Peter Knight

Imperial College London, NPL QMI and UK National Quantum Technology Programme

Quantum Technology: Value and Importance of Standards

NPL *"a public institution …. For standardising and verifying instruments, for testing materials, and for the determination of physical constants" (Terms of reference for the Treasury Committee set up by Lord Salisbury in 1897 in response to the British Association lobby for the creation of NPL)*

The UK National Standards Body is the BSI; the UK National Measurement Standards Laboratory is NPL (usually referred to as our National Metrology Institute

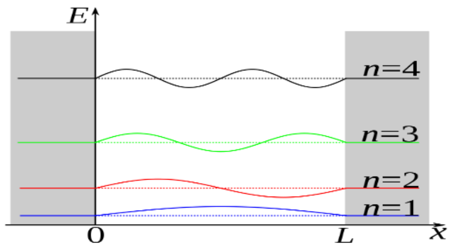
Thanks to colleagues in NQTP and especially NPL for help with slides

My task(s)- scene setting for the day: I need to-

- Introduce the UK quantum programme to the standards folks
- Introduce the standards programme to the quantum folks
- Ignore those very rare folks who have mastered both.

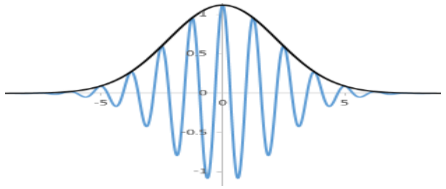
The strange world of quantum- highly counter-intuitive!

Quantization



All quantities are discrete, for example, the energy levels in an atom

Wave Nature of Matter



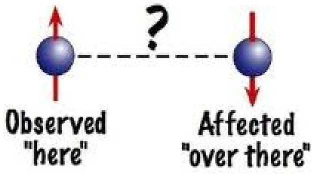
all objects (photons and particles) display both particle and wave properties

Superposition

Classical Bit	Quantum Bit (qubit)
0 or 1	0 and 1 0/1

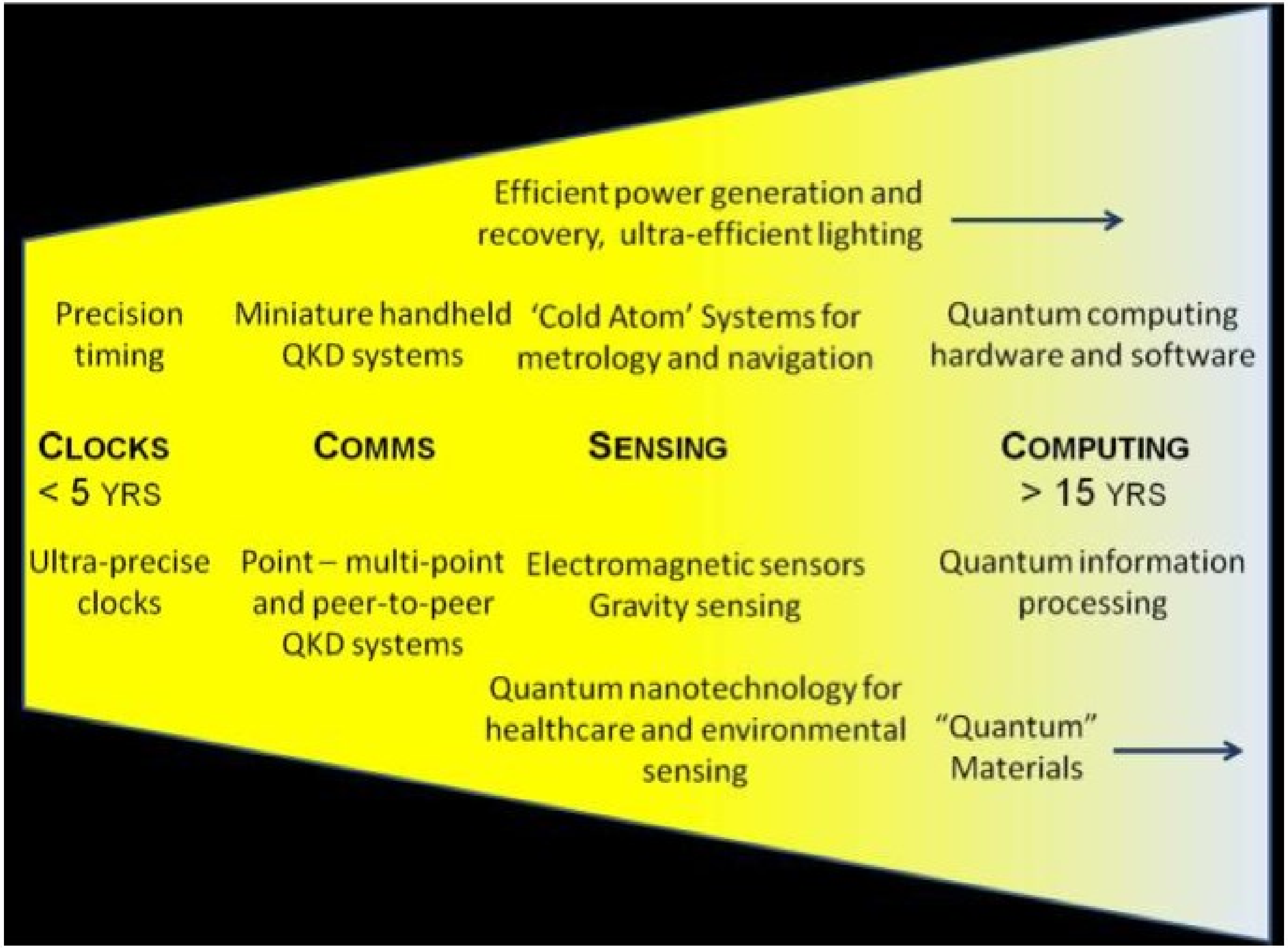
quantum matter can be in two different states at the same time: measurement causes a collapse to one state.

Entanglement



"connection" between separated particles where a measurement of one immediately affects the wavefunction of the other

OK, but you're here to hear about quantum **computing and standards? Not quite…**

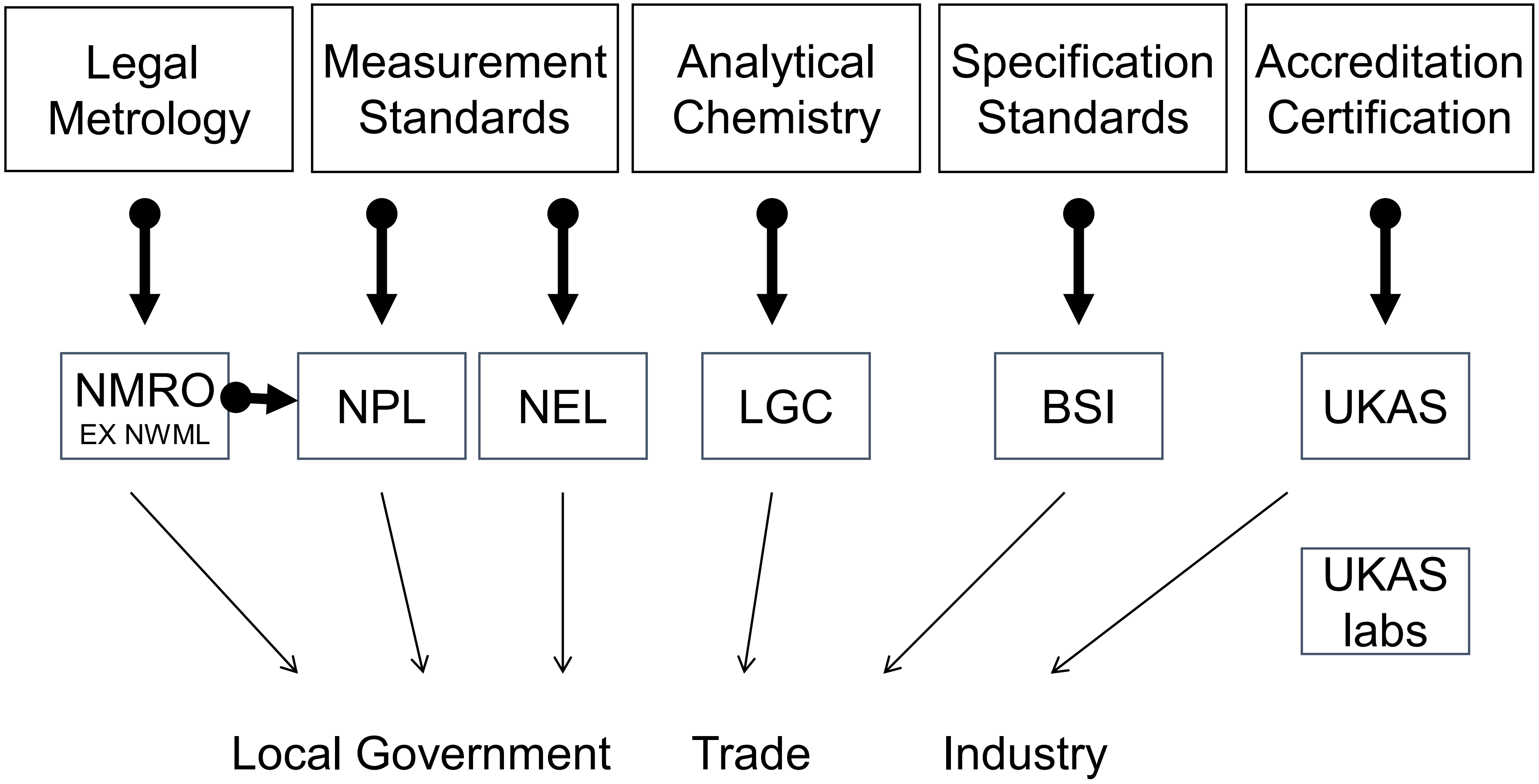


Slide from NPL

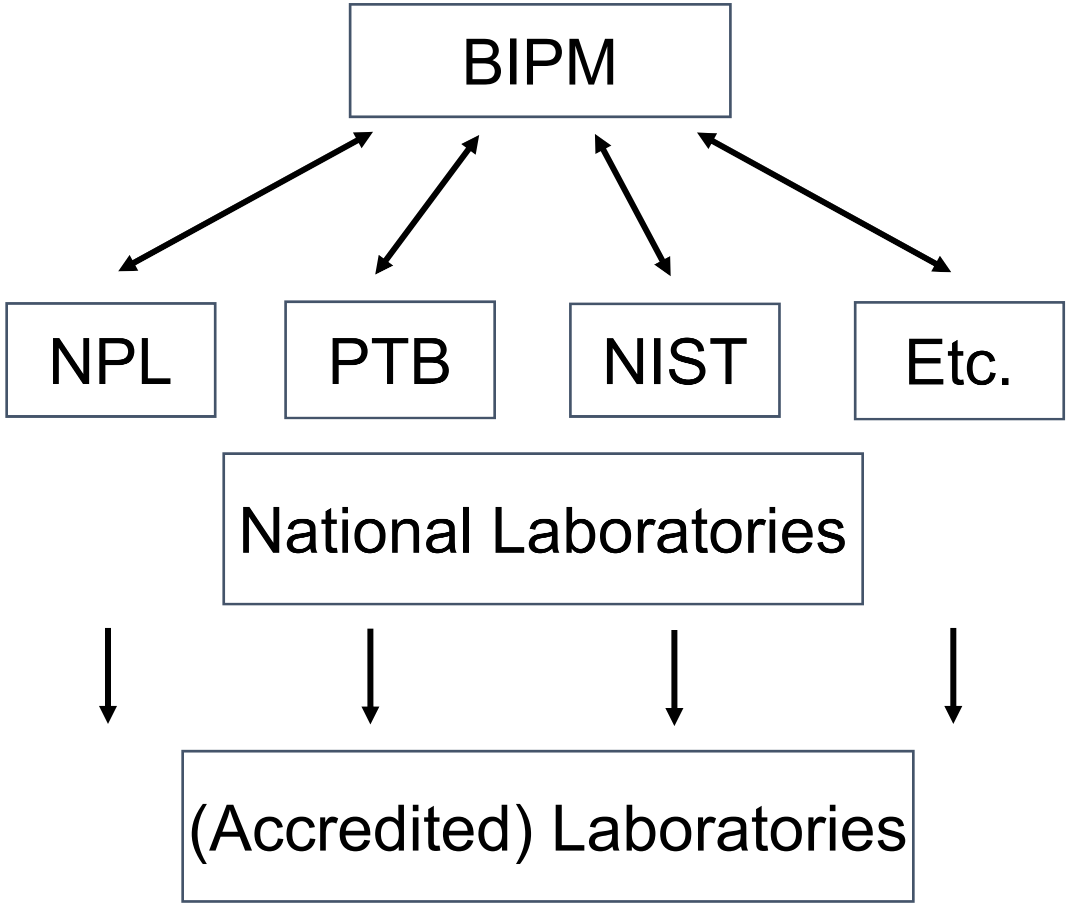
The ‘New’ SI: the underpinning of metrology

