CENTER FOR CYBERSECURITY POLICY AND LAW

Quantum Computing: What It Is and Why It Matters

What Is Quantum Computing?

Quantum computing uses the principles of quantum mechanics to process information in new ways. Unlike traditional bits that are 0 or 1, quantum computing uses qubits* that can be both at once, allowing them to test many solutions simultaneously and solve problems beyond the reach of today's supercomputers.

Why It's Important

Quantum computing could revolutionize science, technology, and society, driving breakthroughs in healthcare, sustainability, and innovation. Yet it also poses major risks, as future systems may break today's encryption. Governments and industries must act now to build policies and safeguards that guide its secure and responsible development.

**Also known as quantum bits, the fundamental unit of information in quantum computing.*

What Happens if We Don't Get Ahead on Quantum Cybersecurity Guardrails?

BROKEN ENCRYPTION STANDARDS

Large-scale quantum computers could crack current encryptions, exposing sensitive government, defense, and financial data worldwide.

LOSS OF DIGITAL TRUST

A quantum-driven breach could erode confidence in online banking, authentication, and communications, weakening trust in the global digital economy.

UNSECURED INFRASTRUCTURE & FRAGMENTED DEFENSES

Critical systems like power grids, hospitals, and supply chains could stay exposed without consistent post-quantum protections, creating gaps attackers could exploit.

MASS DATA COMPROMISE

Bad actors could harvest encrypted data today and decrypt it later, revealing decades of confidential data.

Considerations for Policymakers and Industry

- **Prepare:** The shift to post-quantum cryptography must start now. Waiting until quantum computers can break today's encryption will leave systems exposed for years.
- **Treat Quantum Readiness as Governance, Not Just Technology:** Quantum security is an organization-wide responsibility. Leaders should plan ahead, identify where encryption is used, coordinate with suppliers, and ensure systems can be updated as new protections become available.
- **Global collaboration is essential:** Quantum threats cross borders, so nations must work together on shared encryption standards, testing, and timelines. Governments should also include quantum technology in broader AI and cybersecurity policies to ensure coordination and security.
- **It's not all bad:** Quantum computing is also driving new encryption methods built to resist future attacks, with efforts like NIST's post-quantum cryptography initiative strengthening defenses today.

Resources:

- *https://www.nist.gov/cybersecurity/what-post-quantum-cryptography#:~:text=How%20does%20post%2Dquantum%20cryptography,Learn%20more%20about%20quantum%20cryptography*
- *https://www.centerforcybersecuritypolicy.org/insights-and-research/pqc-lead-the-way-or-fall-behind*
- *https://www.gao.gov/blog/next-big-cyber-threat-could-come-quantum-computers-government-ready?utm_source=chatgpt.com*
- *https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/*