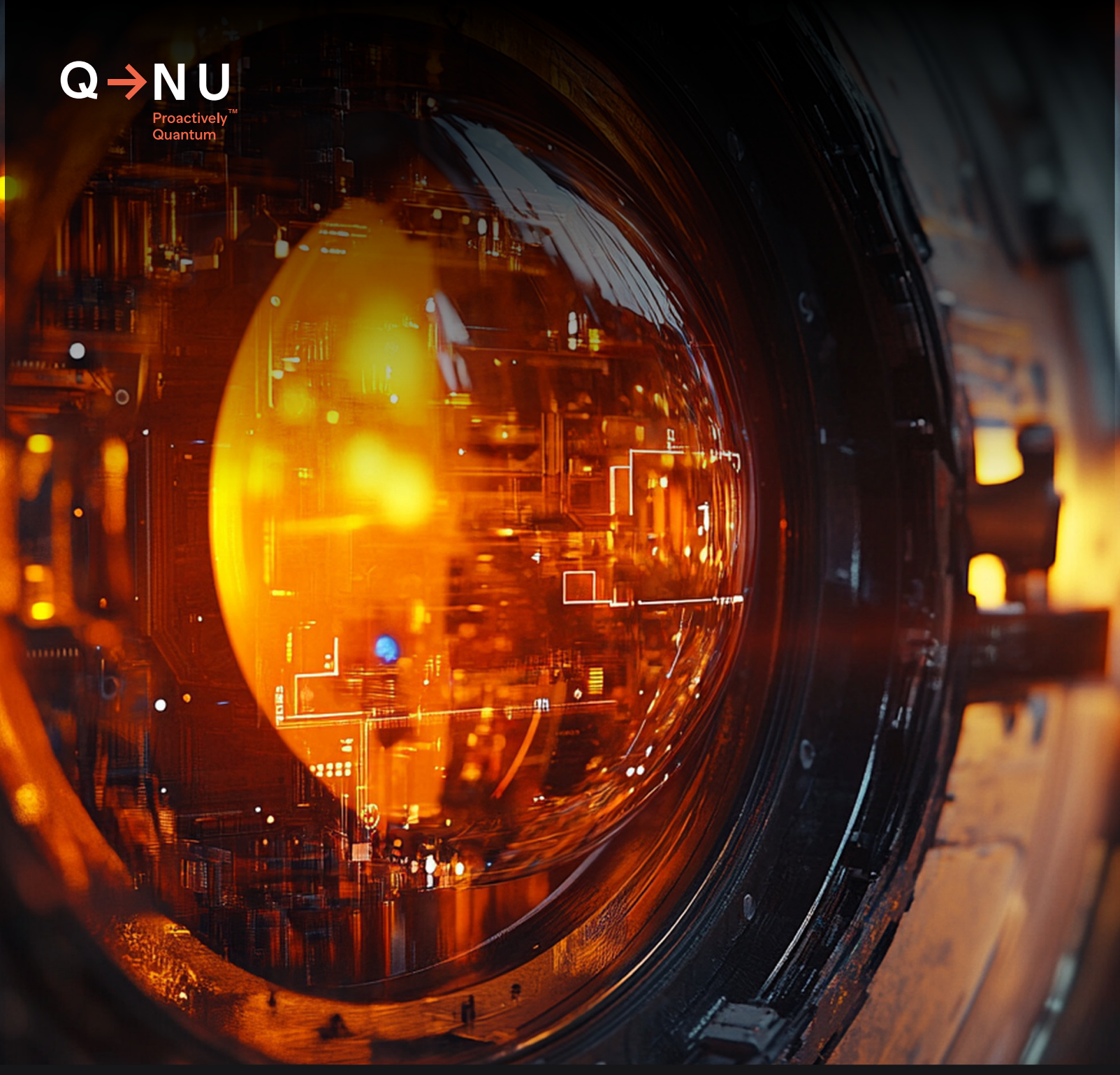
Q→NU
Proactively™
Quantum



Quantum Readiness to Quantum Supremacy for the Defence Sector

Accelerating the Defence Sector's Transition Towards an End-to-End Integrated Quantum-safe Future through Quantum Key Distribution, Quantum Random Number Generator, Quantum Encryption, Post Quantum Cryptography (PQC), Crypto-agility, Quantum Hardware Security Module (QHSM) and more.

