QUANTUM SECURITY
at all distance scales

# The UK National Quantum Technologies Programme and the work of the Quantum Communications Hub

UK Quantum Technology Hub for Quantum Communications

Director: Professor Tim Spiller

QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council

# UK National Quantum Technologies Programme (UKNQTP)

- December 2013 – £270M for a new UK QT Programme

This supported (2014-2019, Phase 1):

- Four Quantum Technology Hubs
- Centres for Doctoral Training (CDTs)
- Innovate UK funding programme (industry-led)
- A new Metrology Centre at the National Physical Laboratory (NPL)
- New QT Training and Skills Hubs linked to the existing CDTs
- Further capital equipment to support UK QT (£2M for quantum network)

2013 Autumn Statement

£270M

UK Government investment in QT development

Note also:

- DSTL (Defence Science and Technology Laboratory) investing some R&D funding, notably in PhD programmes focused on some QT sectors.
- The UKNQTP is continuing 2019-2024, Phase 2. **Total budget now ~ £1billion.**

# National Network of Quantum Technologies Hubs

The four Hubs:

Quantum Technology Hub in sensors and timing:

Birmingham-led; focus on atoms

Quantum Enhanced Imaging (QuantIC):

Glasgow-led; focus on light

Quantum Computing & Simulation Hub:

Oxford-led; focus on ion traps and photonics

but now includes other platforms; NQCC

Quantum Communications Hub:

York-led; focus on QKD applications

UK Quantum Technology Hub Sensors and Timing

QUANTIC

Quantum Computing & Simulation Hub

National Quantum Computing Centre

QUANTUM COMMUNICATIONS HUB

UNIVERSITY of York

QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Engineering and Physical Sciences Research Council

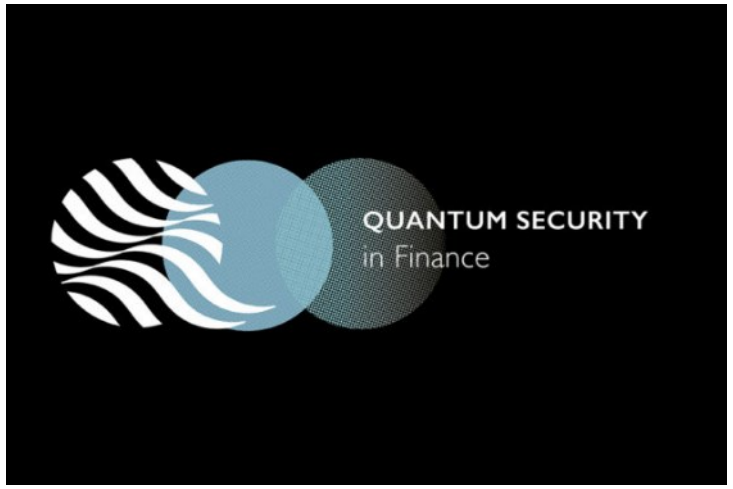
# Quantum Communications provide Quantum Security

# Quantum-Safe Communications

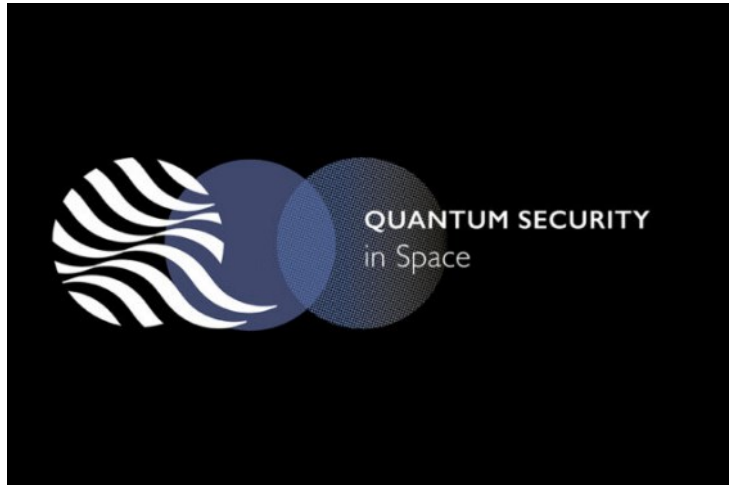
- Quantum computers will render current cryptography (PKI: RSA, elliptic curves…) vulnerable, Shor's algorithm.
- Mosca inequality: If X + Y > Z then worry now!

  Where X= security shelf life;  Y= re-tool time;  Z= time to quantum computer
- Quantum communications technologies and new mathematical techniques (post-quantum cryptography, PQC) are being developed for data security in a future quantum-enabled world.

# Sector perspectives






- Information, data and cyber security is of widespread importance, rather than being specific to certain sectors => **Secure communications underpin all sectors: commercial, government and public.**

# Sector perspectives

- Security requirements, flexibility and distance scales vary with sector, so the solutions and technologies will be more sector-specific.

- Examples: Size, weight & power (SWaP) constraints on devices dictate the form of quantum/conventional hybrid solutions – compact, free-space technologies for short-range mobile and long-distance satellite applications.

- Some technologies can offer more sector-specific solutions (e.g. quantum money and secure tokens for finance/banking).

- Standards and assurance are important for all sectors.

# Quantum Key Distribution (QKD)

Secure sharing of a key between two parties (Alice and Bob!)

- The quantum part is the distribution of the key, with the tamper-detection built into Nature ensuring that only Alice and Bob have copies.
- Once distributed, the (non-quantum) uses of the key(s) cover a wide range of secure information tasks: communication or data encryption, financial transactions, entry, passwords, ID/passports…
- The keys are consumables (use once only for security), so need regular replenishment, which is also “quantum”.
- Authentication (pre-shared key, or PQC) is additionally required.

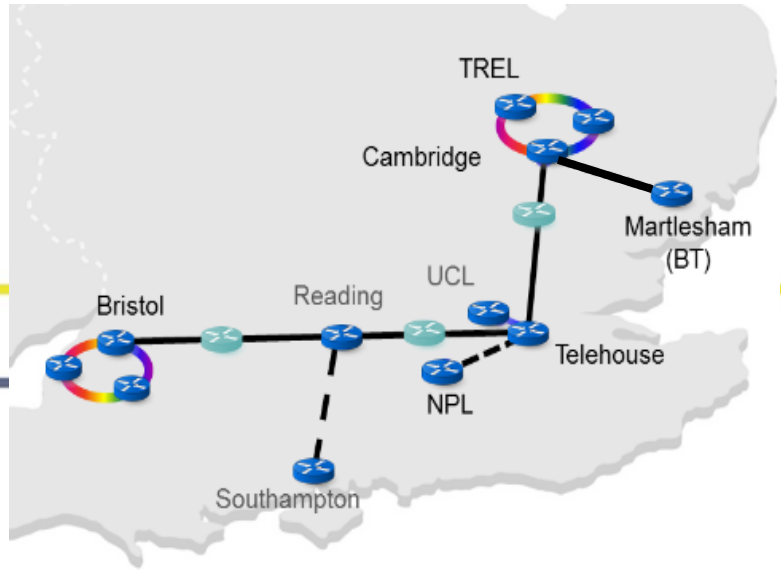
# Secure Comms at Short distances

- Dynamic networking for individuals and consumers requires short range, free space connections for compact devices.
- We have developed “consumer QKD”, now ready for TRL increase and partnership.
- Low SWaP are desirable for all technologies, but particularly this regime. The Hub supported the spin-out of KETS from Bristol.


# Intermediate distances

- Fibre networks provide the basis for conventional communications at metropolitan and intercity scales. Trusted-node QKD can utilise such networks and is progressing to software-defined networks (SDN).

- The Hub established the UK's first quantum network (UKQN) and is now moving to entanglement-based networks preparing for a Quantum Internet.