- **Builds the SI on the most stable things we know:**
  - Natural Constants
- **Removes uncertainty from *definitions* of the units:**
  - Uncertainties in how units are realised should reduce over time
- **Builds a secure foundation for the future development of metrology**

Metrology in the UK



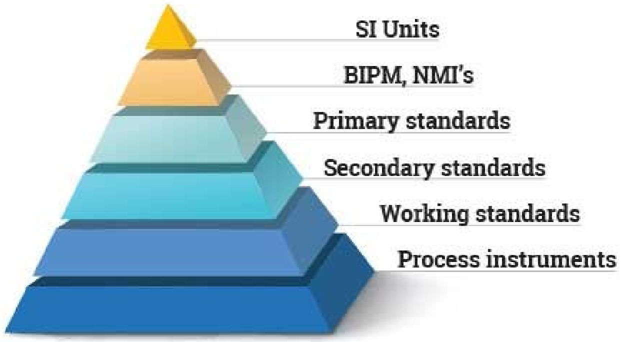
International



Defines the units

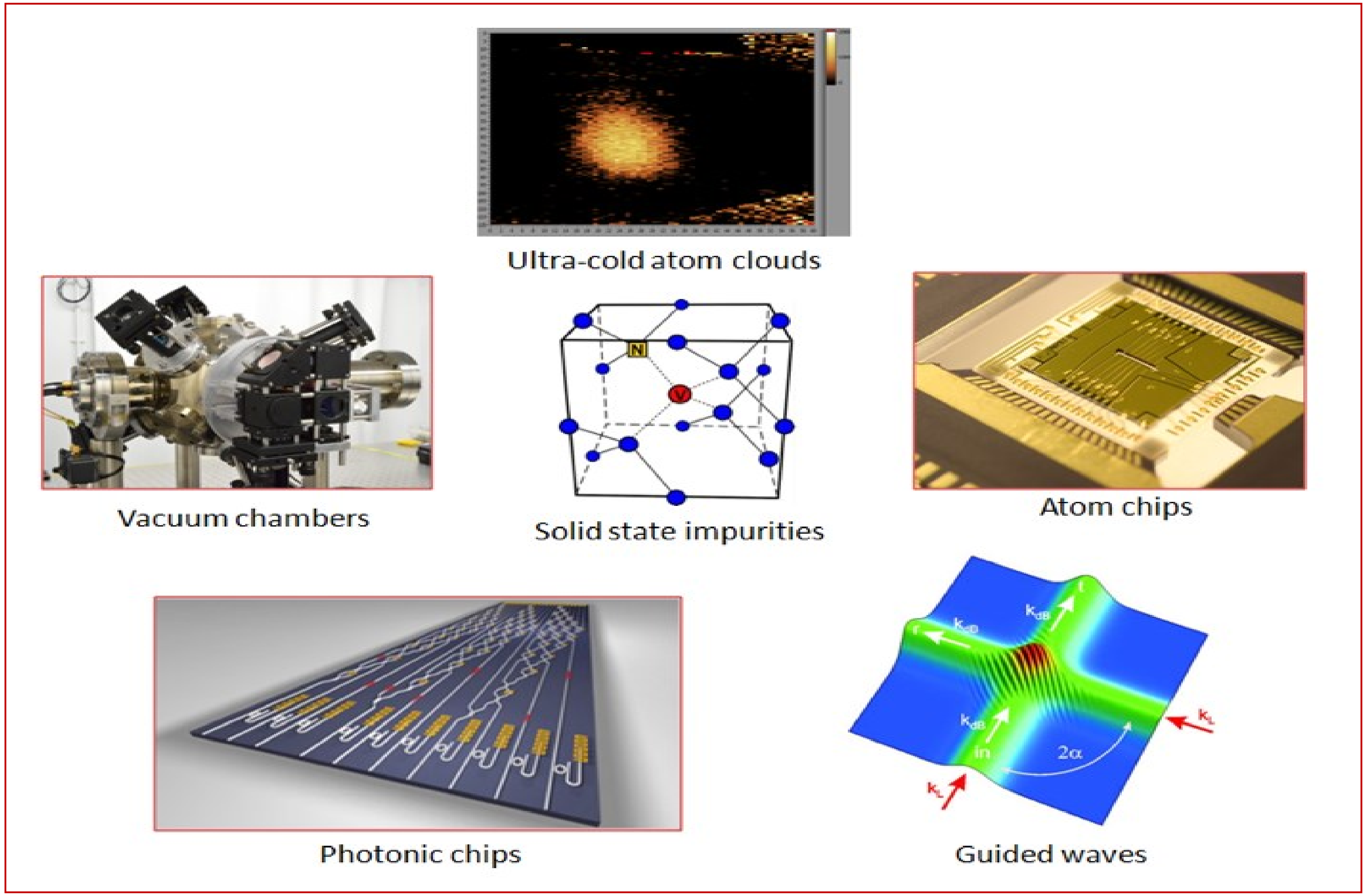
Realise “equivalent” standards

Provide Calibration Services



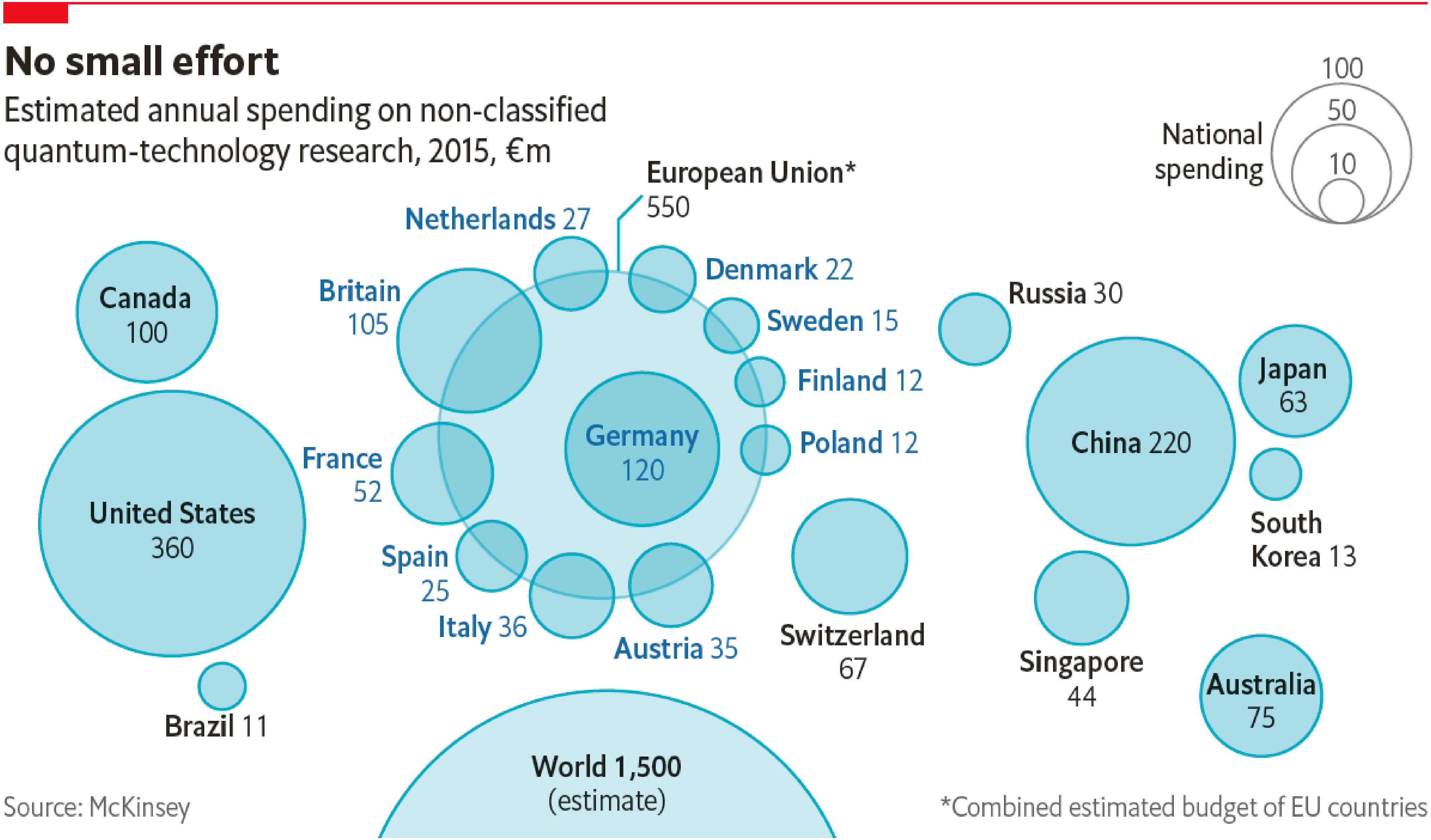
The Quantum Age

- First quantum age gave us lasers, semiconductors…
- Now exploit quantum coherence?
- Impacts multiple sectors
- Enhanced capabilities in timing, sensing, imaging, computing, communications, and more
- Needs to fit with existing infrastructure
- Technology can be faster, cheaper, and higher-performing

