Name of Quantum Technology

Secure Comms

What is the potential vision for this area?

In the next 5 years…

- 1st area to make it
- Integrating quantum with classical
- Not just secure? – channel capacities. How to do this?
- Hybrid quantum/classical
- Device independent QKD
  - security proofs
  - Implementation
- High security point to point links
- An extra layer of security over & above existing classical means
- Beyond QKD

In the longer term…

- Understanding which bit is secure post Quantum compution (post quantum cryptography)
- Quantum comms has matured to have a full system
- Secure wireless systems
- Fully realised quantum repeater
- Full integrations with standards
- Security of Cloud
- Secure networks
- “Broadband quantum channel”
- The “Quantum internet” based on distributed entanglement

- The Quantum Secure Comms communities vision is that a quantum comms system will develop that will seamlessly integrate with the classical comms industry and ultimately replace it.
- Consider Quantum security – not just cryptography
- Quantum computing enabling future Wireless communications

Name of Quantum Technology

Secure Comms

Psychological
Insufficient paranoia

What prevents this vision from being realised?

Research challenges to overcome…

- Overcome reluctance to accept 'Quantum' getting wide buy-in
- Not enough Quantum Network test beds
- How to integrate into existing infrastructure
- Better rates for device – independent QKD protocols – Bell's, Hasrem.
- New information theory frameworks
- Other application for QKD box
- New devices and algorithms
- Incorporating Q comms into wiretap channel – radio
- Formal verification of security protocols combining quantum & classical
- Smaller, cheaper, faster
- Closed experiment – engineering theory collaboration. Device independent verification.

Scientific / technological barriers…

- Defined standards
  - Standard measures of performance
  - Security standards
  - Validation, certification
- Loophole - free test of Bell inequality
- Quantum repeater

- Quantum repeater
- Strength core Q. computer Research
- Integrated device platforms leading to cheaper systems, opening up applications and market.
- Improved / new components (detectors / sources)
- Hardware for the Quantum Internet?
  - sources?) Efficiencies?
  - Channels?) Wavelengths?
  - Detectors?) Integration?

Name of Quantum Technology

What can the UK do to deliver this vision?

What we currently know…

- Have demonstrators already (e.g. Toshiba, ID Quantique)
- Moore's law hits limit.
- Future proof
- Theoretically secure against intercept
- Theory
- RSA has been cracked several times
- C. Crypto can only be computer security.

What we need to know…

- Stimulate the market
- How do we know the most appropriate security/encryption to use for a specific application (Power, processor size, security, etc)
- Security of quantum networks with classical nodes!
- Information theoretic limit
- Formalising gain for QKD
- Which applications are best for quantum cryptography.
- Do we understand all possible attacks on QKD (threat)
- New a crypto application + security analysis
- How to quantify the security of Quantum Cryptography
- Develop a QKD protocol with a full security proof for realistic devices.
- Device independent protocols other than key distribution
  - Randomness generation
  - What else?
- Interfacing between quantum & classical worlds.

Name of Quantum Technology

Secure Comms

What can the UK do to deliver this vision?

What should the UK do differently?

- Develop networks
- Explore the Quantum properties outside the classical application areas
- Define international standards required → for take up
- Actively involve industry
- Training ic & computer science
- Focus on practical applications
- Develop test beds for Qu. Comm
- Talk to security professionals to understand requirements
- Funding for international PhD students
- Articulate clear goals --→ Issue Grand Challenges?
- Train more PhD's
- Fund research at boundaries – Physics, Engineering, Computing, applied Maths, etc.
- Technology development is required to allow quantum comm systems to be robustly delivered.
- Integrated Institutes combining Maths, Physics, Computer Science.
- Create fora for discussion between quantum physicists & engineering groups.
- Explore new applications, e.g. in comms systems other than security.
- Fund R&D of semiconductor sources & detectors
- Integrated photonics
- More research & technical development through procurement
- Productionisation
- FIR Qubits