# Intermediate distances

- The Hub has also established the first fibre network link to industry (Cambridge to BT Adastral Park).
- Our work has facilitated tech transfer into industry-led development (e.g. ISCF AQuaSeC). Note: BT and Toshiba now operate a commercial trial with EY.
- Current work includes collaboration with Network Rail using trackside fibre for QKD, via Hub Partnership Resource Funding (PRF) project QTRAX.



QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council

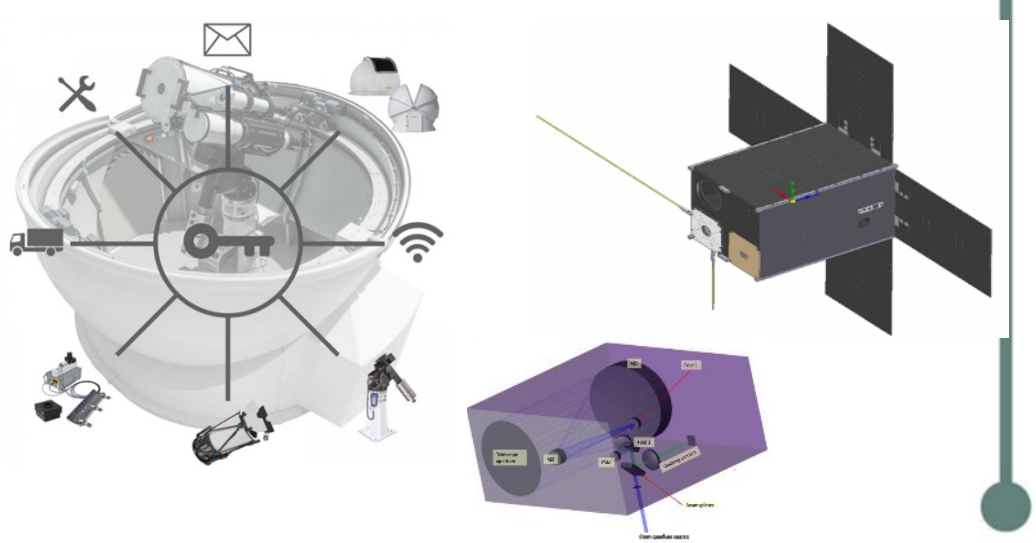
# Worldwide distances

- Quantum communications across oceans and between continents can utilise satellites. R&D is underway worldwide.
- Until satellites support memories, repeaters and entanglement distribution, they form trusted nodes.