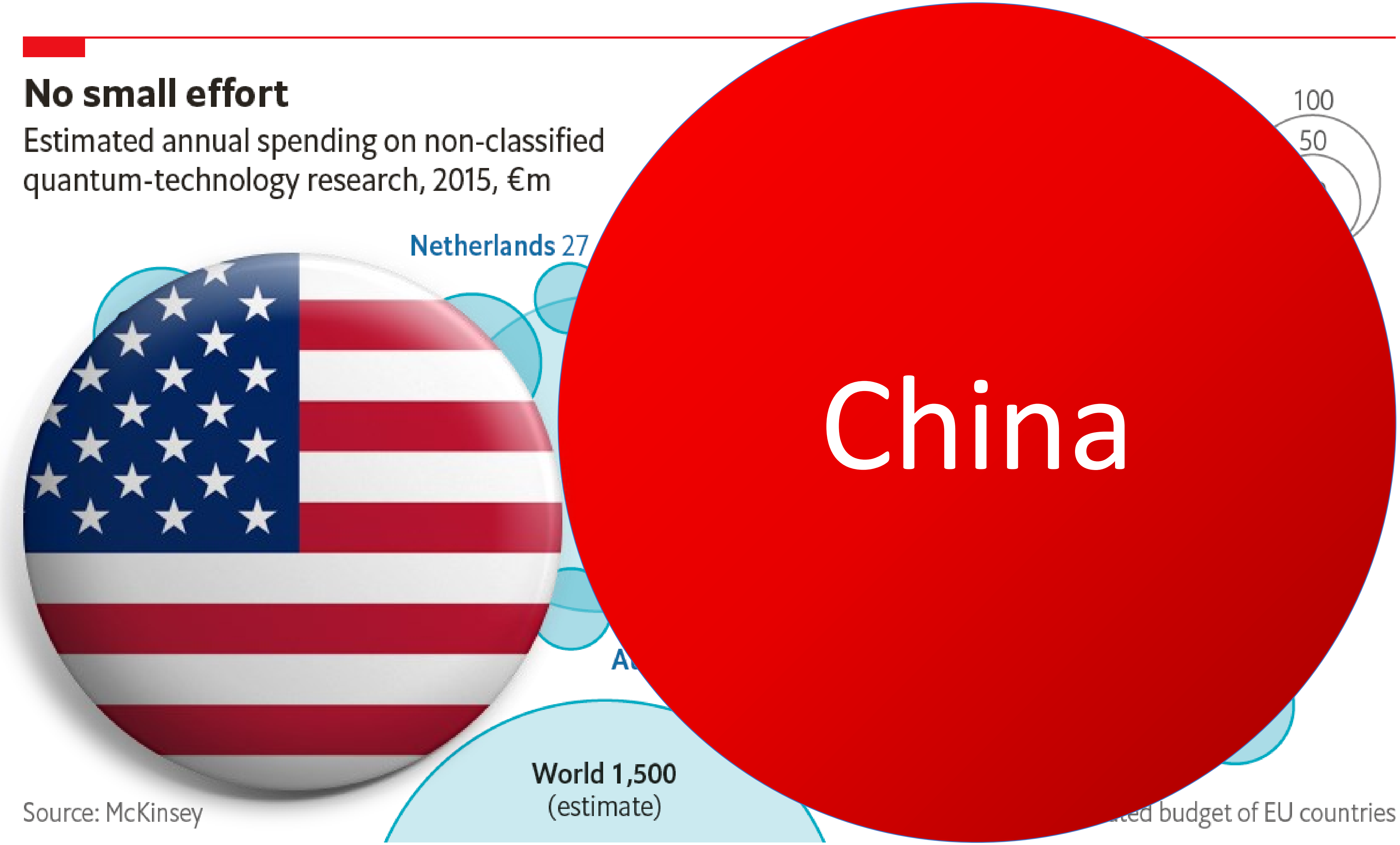


Technologies that enable quantum systems

World-Wide Spending on QuTech — 2015



World-Wide Spending on QuTech — 2018



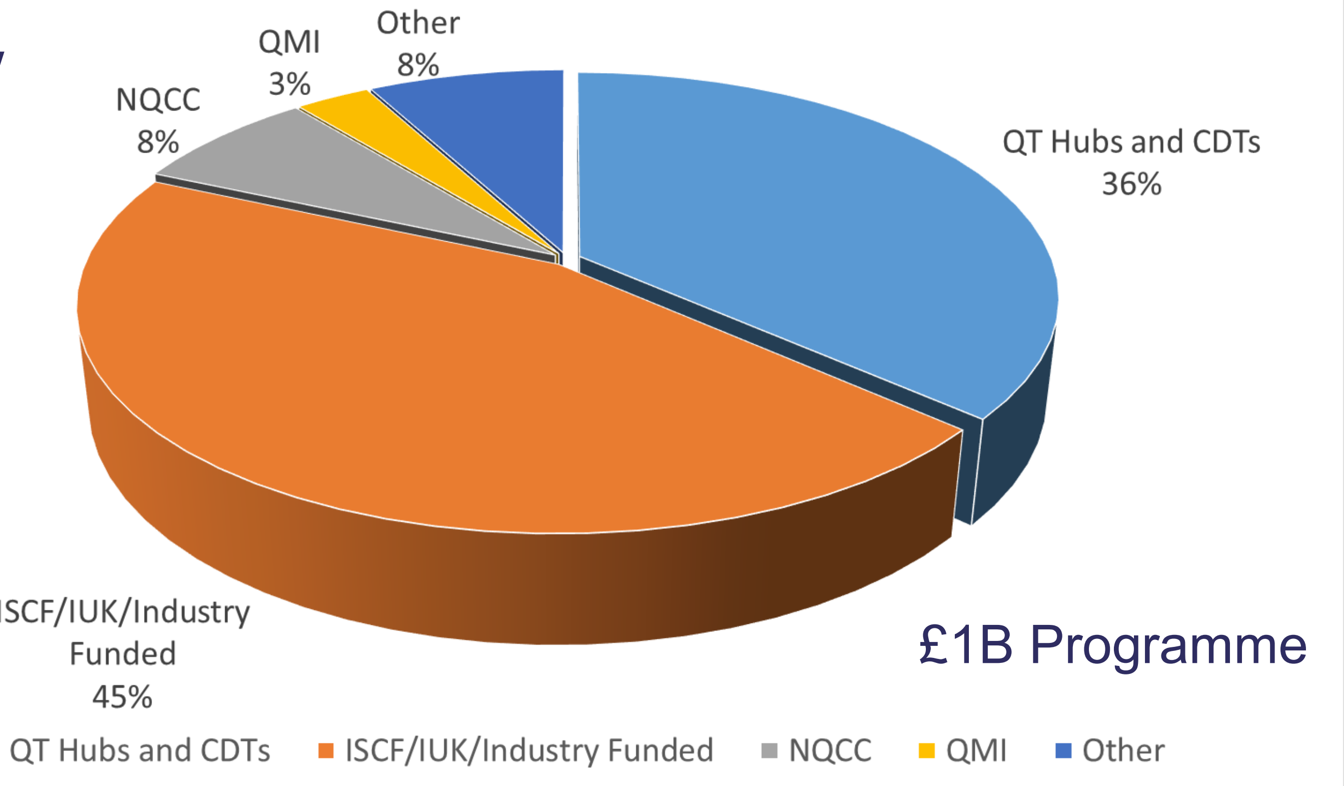
UK government commitment £270M in 2013 has grown……….

INDUSTRIAL STRATEGY

UK Research and Innovation

Phase 1 started 2014 with £270M in 2013 budget, grew to £400M+ by end in 2019; research hubs, skills and industry support

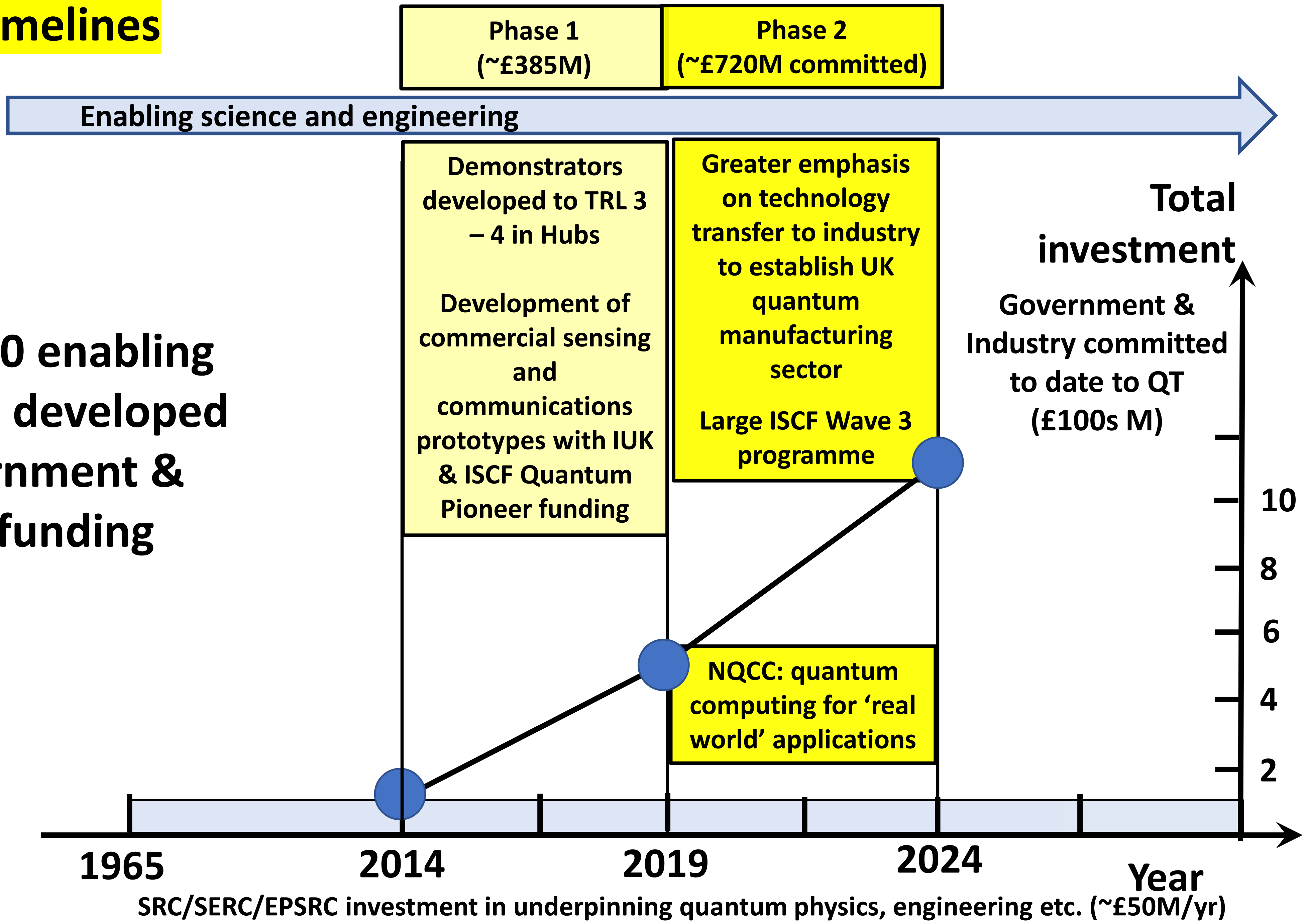
Phase 2 built on this: started 2019-
Hubs renewed (£80M + £15M)
ISCF Waves 2 and 3 (£20M + £153M + £205M Industry)
Skills Package (£67M)
NQCC (£93M+)
International (Singapore with STFC, Canada, Australia)



This is QT: Quantum Science is separately funded especially by EPSRC and STFC

UK funding timelines

Quantum 2.0 enabling technologies developed with government & industry funding

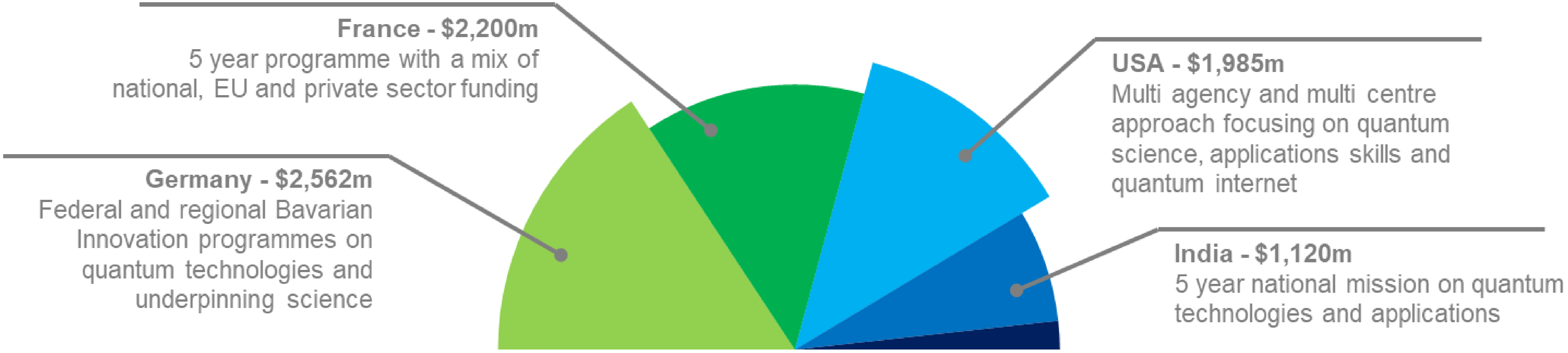


Quantum Programme themes around the world

- **Compact atomic clocks**: for time stamping, flywheels for gps resilience;
- **Quantum metrology and sensors**: where quantum effects such as entanglement or superposition are exploited for highly sensitive measurements;
- **Quantum secure communications:** offer new communication channels, e.g. quantum key distribution (QKD), as well as transmission systems and components that are specific to quantum communications;
- **Quantum simulators**: which enable the accurate modelling of real molecules and materials;
- **Quantum computation**: information processing by using quantum superposition & entanglement
- **To commercialise all this, how can we be assured appropriate standards are in place & our disruptive technology components fit existing infrastructure etc**

2020 Government Announced Investment around the world

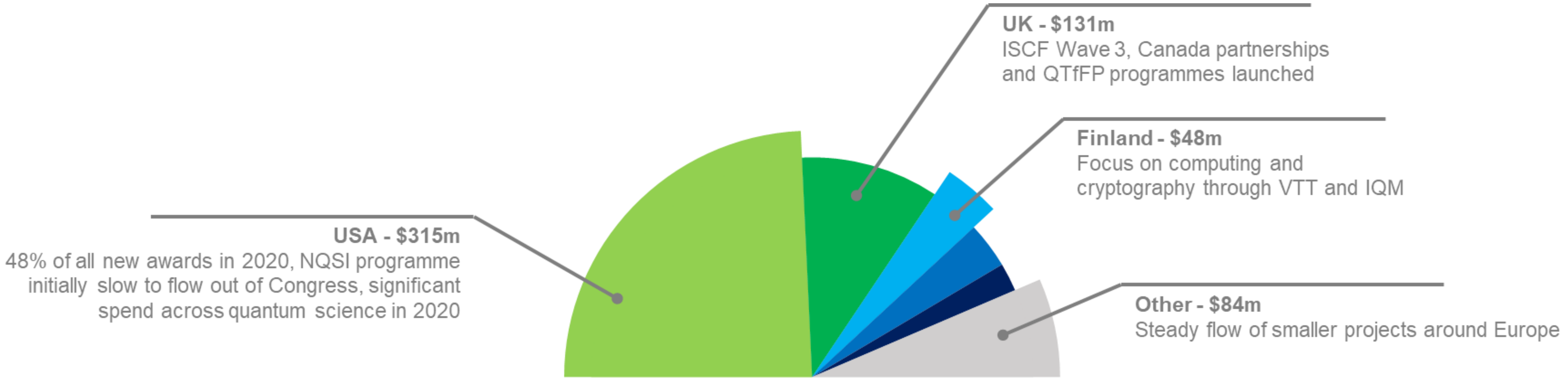
- **$8.2 billion** of new quantum tech funding announced in 2020
    - 59% in Europe, 24% in the US, 17% in Asia

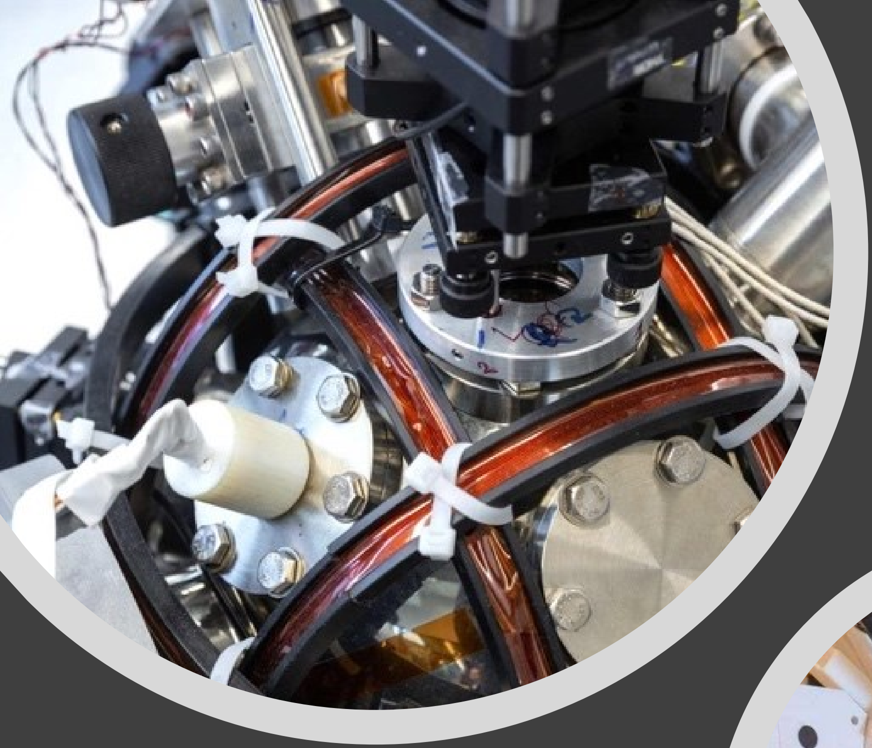


Michael Cuthbert

2020 Government Awarded Investment around the world

- **$649 million** of new quantum tech awards announced in 2020, 48% in the US



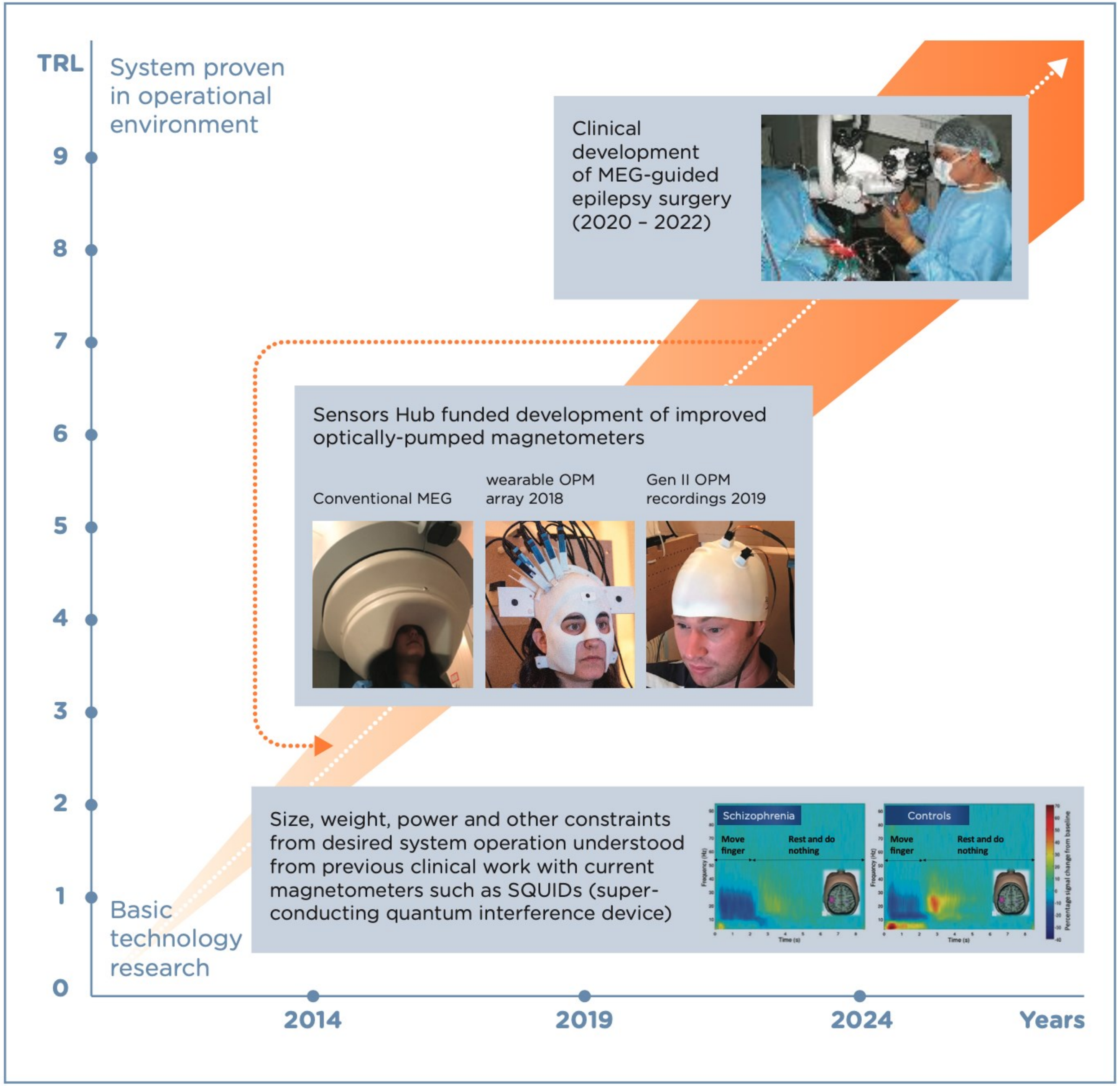


Quantum sensors, timing and imaging

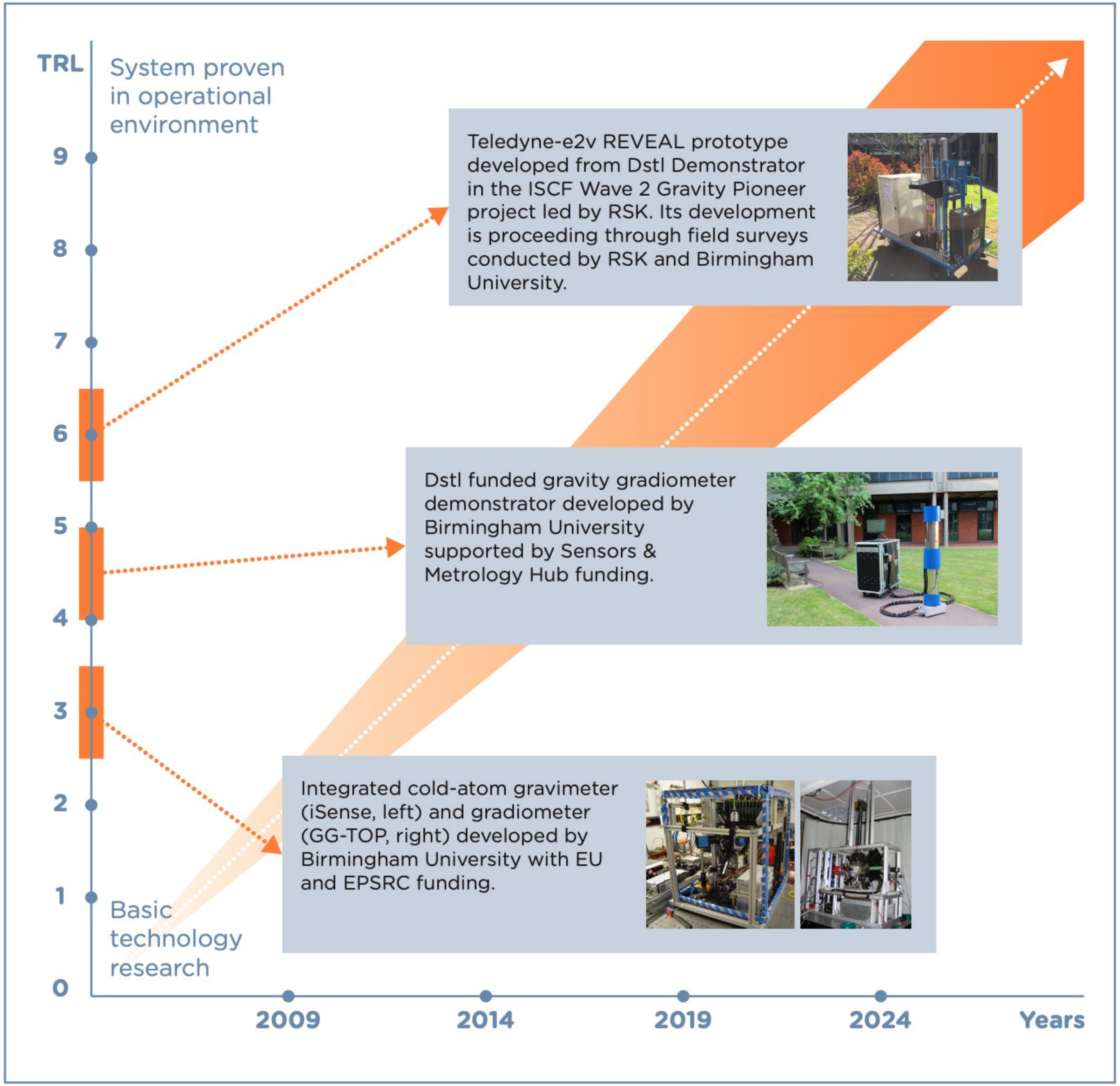
- New time standards and chip scale atomic clocks to address GPS resilience
- The quantum navigator
- Quantum chips for accelerometry, gyroscopes, gravimetry, magnetometry
- Imaging through walls and around corners
- Gravity sensors for oil, gas, minerals and defence
- Electromagnetic field sensors
- Implanted sensors improving health
- Improved magnetic sensing – heart, brain imaging
- Novel cameras with single photon detection for ranging and imaging: “making the invisible visible”
- Seeing without being seen