Content

Executive Summary

Global defence establishments are now at the threshold of one of the most disruptive technological shifts and entering a period of strategic vulnerability. The defence sector has faced similar situations in the past and handled them well during the advent of nuclear weapons and the introduction of satellite communications.

Now, the time has come again, in the form of quantum technology.

The rise of quantum computing and **quantum communication** brings new threats and opportunities. Embracing opportunities and mitigating **quantum threats** are the keys to the industry's success.

The future of defence organisations depends on the decisions they make now in 2025, and any delay from here will put them at a disadvantage compared to their counterparts.

$40B

is committed to quantum tech globally for military & strategic systems.

Source: Spherical Insights.

50%

of federal US IT leaders are moving to post-quantum cryptography.

Source: Quantum Zeitgeist.

This defence sector whitepaper from QNu Labs establishes the **quantum threat** landscape, presents global and **Indian perspectives on quantum readiness**, addresses myths and misconceptions associated with **quantum communication**, outlines top defence use cases, provides a roadmap for adopting quantum cryptography and quantum encryption, and highlights available **quantum security** solutions and products.

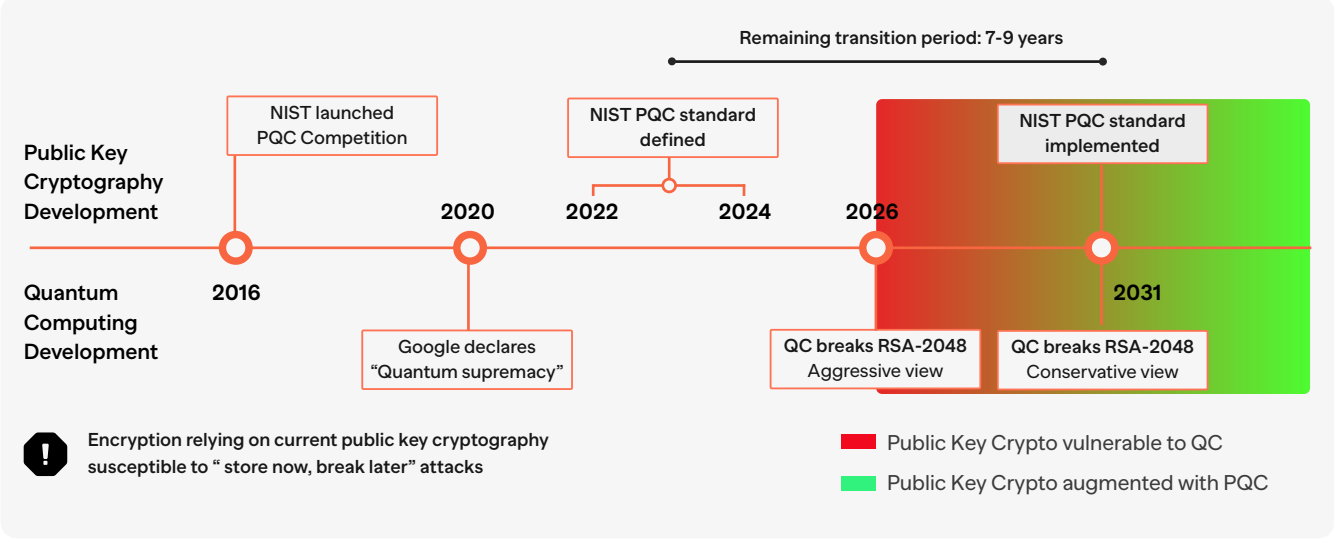
With this whitepaper, at QNu Labs, we aim to help **achieve quantum readiness for the defence sector** proactively and equip to achieve quantum supremacy in the era built on trust, resilience and sovereignty.

Welcome to the world of quantum.

Quantum Disruption

What is Q-Day & when will it happen?

Q-Day, or Quantum Apocalypse, is the day when quantum computers break the current encryption, which forms the basis of all the existing security systems.



Why is quantum a threat to the defence sector?

- ### Vulnerable Encryption

  All existing defence sector security is based on outdated encryption, which quantum computers can break in a few minutes. Without quantum cryptography, all other attempts are futile.

- ### High-value Targets

  Defence communication systems, satellite telemetry, and nuclear command and control are prime objectives for quantum-enabled state-sponsored adversaries.

- ### Sensitive data under threat

  The cryptographic foundations that secure command-and-control systems, space assets, intelligence networks, battlefield communications and other classified data are under direct quantum threat.

- **National sovereignty at risk**

  The impact of a breach in the defence sector is immense. During a conflict, it can alter outcomes on the ground and undermine national sovereignty.

Why does quantum encryption matter "NOW" to the defence sector?

- **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.

- **Migration Timeline**

  Quantum migration will also take considerable time and resources.

- **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.

Quantum encryption is a need, not a choice.

Quantum readiness is a strategic need, not a technical choice.

Achieving quantum readiness and quantum supremacy is feasible for every defence body with QNu Labs.

The answer is to act now. Begin by finding your quantum risk status.

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

Explaining HNDL with a visual

HNDL Lifecycle

Interception Today → Storage Today → Quantum Computer Availability → Future Decryption → Data is exposed

What is quantum readiness?

Quantum readiness is a state of cybersecurity when an organisation is prepared, planned and equipped for the impacts of quantum computing and quantum threats.

68%	57.5%	Only 5%
of organisations believe that quantum will break today's encryption. (Data Threat Report)	of decision-makers expect quantum attacks within 3 years. (Data Science Report)	of the organisations are quantum-safe. (Security Magazine)

Assessing & Understanding Quantum Risk

How to find your quantum risk status?

At QNu, we suggest using a theorem proposed by Dr. Michele Mosca, an established cryptography expert.

You have to consider three key factors: X, Y & Z.

Shelf life: The amount of time your sensitive data should be secure and in active use. **(X)**

Migration time: The amount of time taken to adopt and migrate to quantum security **(Y)**

Q-Day: The timeline of when quantum computers will break existing cryptography **(Z)**

- If X+Y is greater than Z, you are at severe risk already.
- If X+Y is equal to Z, you are at moderate risk.
- If X+Y is lower than Z, you are now in a safe zone and should act immediately.

Note: The time frame between 2026 and 2031 is the quantum risk zone (Z), during which quantum computers will break existing defence security.

Sample

Your X = 10 Years
Your Y = 3 Years
Your Z = 5 Years.

10 + 3 > 5: You are at high risk.

What are the common Myths & Misconceptions about Quantum Communication?

After understanding the quantum risk status, the world accelerates faster towards quantum adoption; however, myths and misconceptions about quantum communication still persist.

If the situation continues, it will:

- Slow down strategic quantum adoption
- Cause misplaced investments
- Leave critical defence and national assets vulnerable

At QNu Labs, we firmly believe that **clarity is the first step towards quantum readiness.**

Myth 1

Quantum Computing and Quantum Communication are the same

Reality: Quantum computing is all about processing power. Quantum communication is about the secure transmission of information. Defence systems need quantum-safe communication today.

QNu's Proactiveness

We build quantum communication systems (like **QKD**) that are already deployable; however, large-scale quantum computers are still a decade away.

Myth 2

Quantum Communication and Quantum Security are different worlds

Quantum communication is the bedrock of quantum security. Security in the quantum era involves protecting information using tools such as QKD and QRNG. Without quantum communication, quantum security would remain incomplete.

QNu's Versatility

Our Armos (QKD) and Tropos (QRNG) solutions demonstrate how communication and security are fused into a single framework.

Myth 3

Quantum communication is science fiction, not practical

Quantum-secure communication is already in use. China has the longest quantum network; Europe and the US are also building theirs. Meanwhile, ISRO and DRDO in India are testing QKD in satellites. This is no longer experimental; it is operational.

