryptography, though these ventures have largely been bootstrapped or received limited seed funding. The DST's Quantum-Enabled Science and Technology (QuEST) program has provided some funding support, while early-stage efforts in quantum hardware—such as superconducting qubits, trapped ions, and photonics—have remained small in scale.

NATIONAL QUANTUM MISSION: A STRATEGIC LEAP FORWARD

Recognizing the global quantum race and India's strategic need to strengthen its capabilities, the **Government of India launched the National Quantum Mission (NQM) in April 2023**, with a **budget outlay of ₹6,003 crore**. This initiative aims to build a **comprehensive indigenous quantum technology ecosystem**, focusing on:

- **A mission-mode approach with significant budget allocation,** reflecting a strong commitment to quantum technology development.
- **Leveraging India's strong theoretical foundation** in quantum physics and information science through established research institutions and universities.
- **Accelerating start-up ecosystem development** by providing substantial funding and support to promising quantum ventures.

- **Clear timelines and well-defined goals** to drive tangible progress across quantum computing, quantum communication, quantum sensing, quantum materials, and workforce development.

FIVE WAYS QUANTUM COMPUTING RESHAPES NATIONAL SECURITY

Quantum technologies are set to redefine national security priorities across multiple domains. From breaking encryption to designing next-generation weaponry, nations that successfully advance quantum capabilities will gain an unprecedented strategic edge.

1. ***Cryptography and Cybersecurity*:** A sufficiently powerful, **fault-tolerant quantum computer (CRQC)** could break widely used **public-key encryption algorithms**, rendering modern **internet security, online banking, and secure communications obsolete**. Countries are in a race to develop and implement **Post-Quantum Cryptography (PQC)** to safeguard their data. Those who master PQC first can protect their critical information while others remain vulnerable. Topology qubit, due to their inherent stability and resistance to errors and the promise of scalability can accelerate the development of CRQC.

2. ***Intelligence Gathering***: Quantum computing could **revolutionize intelligence analysis** by processing vast, complex datasets far beyond classical capabilities. It would **enhance signals intelligence (SIGINT)**, allowing nations to intercept, analyze, and decode communications at an unprecedented scale. The ability to **break encryption** would provide unparalleled intelligence advantages, reshaping espionage and counterintelligence operations. Possibility of million qubits, with realization of techniques like topology qubits, can provide extraordinary capabilities for intelligence gathering and processing.

3. ***Military Applications***: Quantum technologies will drive breakthroughs in **materials science**, leading to **next-generation military hardware**. Quantum algorithms will **optimize logistics, resource allocation, and battlefield strategy**, making defense operations more efficient. Quantum-enabled AI (**Quantum AI**) will power **autonomous military drones and robotic systems**, enhancing both offensive and defensive capabilities. Scalability of qubit systems to million, as promised by the topology qubit, would take weaponization of them to the new level enabling highly sensitive quantum sensors for ultra precise navigation, detection of next gen stealth aircraft and other objects, simulation of complex phenomena, and build robust and resilient control systems for autonomous weapons.

4. ***Economic Warfare***: The ability to **break current encryption** could **destabilize financial markets**, **compromise banking systems**, and **endanger digital payment infrastructures**. Quantum computers could also be used to **steal sensitive intellectual property** from corporations and governments, leading to a new era of economic espionage.

5. ***Geopolitical Power*:** Nations that achieve **early breakthroughs in quantum computing** will establish a **technological and knowledge base** that others will struggle to replicate. Dominance in quantum will also allow countries to **shape global technology standards and norms**, influencing international regulations. Furthermore, leading quantum nations may impose export controls to restrict access to key technologies, preventing adversaries from catching up. With their potential for enhanced stability and scalability, topology qubit would likely solidify the dominance of leading quantum nations.

NATIONAL SECURITY IMPERATIVES FOR INDIA

Quantum computing is a **dual-use technology** with **transformative implications** for defense, intelligence, and cybersecurity. While India has made strides through its **National Quantum Mission**, a **strategic framework** is essential to navigate both **opportunities and threats**.

Accelerating Quantum Computing and Security Preparedness: Breakthroughs in qubit stability, error correction, and quantum software signify accelerating progress. India must prepare for two scenarios:

- *Incremental Advances:* Gradual improvements in qubits, control systems, and algorithms.
- *Disruptive Breakthroughs:* New platforms (e.g., silicon spin or topological qubits) or novel error correction techniques that drastically shorten the quantum timeline.

Advancements in quantum technology would expose the country to increased risk of technological surprise and strategic blind spots. Being caught off guard by quantum driven advancements would jeopardize national security, economic competitiveness, and technological leadership.

Key Recommendations to address the uncertainty associated with quantum timeline:

- Continuous Monitoring: Establish a task force to track global quantum advancements.
- Cryptographic Intelligence: Assess vulnerabilities in critical national systems.
- Directives and guidelines on crypto agility to ensure organizations from leading industry sectors including critical sector are ready to quickly adapt to the possible breakthroughs.
- PQC Transition Plan: Involving risk prioritization-based transition and roadmap, accelerated POCs, testing and certification, and exchanging information about the deployments.
- Early Warning System: Leverage scientific intelligence for potential breakthroughs.
- Technology Access Agreements: Establish bilateral partnerships for rapid adoption, especially the modalities that offer scalability, including topology qubit.
- Flexible R&D Funding: Adapt investment priorities based on emerging breakthroughs.

CONCLUSION

India's quantum security strategy must integrate technology monitoring, research flexibility, and supply chain security while leveraging global partnerships and domestic innovation. A proactive, multi-pronged approach will ensure national security remains resilient in the quantum era.

NOTES

सत्यमेव जयते

NITI Aayog