CURTISS-WRIGHT

Quantum Threat Timeline: Are You Ready?

Timeline of Quantum Threat Evolution

Year	Milestone	Implication
1994	Shor's Algorithm introduced	RSA/ECC vulnerability identified
2022	NIST selects PQC candidates	Industry direction established
2025-2030	Quantum tech matures	Legacy encrytion becomes risky
Post-2030	Cryptanalytic threshold breached	Urgent need for quantum-safe systems

Adversary Strategy: Harvest Now, Decrypt Later

- Data interception is active
- Long-lived encrypted data is being stockpiled
- Quantum decryption could trigger lasting security compromise

Interception	Encrypted Data Scraped	Countdown to Decryption
ACTIVE	1000 TB	10 years 3,652 days 87,648 hours 5,258,880 minutes

Data Defense Strategies

- **NSA Type 1 Encryption:** High-assurance cryptography for classified info
- **CSfC Architecture:** Two-layer full drive encryption, algorithm agility, modular upgrades
- **PQC Transition Planning:** Adopt NIST-approved post-quantum algorithms

Quantum Readiness Roadmap

Don't wait for quantum reality. Design for quantum inevitability.

Cryptographic Preparedness	System Architecture	Strategic Action
▪ Are you using NSA Type 1 or CSfC-approved solutions? ▪ Have you identified systems with long-lived data at risk? ▪ Are algorithm transition plans integrated into your roadmap?	▪ Is your system designed with crypto agility in mind? ▪ Can your hardware and firmware accommodate PQC updates?	▪ Have you conducted quantum risk assessments across mission systems? ▪ Are all stakeholders aligned on transition urgency? ▪ Are you plugged into NIST, NSA, and vendor PQC initiatives?

- **Quantum Supremacy Isn't Theoretical; It's Tactical**
- **By 2030, Legacy Encryption Won't Be Good Enough**
- **Your Readiness Determines Your Resilience**

Learn more about crypto-agile storage solutions at:

curtisswrightds.com