QUANTUM KEY DISTRIBUTION:
What is the opportunity in Defence and Security?

Governments depend on encryption for mission critical data, from managing tax returns to coordinating counter-terrorism operations. Quantum computers will one day crack today's public key encryption, creating major security risks. Quantum safe approaches, including Quantum Key Distribution (QKD), will be needed to secure future communications.

Organisations that rely on secure communications need to start preparing soon. Meanwhile there is a huge commercial opportunity for defence and security contractors to develop capabilities to deliver the world's future secure communications infrastructure.

Why does QKD matter to defence and security?

Military action and the fight against terrorism rely on sharing highly sensitive data which could cost lives in the wrong hands. Public services – from tax payments, to healthcare, to driving licence applications - are increasingly managed online. Future smart grids will use encryption to prevent cyber-attacks. Any discussions about e-voting depend on voter data being encrypted.

These will all be compromised if current encryption can be cracked.

Organised malicious actors and nation states are already collecting encrypted information with the plan to crack it later. So there is already an imperative to adopt "quantum safe" security in some cases, such as when sharing national security data that needs to stay secret for 20 years or more.

Government will look to the defence and security industry to provide this quantum safe future. By talking to the companies innovating in QKD now, the defence and security sector has the chance to identify future partners that can help them deliver QKD as part of their defence-in-depth arsenal. Those that get involved early will find themselves leading the sector when QKD reaches commercial maturity.

Where are we now and where are we going?

Companies including Toshiba and ID Quantique have already developed photon emitters and detectors capable of communicating encoded photons over fibre. Bristol-based KETS is developing chip-scale QKD which could be integrated into handheld devices. The UK Quantum Network provides fibre links within and between Cambridge and Bristol, allowing quantum technologies to be tested on real world infrastructure.

Commercial applications are already viable in highly secure industries where the benefits of securing information from future hacking outweigh the current cost. Over the next five years significant improvements will be made to transmission rates, and reducing size, weight and power, bringing QKD solutions close to market.

WHAT IS QKD?

In conventional encryption, data is encrypted using an algorithm, making it unintelligible to anyone who steals it. The algorithm also generates a key – a long string of random numbers – which allows the intended receiver to decrypt the data. This is secure for now, but such algorithms could be cracked in future by quantum computers.

In QKD, this key is physically distributed using a sequence of photons, whose quantum state is assigned randomly to represent a 0 or a 1. The physical approach means the key cannot be cracked mathematically. It is also impossible to copy or steal the key in transit, since quantum mechanics dictates that any observation will change the quantum state – which can be detected by the receiver.

WHO'S INNOVATING IN DEFENCE AND SECURITY?

The *Services Industriels de Genève* (SIG), Geneva's energy provider, is creating a smart grid network to connect its 800 power stations. Each will be connected to the SIG telecom optical fibre network and electricity network operations centre. To secure data transmission and detect intrusion, it will test QKD technology from ID Quantique in a real operational environment.

How to get involved

As one of the beneficiaries of QKD, we need the defence industry and its suppliers to work with the Quantum Communications Hub to shape QKD innovation and deployment.

Technology partners who serve government customers, including BT and Toshiba, are already involved in the QKD industry. As technologies move towards commercialisation, we also need input from those familiar with highly secure environments to shape the development of the technology and the standards that support it, such as those being developed by the ETSI Industry Specification Group on QKD (ETSI ISG-QKD).

It is important that eventual commercial products meet the needs of end users. By talking to us about their challenges, and engaging with the companies in our network, defence and security can help shape technology development and ensure QKD meets the needs of defence and national security.

Those interested in being involved in these projects, receiving updates, or finding out more should contact:

enquiries@quantumcommshub.net
www.quantumcommshub.net

QUANTUM
COMMUNICATIONS
HUB