Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Quantum technology primer: Overview

For cyber security leaders

Content complexity
MODERATE ● ● ○

cyber.gov.au

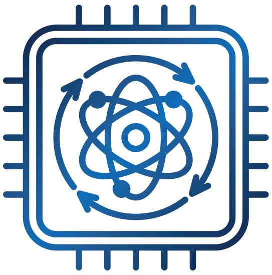
Introduction

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

Quantum technology applies quantum physics to perform tasks that are infeasible for classical systems. Quantum physics studies how matter and energy behave at the smallest scale, often at atomic and subatomic levels. At this scale, quantum physics describes their behaviour more accurately than classical physics.

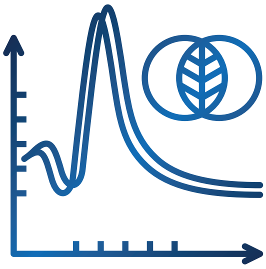
The advancement of quantum-class technologies will enable new devices, systems and capabilities. For example, quantum computers can perform complex calculations that are infeasible for classical computers.

This guidance is part of a series of quantum technology primers. To learn more, search 'quantum' on cyber.gov.au



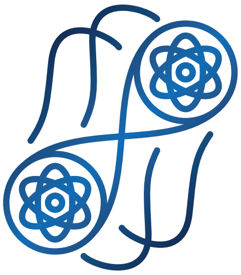
Principles of quantum mechanics

Quantum mechanics is the study of how tiny particles behave, which can be different to what is considered normal. 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 understand 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 preparing for PQC risk cryptographic vulnerabilities and costly remediation.

To prepare for a future shaped by quantum technology, 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.

Types of quantum technologies

Technologies that use quantum mechanics have the potential to enhance a range of devices and systems. They can improve areas such as computational performance, 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. 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 cryptographically relevant quantum computers

quantum information sciences, such as quantum communications through quantum key distribution and quantum networking

quantum sensors, which use properties of quantum mechanics to make more precise measurements than classical sensor technologies.

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

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

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