QNu's Versatility

QNu has already deployed operational quantum-secure networks. For us, this is no longer a lab experiment; it is national security developed and delivered.

Myth 4

Quantum security will replace existing infrastructure

Quantum communication is designed to complement existing systems, not to replace them. Defence organisations don't need to rip and replace entire architectures. They can integrate quantum solutions with existing fibre and satellite links.

QNu's Promise

QNu's products are interoperable, designed for seamless integration without disrupting the existing defence communication frameworks.

Myth 5

Quantum communication is too expensive and futuristic for defence

The cost of a breach is far greater than the cost of implementing security measures. Defence communication losses could result in billions of dollars in operational and strategic consequences.

QNu's Offerings

QNu builds end-to-end, scalable, cost-effective systems tailored for the defence sector, making sovereign-grade security accessible today.

International & Indian Quantum Preparedness

What are the geo-political dimensions & global benchmarks?

The quantum race has become a strategic contest among global powers. Military and defence leaders must recognise that technological leadership in quantum communication will translate directly into national security advantage.

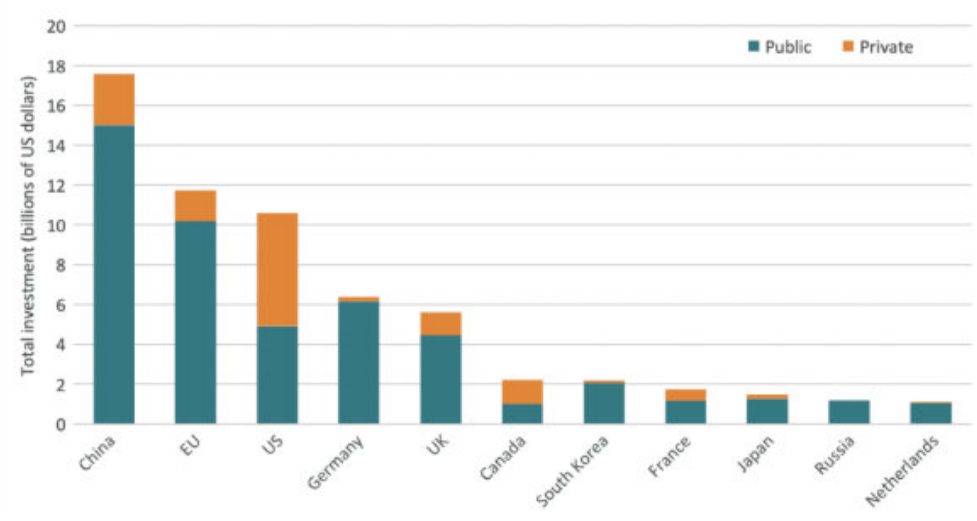
China is the first nation to launch a quantum communication satellite (intercontinental) in 2016. The benchmark has been set so high that catching up is not a viable option; leapfrogging is the right option.

What is the status of Global Quantum Preparedness?

- **US:** NSA and CISA mandated PQC adoption timelines
- **UK NCSC:** A clear migration roadmap has been established. Early adopters are from the defence sector.
- **Australia:** ASD advised post-quantum planning from 2023.
- **EU:** Building EuroQCI (European Quantum Communication Infrastructure) as a multi-nation secure backbone.
- **China:** Invested billions into quantum research and demonstrated intercontinental QKD.

- **Russia:** The country is developing its own home-built PQC research, with a special focus on secure communications for military operations.
- **NATO:** Focusing on Quantum as a strategic defence.
- **India:** Empowered with **National Quantum Mission** (NQM) funding, entanglement trials, 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.

What is India's Quantum Preparation?

The National Quantum Mission (NQM) is India's significant initiative to propel the nation to the forefront of quantum technology research and development, with a budget of ₹6,003.65 crore, placing India among the few nations actively preparing defence systems for the quantum era.