An example: MEG

UK programme already rolled out to hospitals; Nottingham lead

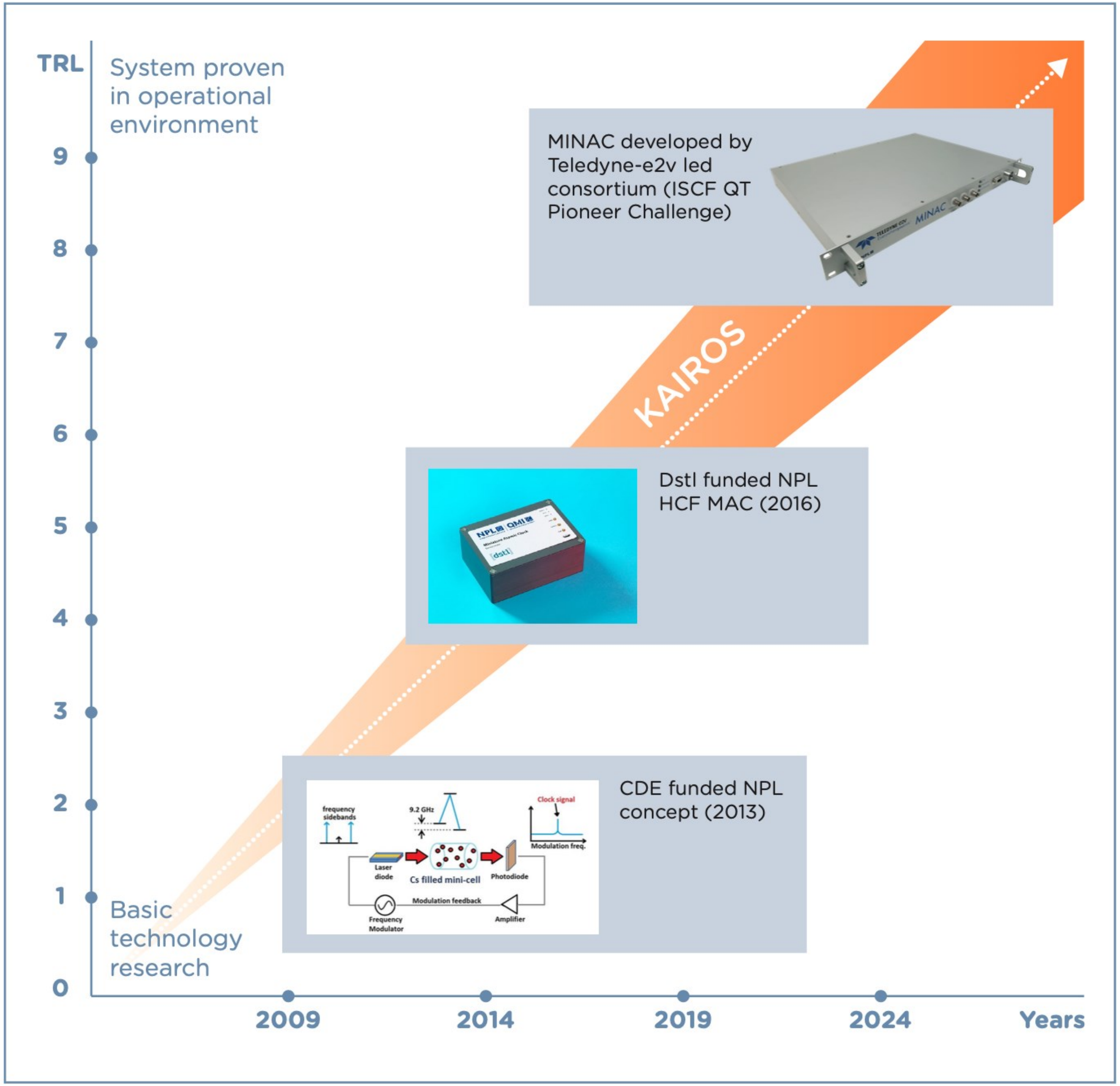


Gravimeters:
This field-deployable gravity sensor will have wide-ranging uses in earth and climate sciences, agriculture and water management, surveying (infrastructure, oil, gas and minerals), and in navigation.



Compact clocks:

Atomic clocks provide highly accurate timing, with applications across a wide variety of technology sectors, including defence and security, aerospace, telecoms, and infrastructure. Atomic clocks can be used to time stamp high-frequency trading transactions in financial markets, ensuring that an accurate record is kept, impervious disruptions.



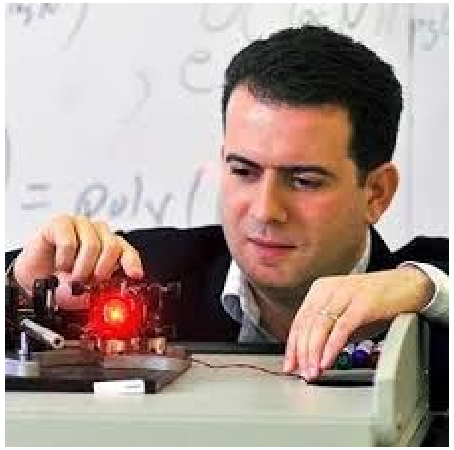
Crypto-apocalypse

- **Information security** and e-commerce are based on PKI use of **NP** problems that are not in **P : factoring**
  - must be“hard”(not in **P**) so that security is “unbreakable “
  - requires knowledge/assumptions about the algorithmic and computational power of your adversaries
- **Quantum algorithms** (e.g., Shor’s factoring algorithm) require us to reassess the security of Public Key systems
- Quantum computers of substance maybe a decade away
- Replace Public Key crypt within a decade- yet this underpins https, ie all of commerce!
- Lessons:
  - algorithms and complexity classes can change!
  - information security is based on assumptions of what is hard and what is possible- better be convinced of their validity!

When worry: Mosca

- **How long does your information require to be secure (x years)?**
- **How long to re-tool existing infrastructure with quantum safe or resistant solutions (y years)?**
- **How long until a large-scale quantum computer is built (z years)?**

Mosca's Theorem: If x + y > z then worry

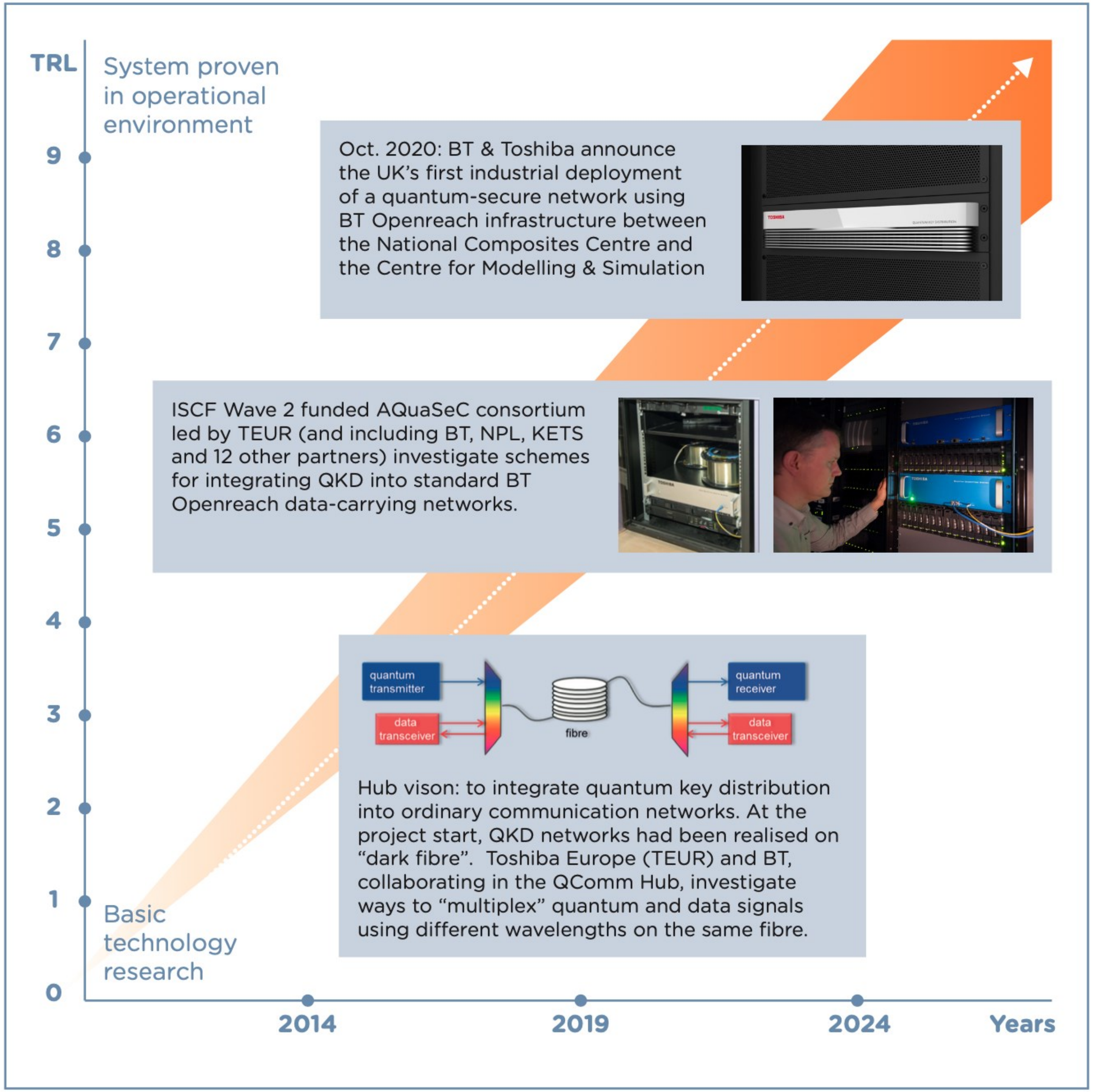


Quantum comms:

Improvement in secure transmission of information is important for government, businesses and individuals. Public (shared) key cryptographic systems, based on current cryptographic algorithms using one-way functions, will become vulnerable to attack by future quantum processors.

