Quantum technology primer: Overview

For cyber security leaders

Introduction

Quantum technologies are devices and systems that harness principles of quantum physics. This enables new ways to measure, analyse and understand the environment around us.

As quantum technologies advance, they will support new types of systems and applications. For example, quantum computers can perform complex calculations that are infeasible for classical computers.

Quantum technologies may shape future competitive advantage, digital infrastructure and cyber security for most organisations. While having a major impact, they will likely become part of routine business workflows.

This guidance is part of a series of quantum technology primers for cyber security leaders. To learn more, refer to cyber.gov.au/quantum

Principles of quantum mechanics
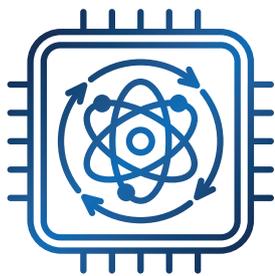
Quantum mechanics is the study of how tiny particles behave, often at atomic and subatomic levels. At this scale, quantum physics describes their behaviour more accurately than classical physics.

Concepts like superposition and entanglement form the basis of quantum phenomena. Quantum technologies use these concepts to enable their unique and enhanced capabilities.

Superposition

Superposition means a particle exists as multiple possible states at the same time. Measuring the particle collapses it into a single definite state. This property enables quantum systems to explore many potential outcomes simultaneously. For example, in classical physics, flipping a coin results in either heads or tails. In quantum physics, superposition means the coin exists as both heads and tails until observation determines the outcome.
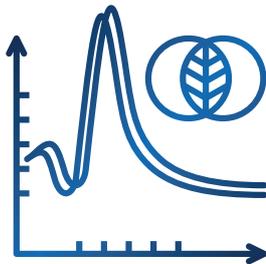
Entanglement

Entanglement refers to particles that share a quantum state. This creates correlations that persist even across vast distances, so measuring one particle reveals information about the other. For example, rolling two dice normally produce independent random numbers. Entanglement means the dice are correlated and rolling one can reveal the result of the other, even if they are far apart.
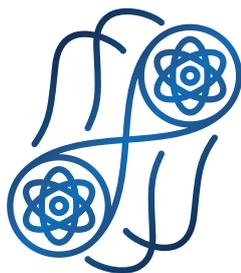
Cyber security considerations

Organisations should consider how quantum technologies might affect business functions and factor this into their cyber security plans. Following best practices can manage most cyber security risks from these technologies.

Preparing now for quantum technologies is crucial. Adopting post-quantum cryptography (PQC) is a key example, as capable quantum computers will break some current cryptography. Organisations that delay planning for PQC remain exposed to the risks of legacy technologies.

To prepare for a future shaped by quantum technologies, organisations should consider proactive steps. This includes:

- ensuring cyber security plans are up to date and align with current cyber security best practice
- developing a plan to adopt and implement PQC across networks
- assessing risks across data lifecycles and ensuring sensitive information remains secure as part of information technology security best practice
- verifying service providers and vendors align with the organisation's quantum adoption and readiness plans
- continuing staff education and training on good cyber security practices to help mitigate threats.

For more information, search 'planning for PQC' on cyber.gov.au

Types of quantum technologies

Quantum technologies have the potential to enhance a range of devices and systems. They could support areas such as computational problems, optical communications and sensing. While most quantum technologies are still in early development, some are already in use.

Quantum-class technologies and sciences represent a broad and evolving group of capabilities. Some of these technologies will increasingly become part of an organisation's supply chain and digital infrastructure. Examples of quantum-class technologies include:

quantum computing, such as noisy, intermediate-scale quantum computers and future cryptographically relevant quantum computers

quantum communications, such as lasers for optical communications and other quantum networking components
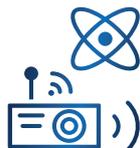
quantum sensors, which aim to provide precise and sensitive measurements of activity in the physical world.

To learn more about how your organisation can factor specific quantum technologies into its cyber security plans, read our upcoming quantum primers.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre