DO YOU KNOW?

QUANTUM COMPUTING AND THE FUTURE OF CYBERSECURITY

Are our laws ready for the post-quantum world?

WHAT’S CHANGING?

- Classical computers use bits — 0 or 1.
- Quantum computers use qubits, which can be both 0 and 1 simultaneously.
- That makes them exponentially faster at solving certain problems, including the ones that protect our data.

THE SECURITY THREAT: ENCRYPTION PARADOX

- From Banking to Aadhaar, today’s digital world runs on cryptography.

- But quantum algorithms like Shor’s Algorithm could break RSA and ECC encryption, the very foundation of cybersecurity.

- These encryption standards underpin the IT Act, DPDP compliance, and e-governance systems.

HOW QUANTUM BREAKS ENCRYPTION

- RSA and ECC depend on problems that take classical computers thousands of years to solve.

- A large-scale quantum computer could solve them in minutes.

- When that happens, everything from digital signatures to VPNs could be exposed.

HARVEST NOW, DECRYPT LATER: SILENT RISK

- Attackers are already storing encrypted data now to decrypt it later when quantum computers arrive.

- That includes government archives, healthcare data, and cross-border transfers.

- **Legal implication:** Sensitive data under DPDP and the IT Act could be retrospectively exposed.

THE POLICY TIMELINE: COUNTDOWN TO Q-DAY

- Experts estimate quantum-capable decryption by 2035–2040.

- Global initiatives like NIST’s Post-Quantum Cryptography (PQC) and India’s National Quantum Mission (NQM) are *racing to prepare*.

LEGAL AND GOVERNANCE GAP

- IT Act (2000), DPDP Act (2023) and global data laws assume classical encryption.
- None address the quantum risk horizon or mandate quantum-resistant standards yet.
- *CRGCL research indicates the need for forward-compatible cybersecurity and data protection frameworks.*

THE QUANTUM DEFENCE: POST-QUANTUM CRYPTOGRAPHY (PQC)

- Post-Quantum Cryptography (PQC) uses mathematical problems resistant to quantum attacks.
- Governments and companies must migrate early inventory, update, and future-proof.
- India should align NQM and MeitY encryption standards with NIST PQC protocols.

WHAT CRGCL RECOMMENDS

✅ Update cybersecurity rules to include quantum-safe encryption.

✅ Mandate crypto-agility in IT compliance frameworks.

✅ Integrate quantum resilience into digital public infrastructure (DPI) design.

✅ Build capacity for PQC testing and certification.

Centre for Research and
Governance on Cyber Law

Empower Yourself—
Know Your Digital Rights!

Share this post to spread awareness. Follow CRGCL for more updates on digital governance and cyber law.

www.crgcl.com