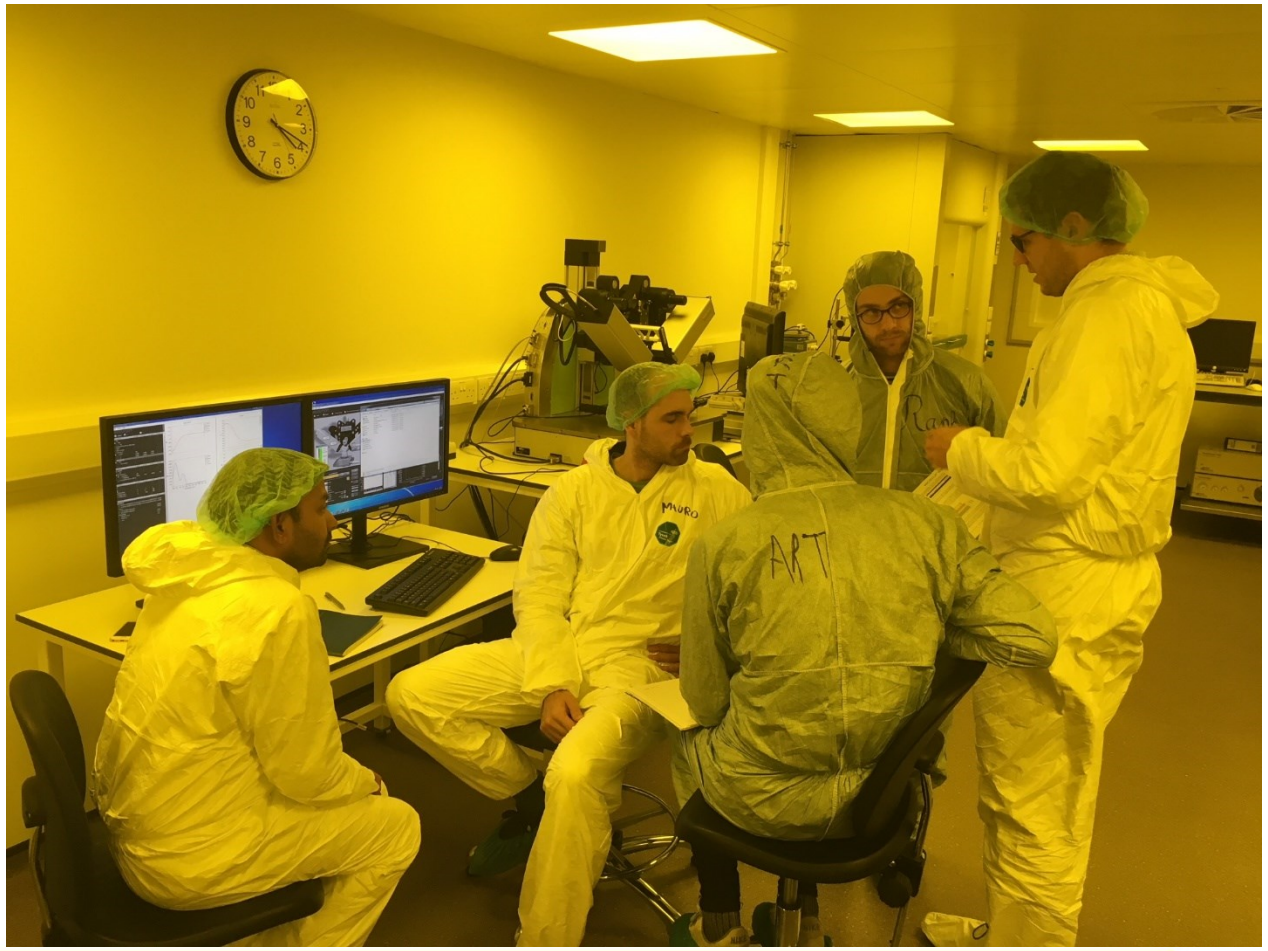
Engineering and Physical Sciences Research Council

# Worldwide distances

- The Hub is undertaking an in-orbit demonstration (launch 2024) of QKD from a CubeSat (supplier ISISPACE) to an optical ground station (Errol Airfield, Scotland).
- Other UK missions: ROKS, SPEQTRE.
- Other Hub-related activity e.g. Canadian QEYSSat mission: UK-Canada QT programme downlink source; Hub PRF project uplink entangled source.




# Beyond networking



- Sovereign capability and UK supply chain for Quantum Communications components such as Sources & Detectors.

# Beyond networking

OCTOBER 5, 2022

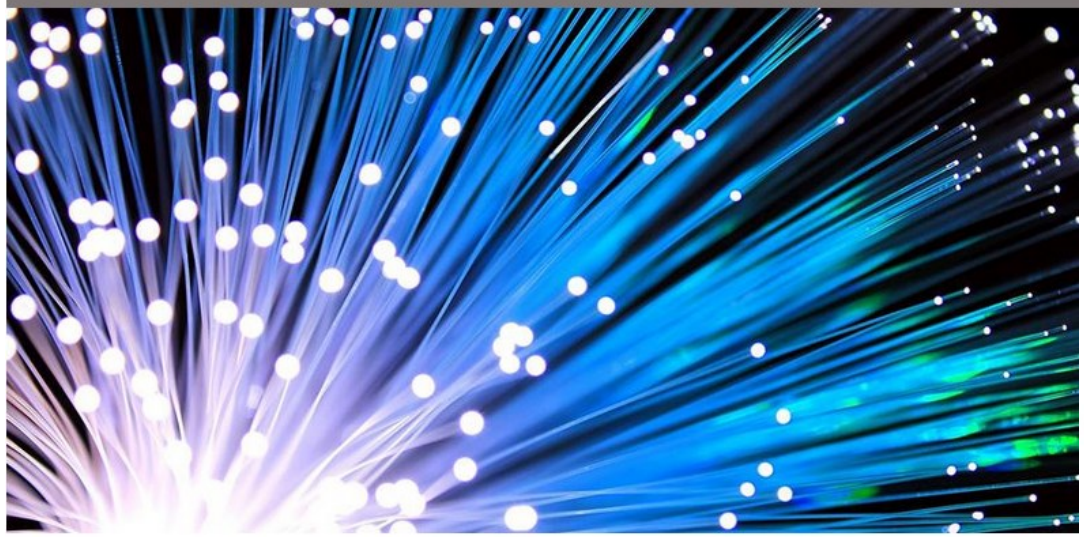
**Maximum randomness from untrusted devices**