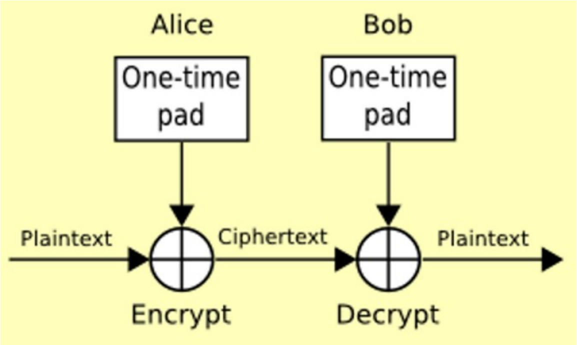
Quantum key distribution is a provably secure (provided certain system vulnerabilities are protected), mature quantum technology for the secure transmission of encryption keys. The UK is developing a number of approaches to this technology, including chip scale, portable QKD-based devices which are robust, cost-effective and, through mass manufacture and integration into conventional technologies, commercially viable.

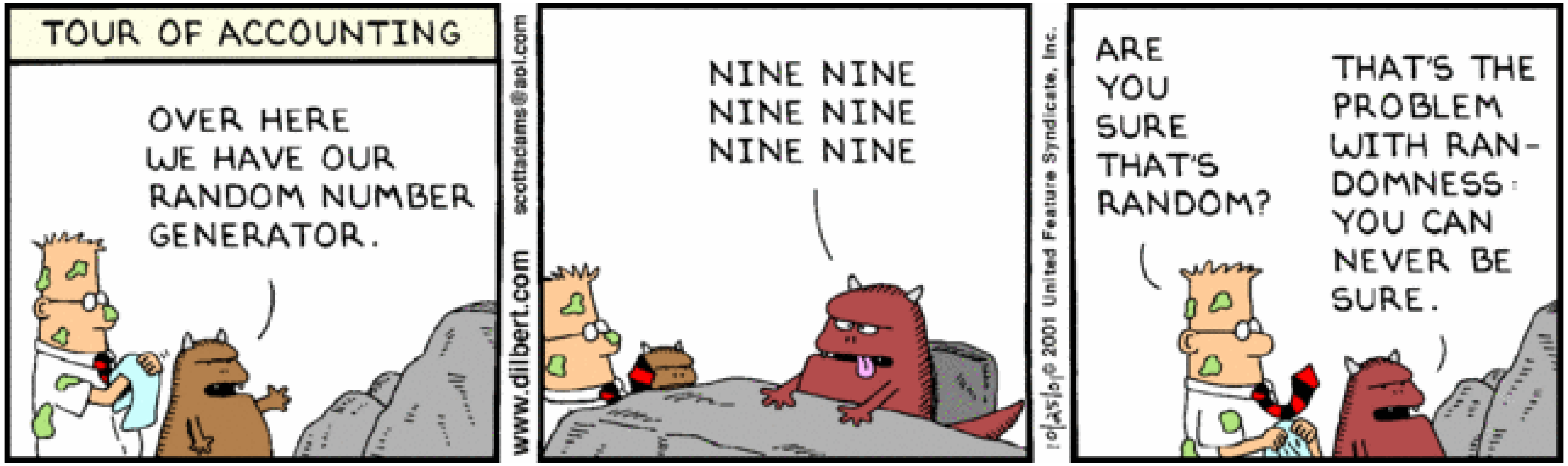
QKD-based communications systems are expected to find widespread use in the world's future secure communications infrastructure.



Quantum security: how guarantee reliability?

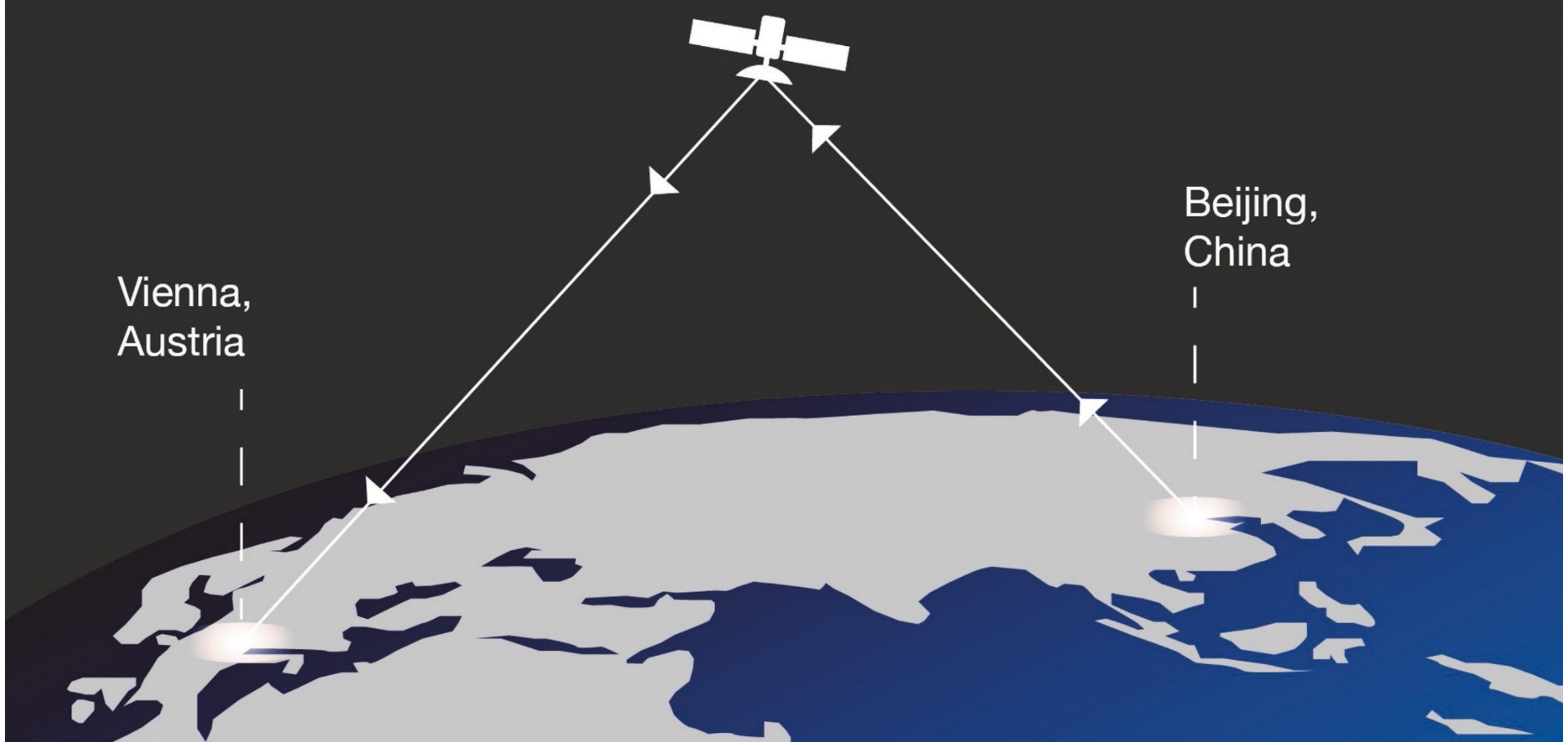
- Use shared random numbers to develop a one time pad
- Classical physics isn't random
- So use quantum
- How do you know its random
- Testing, validation & standards





China: Quantum Communication

China launched a satellite, called Micius, in August 2016 for a space-based quantum communication test bed. It reported a successful quantum communication links from China to Vienna via the satellite in June 2017.

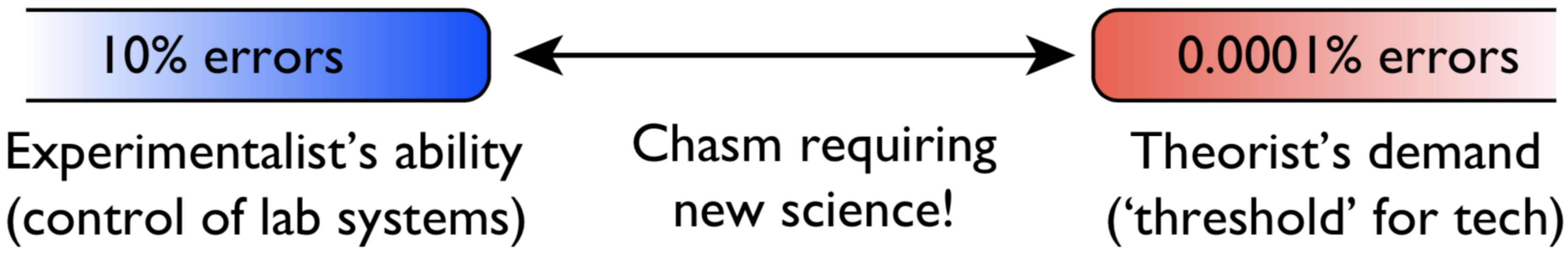


China demonstrated quantum key distribution over 32 trusted nodes along a 1,240-mile optical fiber route in September 2017.

Schroedinger's Engine-Basic idea of Quantum Computing

- Computation with n Qubits.
- Main difference: build **coherent superposition** of states
- State space grows exponentially with number n of qubits: 2^n
- Behaves like a massively parallel computer
- Solves problems in much fewer steps in carefully constructed algorithms: see https://quantumalgorithmzoo.org

How did things look in 1996?



Q: How long will it take to close a 'performance gap' of a factor of 10,000?

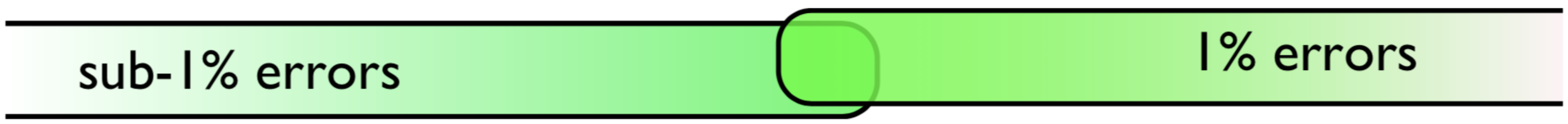
No one knew! But many people guessed!

"A few years." "Many decades." "Never — it's impossible!"

How do things look now?

The theorists have found better and more practical ways of protecting qubits.

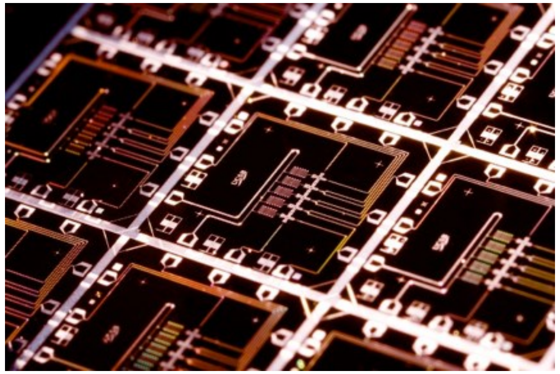
The experimentalists have massively improved the levels of control that are possible.