Objectives of NQM

- To develop quantum computers: with 20-50 physical qubits in 3 years, with 50-100 physical qubits in 5 years, and 50-1000 physical qubits in 8 years.
- To establish satellite-enabled quantum-secured communication between two ground stations over 2000 km within India and extend to other countries.
- To implement quantum-secured communication spanning 2000 km using trusted nodes and wavelength division multiplexing (WDM) on existing optical fibre infrastructure.
- To develop a multi-node quantum network incorporating quantum memories, entanglement swapping, and synchronised quantum repeaters at each node, enabling scalable and robust quantum communication (2-3 nodes).
- To design highly sensitive quantum devices for precision timing, navigation, and secure communication.
- To develop and synthesise next-generation quantum materials such as superconductors, novel semiconductor structures, and topological materials.

Exploring Quantum Cybersecurity

The Quantum Trinity: QKD, QRNG & PQC

Post-Quantum Cryptography (PQC)

— NIST-compliant mathematical algorithms resistant to quantum attacks

— Deployable on existing hardware, radios and networks

— Quantum cryptography is perfect for hybrid usage

— Ideal for mass deployment across drones, systems and IoT

Quantum Key Distribution (QKD)

— Uses the laws of physics for security

— To ensure that your data is safe at all times (in rest and in transit)

— No eavesdropping & instant detection of any interception

— Ideal for the defence sector as it requires ultra-high reassurance

Quantum Random Number Generator (QRNG)

— Root of trust providing true random numbers

— Uses quantum phenomena for creating truly unpredictable keys

— Multiple application usage

— Can be embedded in defence radios, satellites, and cryptographic modules.

Together, these three pillars, QKD + QRNG + PQC, represent the **quantum trinity of security.**

What are NIST-approved Post-Quantum Cryptography Algorithms?

- **CRYSTALS-Kyber**
  FIPS 203, primary & for all general encryption. Also known as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).
- **CRYSTALS-Dilithium**
  FIPS 204, for digital signatures. Also known as Module-Lattice-Based Digital Signature Algorithm (ML-DSA).
- **Sphincs+ algorithm**
  FIPS 205, for digital signatures. Also known as Stateless Hash-Based Digital Signature Algorithm (SLH-DSA).

- **FALCON**
  FIPS 206, for digital signatures. Also known as FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA).

- **HQC**
  Hamming Quasi-Cyclic is a backup for ML-KEM, and it is yet to be standardised by NIST. **Source: NIST**

Achieving Crypto-agility is the first step

Crypto agility is the ability to transition rapidly from one type of encryption to another.

— It adds flexibility to adopt any advanced encryption methods, such as quantum encryption.

— It strengthens security by adopting the latest technology.

— It reduces the migration time and cost.

What are the Quantum Communication Use Cases for the Defence Sector?

Quantum security for the defence sector and governments is varied. We have listed the top use cases of quantum communications in the defence sector and government bodies.

- **Classified Communication**
  With high entropy, you can secure wireless communications, preventing intelligence leaks without any compromise.

- **Routing Systems**
  Unpredictable selection and patterns in routes improve operational secrecy, which is impregnable to quantum computers.

- **Secure VPN**
  Securing battlefield and headquarters communication is of higher importance, which demands defence-grade data transfer through quantum-secure tunnels.

- **Command & Control Systems**
  QKD-enabled communication lines shield classified communication from interception. Man-in-the-middle attacks are invalidated.

- **Government Data Centres**
  Building and protecting zero-data leakage environments is imperative, as the quantum threat is looming larger every single day.

- **File Transfers**
  The point-to-point encryption must be risk-free, as it can pose a threat even after several years have passed.

- **Intrusion Detection**
  Since quantum security solutions provide an intrusion detection feature, every attempt to intercept will be detected and reported.

QNu's Quantum Journey with the Defence Sector

Journey so far: QNu & Defence Sector

QNu is on a mission to make India not just digitally advanced, but digitally invincible!

— Providing end-to-end quantum security, offering both hardware and software products and solutions

— Launched nation-first Quantum Key Distribution (tested, trusted, indigenously developed, proven) for India's defence. This detects and prevents man-in-the-middle (MITM) attacks. Backed with "Type Approval" Certification from Telecommunication Engineering Centre (TEC), under the Department of Telecommunications (DoT).

