Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Quantum technology primer: Communications

For cyber security leaders

Content complexity
MODERATE ● ● ○

cyber.gov.au

Quantum communications seek to leverage quantum mechanics to encode and transmit information between quantum systems, regardless of distance. This encompasses a broad set of emerging capabilities that aim to enable new forms of secure and efficient communication.

As of today, quantum communications don't offer a practical cyber security solution. Organisations should prioritise strengthening their security posture and planning for post quantum cryptography (PQC).

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

About quantum communications

Quantum communications use quantum phenomena, such as superposition and entanglement, which have no classical equivalent. These properties enable uniquely different approaches to performance and security compared to classical communications.

While the method for encoding information differs from classical communications, the underlying transmission medium is often similar. For example, using photons (a quantum of light) as a physical carrier over optical fibre or free space.

The impact on cyber security

Quantum communications could bring new methods for transmitting sensitive data with unique security properties. However, practical limitations such as transmission distance, hardware requirements and environmental sensitivity can affect the reliability and scalability of quantum communications.

Quantum communications don't replace the need for classical cryptographic security. In some cases they rely on classical cryptography for security, including authentication. As quantum computing advances, it will threaten classical asymmetric cryptographic algorithms and place unsecured sensitive data at risk. These risks, combined with the limitations of quantum communications, highlight the need for organisations to begin transitioning to quantum-resistant algorithms. Organisations may consider monitoring evolving standards, investing in research and development, and assessing vendor readiness. For more information, search 'planning for PQC' on cyber.gov.au

Quantum key distribution

The Australian Signals Directorate (ASD) will continue to monitor methods of securing communications in the presence of a cryptographically relevant quantum computer, such as quantum key distribution (QKD). However, practical limitations of QKD – including specialised hardware, and concerns around availability and native authentication – mean that ASD does not support its use for secure communications.

Cyber security risks

Quantum communication introduces a range of cyber security considerations. While quantum technologies will influence the cyber security landscape, organisations can manage many of these risks through proactive measures grounded in cyber security best practice.

The following are some potential risks that organisations should factor into their cyber security plans and posture.

Authentication and identity security

Quantum communications often depend on classical authentication channels for authentication and identity verification. If these channels are not cryptographically secure, attackers could impersonate endpoints and insert themselves into the communication session.

Organisations should consider adopting quantum-resistant authentication mechanisms (such as post-quantum digital signatures), multi-factor authentication and secure key storage.

Supply chain risks

Quantum technologies may depend on specialised materials or vendors. The associated hardware and firmware could be prone to tampering, counterfeit parts or malicious implants.

Organisations should consider establishing a verifiable chain of trust across hardware, firmware and software components to support supply chain integrity. It is important to assess vendors for secure development practices and require transparency across the supply chain.

Interoperability challenges

Quantum communication systems may not be compatible with existing infrastructure, protocols or security frameworks. This may hinder adoption and integration of quantum communications.

Organisations should ensure quantum communication systems integrate with classical infrastructure such as networking, security and hardware. Systems should align with emerging standards and best practices from reputable industry sources. To support interoperability and resilience, implement a plan for adopting new technologies and standardising protocols.

Key management complexities

Secure key distribution and lifecycle management remain crucial in quantum communication environments. Effective key management can ensure the integrity and authenticity of data transmission, while poor key management can lead to unauthorised access or data compromise.

Organisations should implement robust key management processes that includes secure key generation, distribution, storage, rotation and destruction.

Scalability and operational limitations

Current quantum communication systems face scalability constraints, such as limited transmission distance, bandwidth and infrastructure availability. These limitations can affect performance and coverage. Additionally, quantum communications can be sensitive to loss, interference and environmental disturbance. Such disruptions can lead to denial of service (DoS).

Organisations should monitor advancements in quantum-secure communication protocols, including quantum repeaters and satellite-based quantum communications. Applying cyber security best practices can help mitigate operational risks such as DoS.

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.

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