Researchers working in the Quantum Communications Hub have shown new tight bounds on the amount of randomness that can be generated from a given amount of nonlocality. Random numbers are an essential resource for modern day society, with cryptography being an important application. Here it is crucial that the numbers are not only evenly distributed, [...]

Read more

- Device Independence
- New Quantum Security Protocols (quantum signatures / quantum money / quantum secure tokens …)
- Of particular relevance to finance services

Ultra-secure form of virtual money proposed



**A new type of money that allows users to make decisions based on information arriving at different locations and times, and that could also protect against attacks from quantum computers, has been proposed by a researcher at the University of Cambridge.**

The theoretical framework, dubbed 'S-money', could ensure completely unforgeable and secure authentication, and allow faster and more flexible responses than any existing financial technology, harnessing the combined power of quantum theory and relativity. In fact, it could conceivably make it possible to conduct commerce across the Solar System and beyond, without long time lags, although commerce on a galactic scale is a fanciful notion at this point.

Researchers aim to begin testing its practicality on a smaller, Earth-bound scale later this year. S-money requires very fast computations, but may be feasible with current computing technology. Details are published in the *Proceedings of the Royal Society A*.

> *"Instead of something that we hold in our hands or in our bank accounts, money could be thought of as something that you need to get to a certain point in space and time"*
>
> *– Adrian Kent*

QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council

# Beyond networking

- Quantum standards: ETSI and now many other bodies.

- Combining post-quantum cryptography (PQC) and QKD.

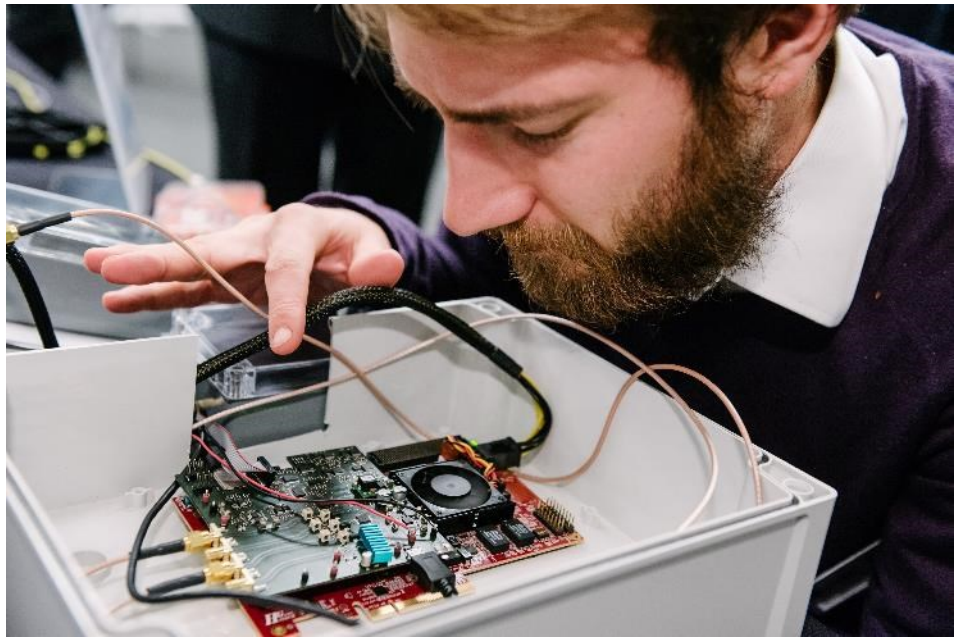
bsi.

