KAMARAJ IAS ACADEMY
Only IAS Academy by Grandson of "Peruntholaivar Kamarajar"

Quantum satellite

Published On: 25-12-2024

Why in news?

India's plans to launch a **quantum satellite** in the next 2-3 years to enable quantum communications reflect the country's growing interest in the field of **Quantum Technologies (QT)**. The satellite would enhance security for data transmission, leveraging the principles of **quantum physics** to protect information from potential cyber threats.

National Quantum Mission (NQM):

The **National Quantum Mission (NQM)**, with a total outlay of **?6003.65 crore** over eight years (2023-2031), aims to establish India as a leader in **quantum technology**. Conceptualized by the **Prime Minister Science Technology Advisory Council (PM-STIAC)**, the mission focuses on scientific and industrial research and development, and the creation of an innovative ecosystem in quantum technology.

Key components of the mission include the establishment of **four Thematic Hubs (T-Hubs)** in the following areas:

1. **Quantum Computing**
2. **Quantum Communication**
3. **Quantum Sensing & Metrology**
4. **Quantum Materials & Devices**

What is a Quantum Satellite?

A **quantum satellite** is designed to use the principles of **quantum physics** to ensure **secure data transmission**. In the era of quantum computing, traditional cryptographic systems are at risk of being compromised, making **quantum cryptography** an essential tool for future-proof security in communications. Quantum satellites are particularly geared toward **Quantum Key Distribution (QKD)**, which enhances communication security by detecting eavesdropping attempts.

How Does Quantum Communication Secure Messages?

1. **Quantum Measurement**: Quantum systems, such as photons, change when measured. If an eavesdropper intercepts a quantum key encoded in photons, the process of measurement will alter the photons, signaling a breach to both the sender and receiver.
2. **Quantum Entanglement**: When particles are entangled, any change to one particle immediately affects the other, regardless of distance. This property ensures that any interception of data can be detected in real time, thus safeguarding the integrity of the communication.

Global Scenario:

- **China** has been a leader in quantum satellite technology, launching the world’s first quantum satellite, **Micius**, in 2016, followed by others such as **Quantum Experiments at Space Scale (QUESS)**.

- **United States**: Boeing is working on deploying a small quantum networking satellite by 2026, highlighting the global push towards quantum communication systems.

Challenges with Quantum Key Distribution (QKD):

Despite its promise, **QKD** faces several challenges:

- **Authentication Issues**: QKD does not inherently authenticate the source of the transmission, which is a vulnerability in security systems.
- **Hardware Dependency**: QKD requires specialized hardware, which makes it difficult to update or patch, posing risks for long-term security.
- **High Costs**: The infrastructure costs for implementing QKD can be significant, limiting its widespread adoption.
- **Denial-of-Service (DoS) Risks**: An eavesdropper could potentially disrupt the system, preventing legitimate users from accessing the communication network.

Post-Quantum Cryptography (PQC) as an Alternative:

In light of the challenges associated with QKD, the **U.S. National Security Agency (NSA)** recommends **post-quantum cryptography (PQC)**. Unlike QKD, which relies on quantum principles, **PQC** employs **classical encryption methods** that are designed to resist attacks from both classical and quantum computers. This provides a more robust solution for secure data transmission.

Conclusion:

India’s upcoming quantum satellite project is a significant step toward enhancing data security through quantum communication. While **quantum key distribution** presents immense potential, its challenges need to be addressed for practical implementation. In the meantime, **post-quantum cryptography** offers a viable alternative to safeguard data against future quantum computing threats. As quantum technologies evolve, these initiatives position India at the forefront of global scientific advancements in secure communication systems.