

DRDO's Quantum Key Distribution (QKD) Platform

Prelims: Current events of national and international importance | Defence

Why in News?

The DRDO has successfully configured and tested a QKD platform on the live network at the Proof and Experimental Establishment (PXE) in Chandipur.

Quantum Key Distribution (QKD)

- **QKD** - It is a secure communication protocol that leverages quantum mechanics to generate and distribute a shared secret cryptographic key between two parties.
- This cryptographic key can then be employed to encrypt and decrypt messages.
- The protocol allows communicating parties to detect any attempts to intercept the quantum key, provided the protocol's security assumptions hold.
- **Aim** - To secure real-time critical observations and telemetry during artillery and armoured weapon testing.

Quantum Key Distribution (QKD) Platform	
	Feature
	Organisation
	Test location
	Technology
	Development cluster
	Production partner
	Primary application
	Other potential applications
	Details
	DRDO
	Proof and Experimental Establishment (PXE), Chandipur
	Quantum Key Distribution (QKD)
	Microelectronic Devices, Computational Systems and Cyber Security (MCC) cluster of DRDO
	Taqbit Labs
	Secure defence communications
	Finance, telecommunications and strategic communications

Types of QKD Communication

Fibre-based QKD	Uses optical fibres to transmit quantum signals
-----------------	---

Free-space QKD	Uses light through an open-air optical path; can avoid laying dedicated optical fibres
----------------	--

- **Importance of Free-Space QKD**

- Free-space QKD reduces the reliance on installing optical fiber infrastructure.
- This approach is particularly advantageous in challenging terrains and densely populated urban environments.
- It may also minimize infrastructure disruption and lower deployment costs in appropriate scenarios.
- However, free-space QKD requires appropriate optical links and unobstructed line-of-sight conditions, limiting its applicability in certain environments.

- **Advantages and Limitations**

Advantages	Limitations / Considerations
Enables detection of interception attempts	Requires specialised quantum hardware
Supports secure cryptographic key distribution	Practical range and channel losses can be limiting
Useful for sensitive strategic communications	Deployment and maintenance can be expensive
Can complement existing encryption systems	Does not automatically secure compromised endpoints or the entire network

- **Applications**

- **Defence** - It can secure telemetry, weapon-test observations, and strategic communications.
- **Finance** - It enables the protection of sensitive financial data transmissions.
- **Telecommunications** - It enhances the security of selected communication networks.
- **National security** - It protects critical information infrastructure.

Reference

[TOI | DRDO's Quantum Key Distribution \(QKD\) Platform](#)