NPL National Physical Laboratory

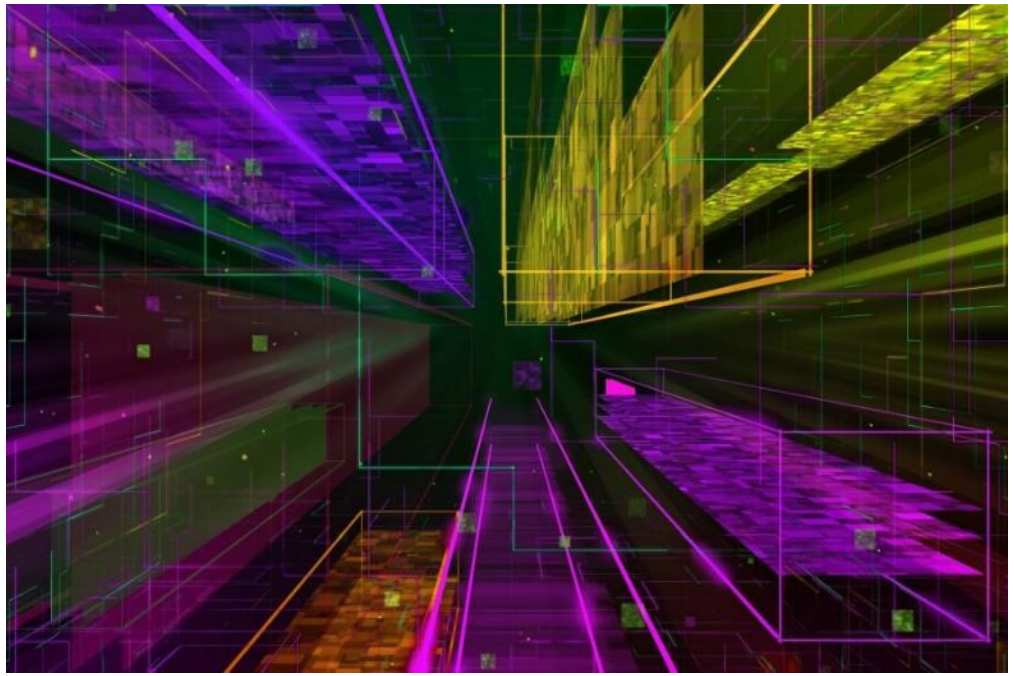
ETSI

NIST National Institute of Standards and Technology

# Beyond networking



- QRNG Assurance with Hub PRF project has led to a major ISCF consortium AQuRand, led by NPL.