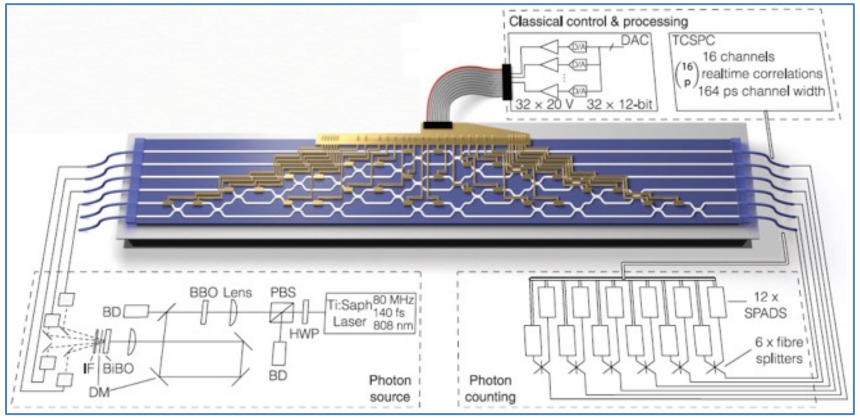
Q: How long will it take to close a ‘performance gap’ of a factor of 10,000?

About two decades, apparently!

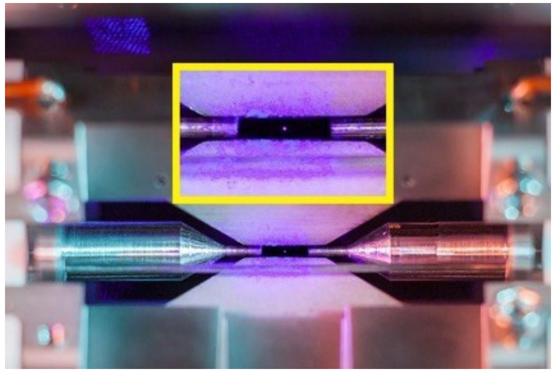
Quantum Computer Hardware Startups



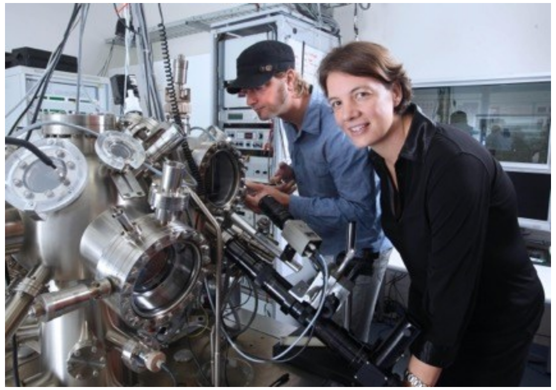
Superconducting
Intel, IBM, Google, Rigetti



Optical : Xanadu, PsiQuantum (Imperial cofounder), ORCA (Imperial co-founder)

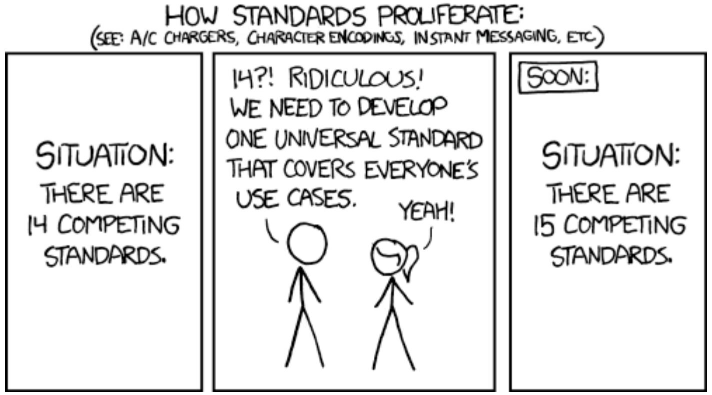


IONQ OXFORD IONICS



Semiconductor
Silicon Quantum Computing

Compatibility, interoperability

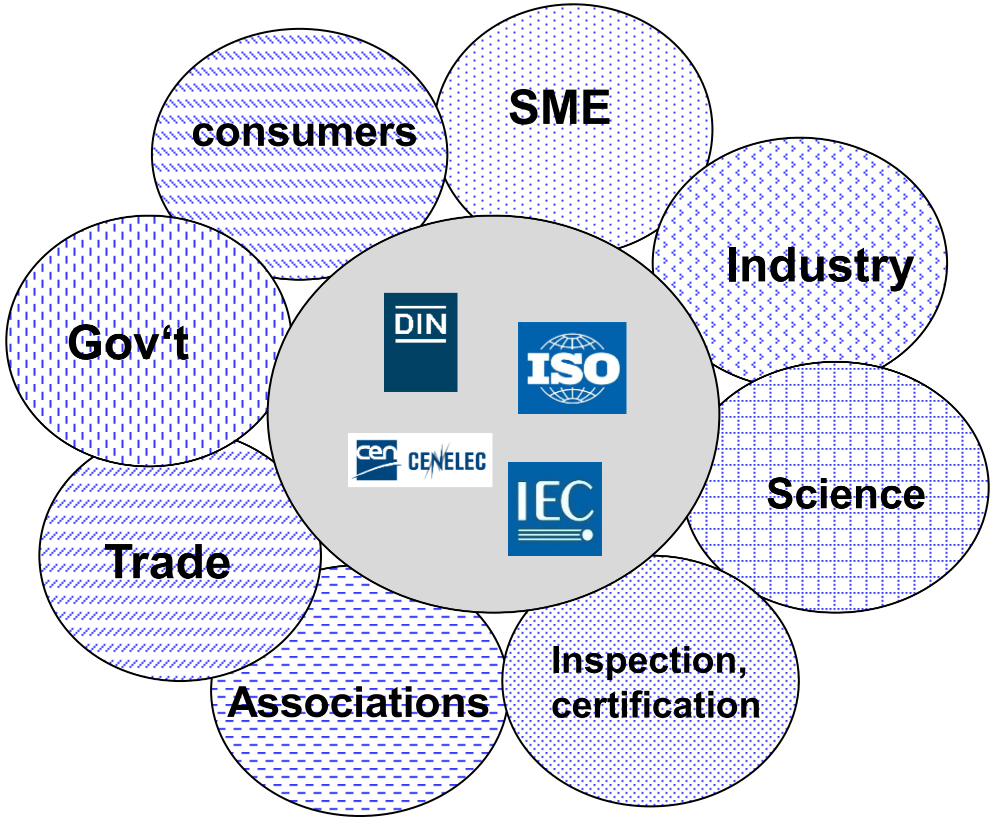


Standards require agreement

- *An agreed, repeatable way of doing something.*
- *It is a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition.*

Standards are **voluntary** reference documents that reflect any agreed issues between parties

Interested Parties



Picture: Joachim Lonien
Brussels, 2019-03-28

First measurement 'standard' for a Quantum Technology

Defined procedures for calibrating QKD hardware are essential for security assurance and supply chain provision

Document:

- Specifies performance parameters and 15 procedures for traceably calibrating quantum-layer components in QKD systems (138 pages)
- Published May 2016

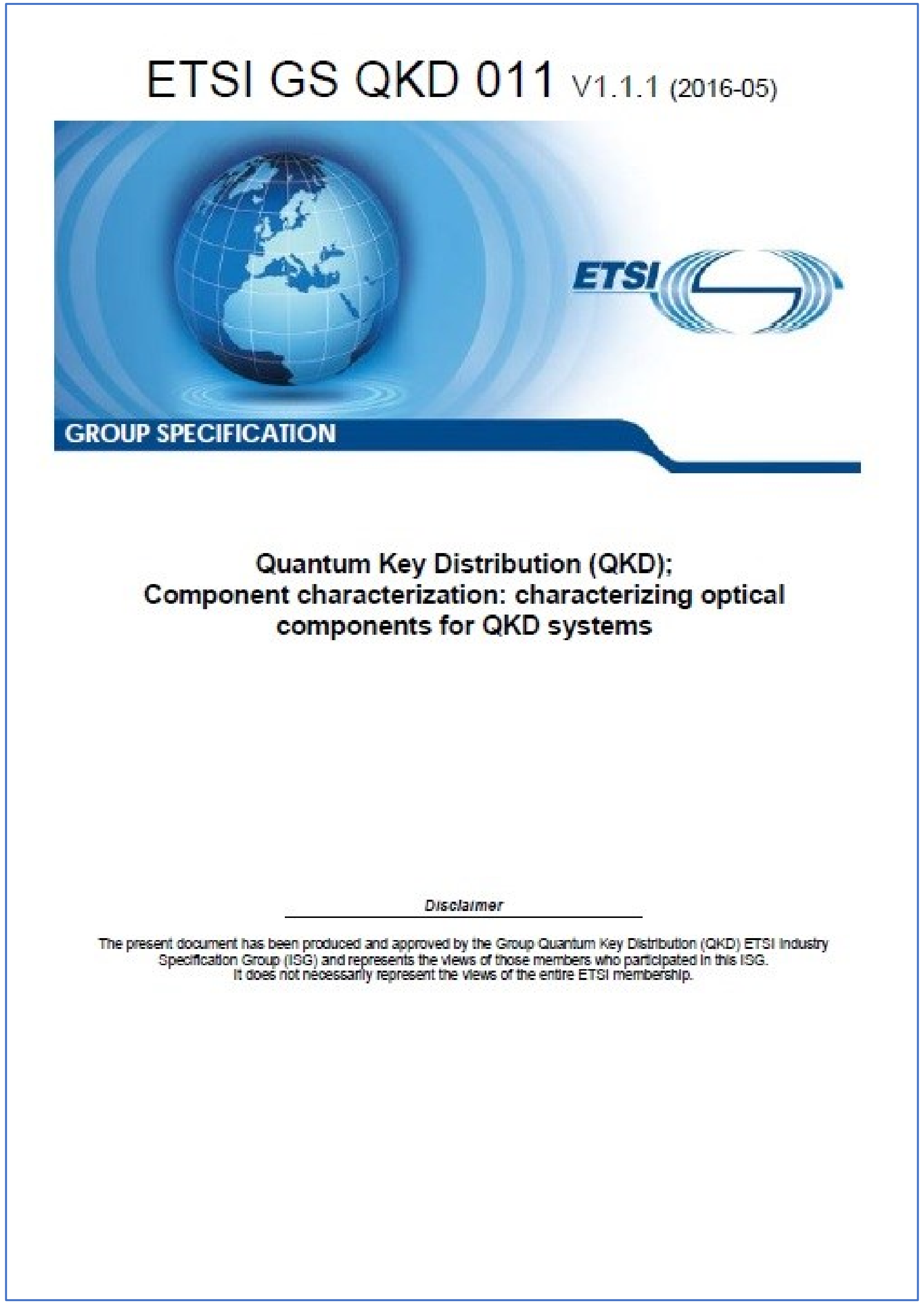
Effort:

- 2 years to compose, based on earlier preparatory work

Authors:

NPL (UK – Rapporteur), Applied Communications Sciences (USA), Austrian Institute of Technology (Austria), INRIM (Italy), JRC Ispra (European Commission), NTT (Japan), NIST (USA), PTB (Germany), Toshiba Research Europe Limited (UK), University of Waterloo (Canada).