— Launched India's first indigenously developed Quantum Random Number Generator (QRNG) that offers true randomness with high entropy and was certified by CR RAO AIMSCS.

— Additionally, robust defence security is strengthened by Q-ORE, a quantum-safe drone communication platform.

— Received DSCI's Most Innovative Product of the Year (2019)

— Established a Quantum Lab for the Indian Army at Mhow (2021)

— Received the Raksha Anveshan Ratna Award for Tech Breakthrough by MoD (2022)

— Received National Technology Award from the Department of Science & Technology, India (2022)

— Winner of Innovations for Defence Excellence (iDEX – Open Challenge 2.0 in 2022)

— Developed Hub & Spoke QKD as a part of the NSCS grant (2023)

— Deployed Quantum Safe Wi-Fi Solution for MCEME and MCTE (2024 and 2025)

— Established a 300Km QKD network for the Indian Army at Jodhpur (2025)

— Participation in shaping India's and state-wise national quantum security roadmap (QIB 2025)

— Received Cybersecurity Company of the Year at the 4th MSME Innovation Summit and Digital Innovator Award from Intellyx, a Dutch analyst firm (2025)

— Ongoing Deployment of QKD at 5 locations for the Indian Navy

— Building the world's largest commercial QKD Network of 500 KMs

How QNu helps the Defence Sector?

Guided by the philosophy "Quantum-secure. Nation-first. Future-ready," and strengthened by deep R&D and global collaborations, QNu Labs provides an end-to-end quantum safe integrated platform that safeguards nations, businesses, and people everywhere from the threats of the quantum world.

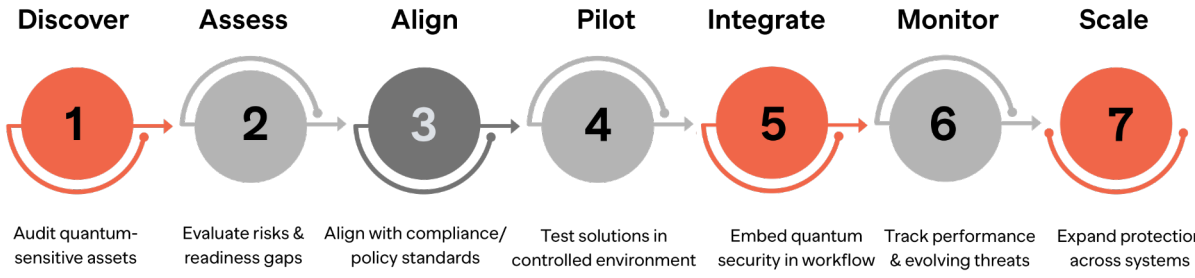
We proudly call ourselves the Architects of Trust, Privacy, and Security in a Quantum Future.

QNu's Quantum Products & Solutions for the Defence Sector

- **Armos (QKD)**
  100% secure quantum key distribution over long distances with range extension using trusted nodes.
- **Tropos (QRNG)**
  Generates a million random numbers per second and forms the basis of quantum encryption.
- **QShield™**
  Next-generation SaaS platform offering a flexible, scalable, and future-proof framework
- **Hub and Spoke**
  Point-to-Multipoint topology, link up critical establishments in a quantum secure network
- **QConnect**
  Quantum secure VPN and secure tunnel built for mission-critical infrastructure
- **Q-ORE**
  Quantum safe end-to-end drone communication platform
- **QHSM**
  End-to-end quantum hardware security module
- **QVerse**
  End-to-end quantum-safe messaging and collaboration platform

All our offerings are born in India, built for the world.

Quantum Security Roadmap: Implementation Plan



India's defence establishment has a rare opportunity: not just to shield the nation, but to shape the very architecture of global quantum security.

QNu Labs positions India as a global leader in the quantum communications space. Join us in this journey today.

Your First Step Towards A Quantum-safe Future

Through this whitepaper, the quantum threat landscape is established, presenting both global and Indian perspectives on quantum readiness and dispelling the myths associated with it. Knowing the top use cases of quantum communication and the roadmap for a quantum secure future is the key.

Begin your quantum journey.

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