AQuRand
ASSURANCE OF QUANTUM RANDOM NUMBER GENERATORS

University of York

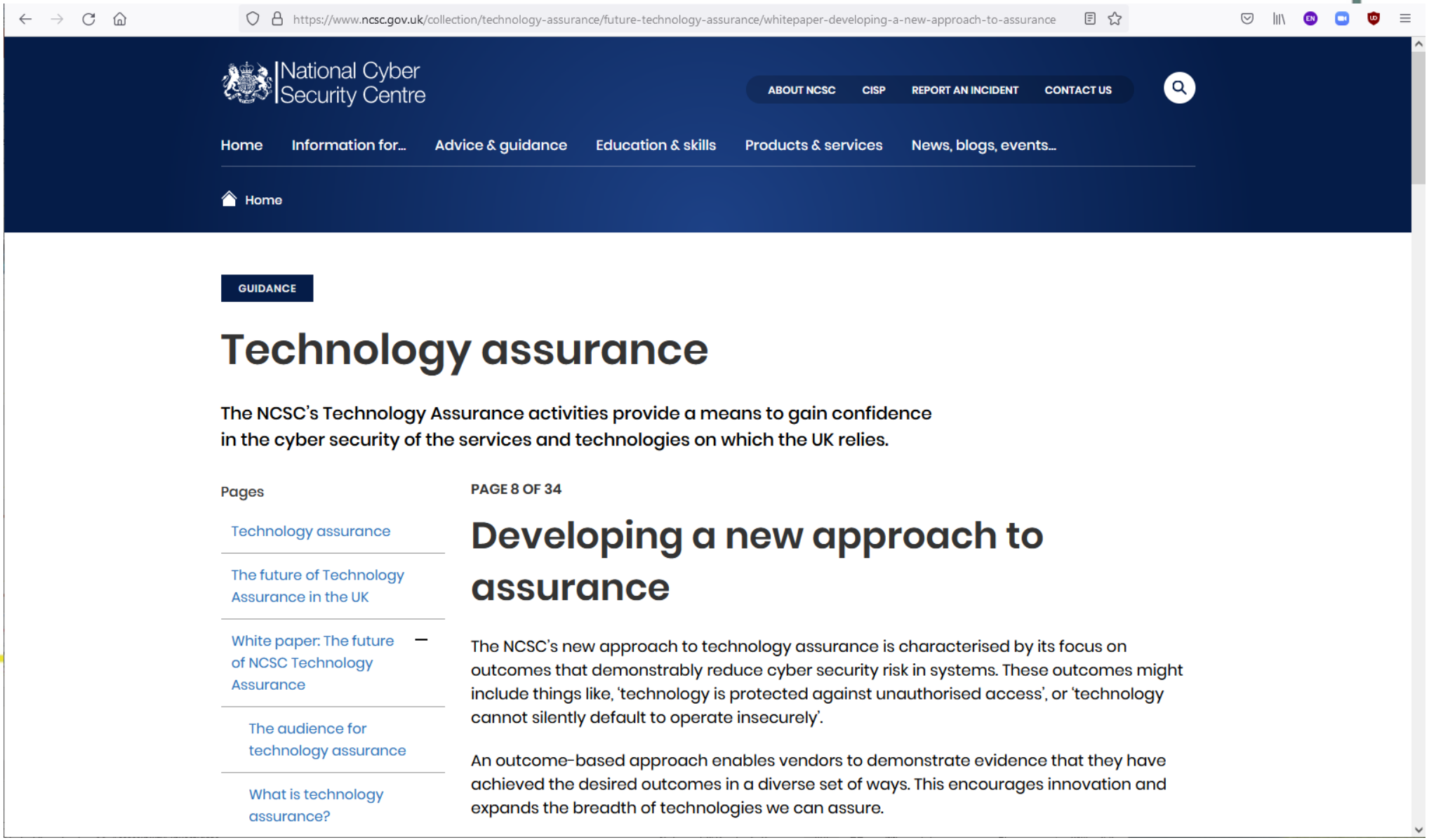
Quantum Communications Hub

UK National Quantum Technologies Programme

UKRI Engineering and Physical Sciences Research Council

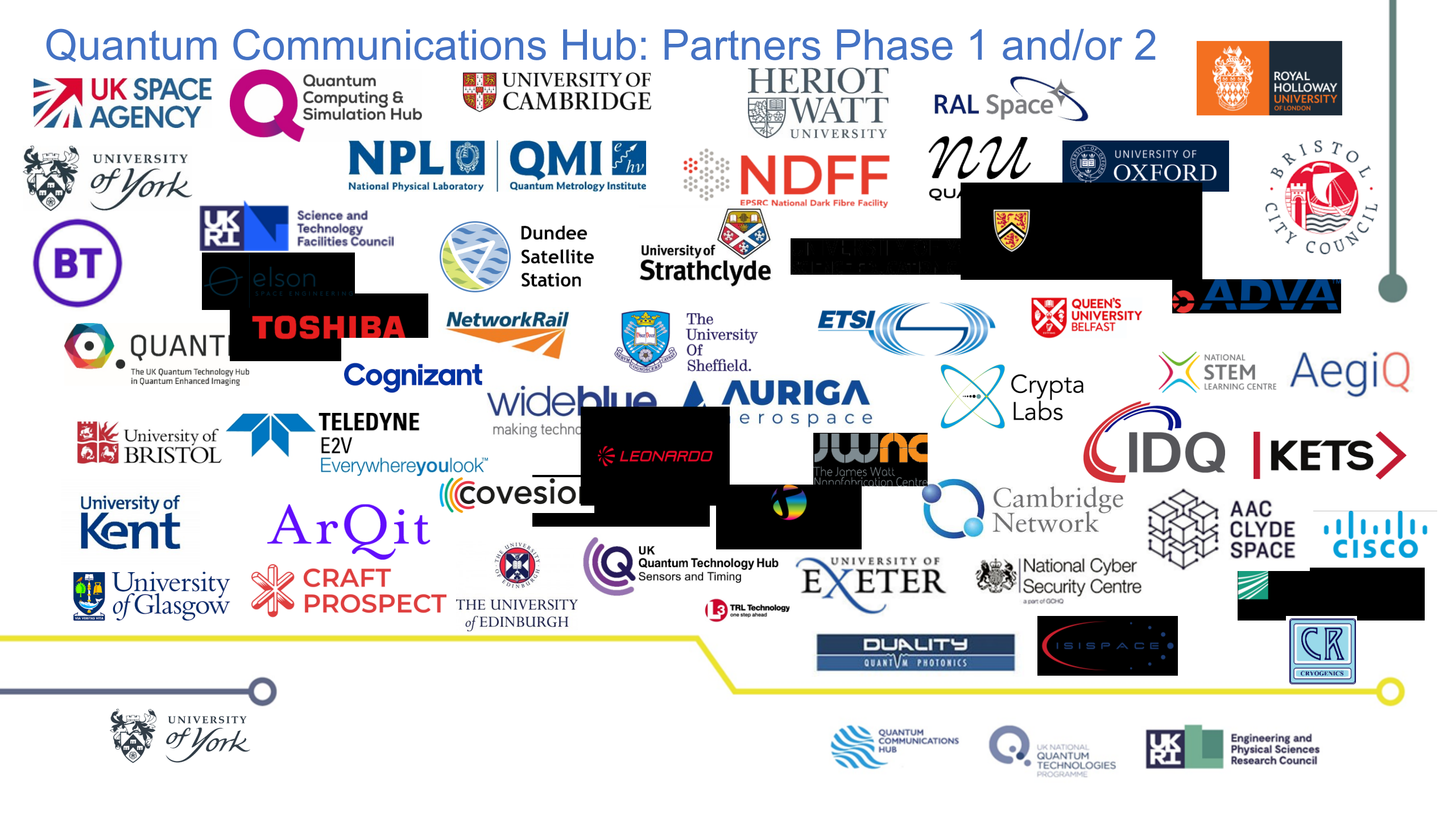
# Beyond networking

## Assurance beyond QRNGs




UNIVERSITY of York

# Quantum Communications Hub: Partners Phase 1 and/or 2



# Further UK Quantum Information

- The UK National Quantum Technologies Programme:

  http://uknqt.epsrc.ac.uk/

- The Quantum Communications Hub:

  www.quantumcommshub.net/

- Hub Annual Reports, other articles and detailed list of research publications:

  https://www.quantumcommshub.net/resources/

  https://www.quantumcommshub.net/research/

- Contact us: enquiries@quantumcommshub.net
- Follow us on Twitter: @QCommHub
- Quantum Technologies: UKGov 2023 National Quantum Strategypolicy paper https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-accessible-webpage

UKGov: New funding commitment of **£2.5billion** for ten years from 2024

UNIVERSITY of York

QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council