Slide courtesy of Rhys Lewis, NPL



ETSI GS QKD 011 V1.1.1 (2016-05)

Quantum Key Distribution (QKD);
Component characterization: characterizing optical components for QKD systems

Disclaimer

The present document has been produced and approved by the Group Quantum Key Distribution (QKD) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Financial regulation – EU requirements for time stamping of trades

- Markets in Financial Instruments Directive II
  - Traceability to UTC
  - HFT algorithm 100μs to UTC, 1μs resolution
  - Electronic 1ms to UTC, 1ms resolution

esma European Securities and Markets Authority

  - operators of trading venues and their members or participants are required to synchronise the clocks they use for any reportable events with UTC (Article 50 of Directive 2014/65/EU and Article 1 of Commission Delegated Regulation (EU) 2017/574)

3rd Jan 2018

Slide courtesy of Rhys Lewis, NPL

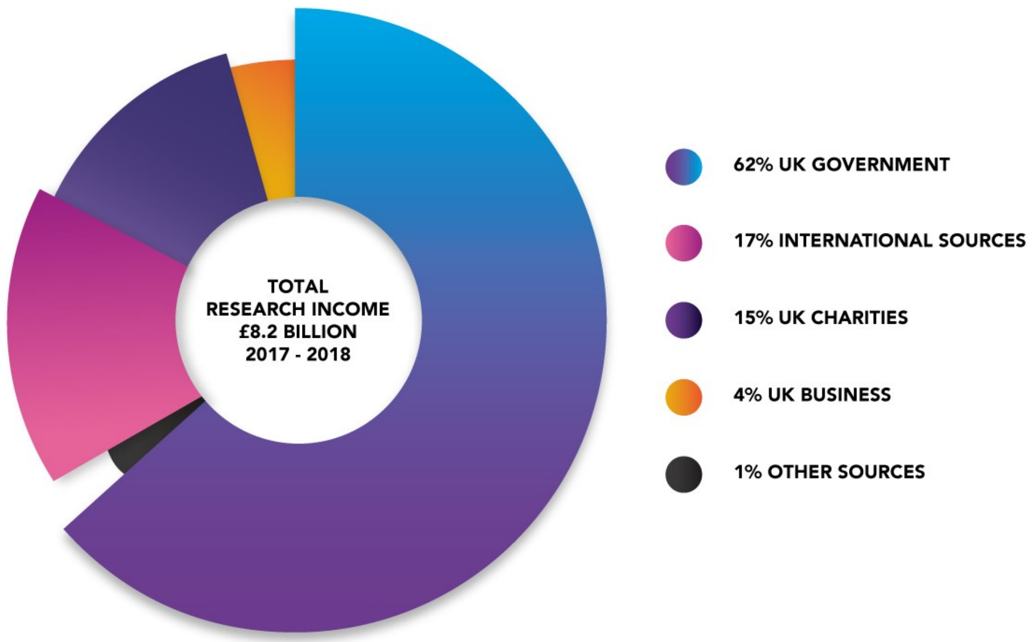
From JRC 2020 Report #Standards 4Quantum Making Quantum Technology Ready for Industry

- I quote: Discussed “how to bring inventions to the market, thus completing the pathway of innovation. Planning at an early state and incorporating standardisation can be crucial for accelerating market uptake of research findings.
- Technologies built on the basics of quantum mechanics, occurring on an atomic scale, are approaching markets with the promise to create many new businesses and help solve many of today’s global challenges. These applications will be a pivotal factor for success in many industries and markets. Some of these applications are of strategic importance to Europe’s independence and safety, i.e. in the field of secure information storage and transmission or in creating new materials for energy solutions and medicine.
- CEN and CENELEC recognized that in their ranks no Technical Committee or Working Group follows a Quantum technology specialisation. The Standards Organisation expressed concerns about a potential lack of standardisation activities around industrial products that are based on Quantum technology. ”

In Quantum: international agreement of documentary standards

- In the UK: new Digital Standards team, led by DCMS within Digital Technology Policy Directorate; includes HMG bodies, BSI, NPL.
- UK NQTP Hubs in York, Glasgow, Birmingham and Oxford plus NQCC all engaged. See eg https://www.quantumcommshub.net/wp-content/uploads/2020/09/QCH-Standards-for-Quantum-tech.pdf
- In quantum computing: ISO/IEC JTC1/WG14 established including NPL
- In Europe: CEN-CENELEC Focus Group on QT set up in June '20 including NPL to generate roadmap for standardization activities in Europe and mirrors the H2020 Quantum Flagship. Also European Metrology Network for Quantum Technologies (EMN-Q) for NMIs roadmapping work; NPL involved- Rhys Lewis is UK vote holder plus…
- IEEE standards work: P7130 in QC terminology; another on benchmarking and performance specs: I don't know about UK involvement. https://quantum.ieee.org/standards. The following quantum standards efforts are now active:
  - P1913 - Software-Defined Quantum Communication
  - P7130 - Standard for Quantum Computing Definitions
  - P7131 - Standard for Quantum Computing Performance Metrics & Performance Benchmarking

International Nature of Research



- A fifth of the world's scientific papers are produced through international collaboration: these partnerships play a vital role in scientific progress, and this has implications for IP and commercialisation.
- The UK champions a rules-based system, which has served our interests as a global nation.
- This system has enabled global cooperation to protect shared fundamental values of respect for human. For academia this is demonstrated by the importance the UK places on the protection of academic freedom, something enshrined in law.
- Universities in the UK work closely with partners from across the world - more than half of UK research is a product of international partnerships. These international relationships extend further than research funding and collaboration; 42% of postgraduates and 31% of staff in universities are from outside the UK.
- Developing and maintaining these international relationships is key to the success of research and innovation.

Quantum Nationalism

- Quantum technology builds on a great quantum science base which critically depends on international collaboration and open sharing of ideas.
- But governments invest heavily for local strategic and economic advantage, which may well affect openness.
- We see increasing signs of barriers being erected to international collaboration in quantum science and technology around the world in national programmes (eg in the EU, USA and elsewhere).
- This may well affect the collaboration needed for world-wide appropriate standards

What's the Role of the UK National Measurement System?

- Makes sure UK standards meet industrial needs
- Represents UK on international metrology bodies
- Provides traceable measurement for all users
- Enables manufacturers to comply with legislation, trade requirements, etc
- Does what companies can't afford to do themselves
- Provides services to companies
- Raises awareness and encourages better measurement

NMS Programme Objectives:

- to maintain and develop national measurement standards at a level consistent with the current and future needs of the UK;
- to ensure that UK measurement standards are harmonised with those of UK's trading partners, through inter-comparisons and collaborative research leading to mutual recognition;
- to develop new methods of measurement to meet identified UK business and public sector needs, and promote international standardisation of these methods;
- to promote knowledge transfer from the programmes, and to provide technical support and advice to UK businesses and individuals undertaking accurate measurements.

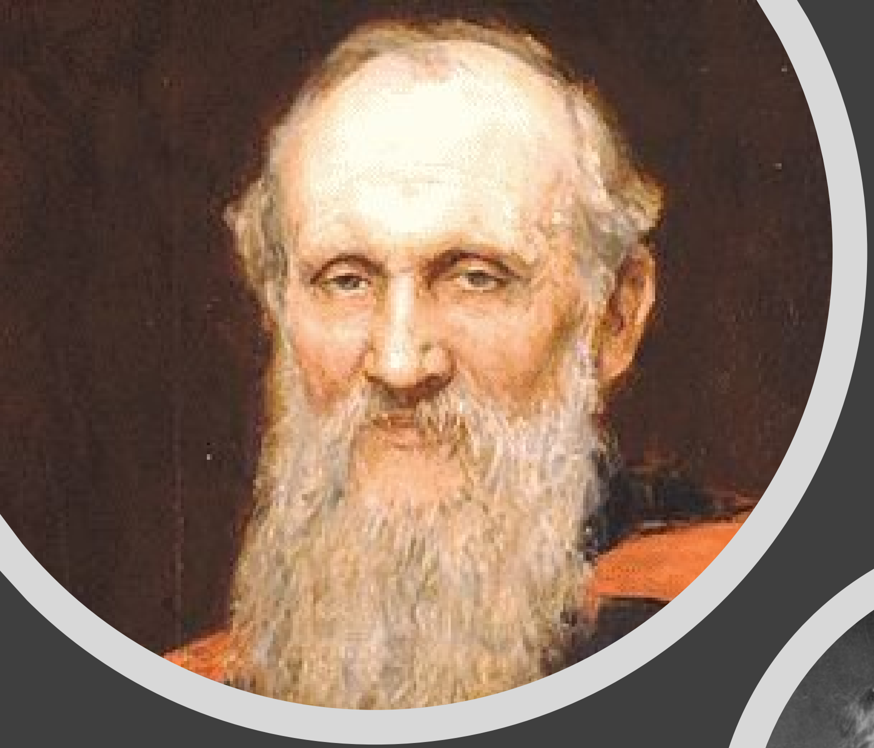
Some historical context to finish:

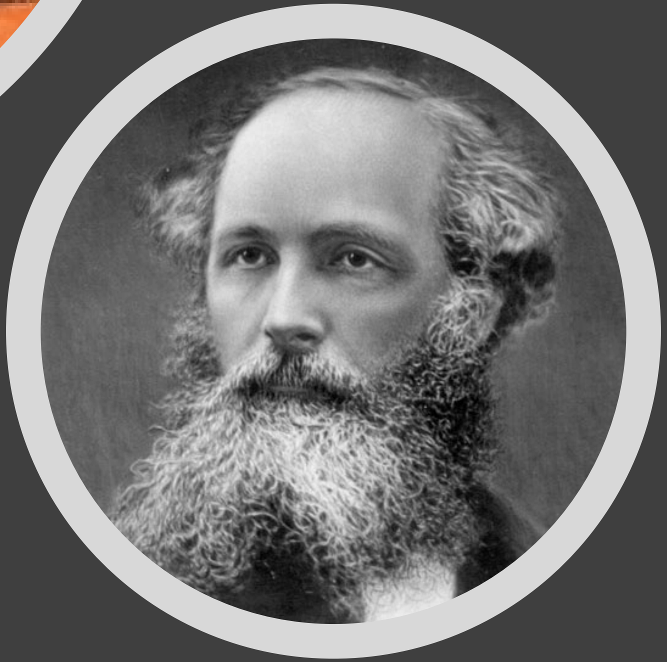
Why do you need accurate measurement?

- Industry and society rely on it without thinking
- So scientific measurements can be reproduced and are reliable
- To maintain international trade
- To reduce fraud

Magna Carta - 1215

"There is to be one measure of wine and ale and corn within the realm, namely the London quarter, and one breadth of cloth, and it is to be the same with weights."





Measurement has always been important
The bearded savants

- "The Lord abominates a false balance, but a just weight is His delight" *(Proverbs 11:1)*

- "There shall be one measure throughout the realm" *(Magna Carta)*

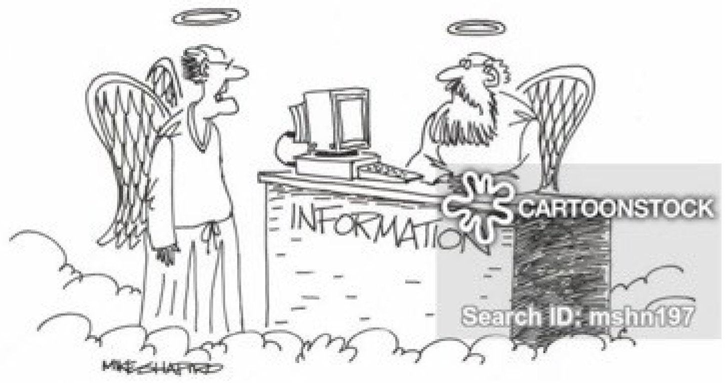
- "You can only make as well as you can measure" *(Whitworth)*

- "When you can measure what you are speaking about and express it in numbers you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge of it is of a meagre and unsatisfactory kind" *(Lord Kelvin)*

- "If, then, we wish to obtain standards of length, time and mass which shall be absolutely permanent, we must seek them not in the dimensions, or the motion, or the mass of our planet, but in the wavelength, the period of vibration, and the absolute mass of these imperishable and unalterable and perfectly similar molecules."

- James Clerk Maxwell, 1870

Messages for today



"I still don't understand quantum theory."

- My key foci:
  - Transformative technology being demonstrated
  - The international picture of rapidly increasing interest and investment
  - Real technology,
- Questions to bear in mind for today:

  How do we agree appropriate standards to ensure effective roll out of this disruptive technology?

  - Where should we focus efforts for fast and valuable outcomes?