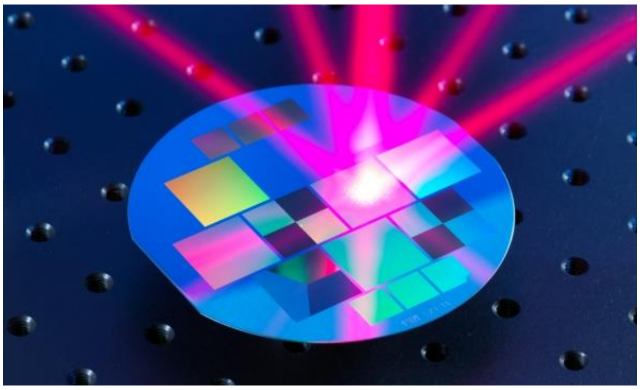
HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 552 April 2017

Quantum Technologies



Quantum technologies use the behaviour of matter and light that is normally only observed at very small scales. Some technologies build on established approaches, while others are totally new. This note introduces recent advances, applications, and UK initiatives to support their development and commercialisation. It also reviews policy concerns such as privacy, access to new technologies and secure communications.

Overview

- Estimates suggest that quantum technologies could become comparable in size to the consumer electronics sector.
- Quantum technologies have many potential uses including in navigation, health, telecommunications and oil and gas exploration. Trade in some technologies could be limited by export controls.
- A new generation of quantum technologies are becoming commercially available, others may take over a decade to develop.
- Quantum technologies may have implications for privacy.
- Universal quantum computers, which could run any quantum algorithm (sequence of calculations), would undermine current encryption that protects sensitive data; organizations are advised to prepare for new encryption systems.

Background

At very small scales, the classical laws of physics break down and the laws of quantum mechanics take over. Scientists have found ways to exploit the behaviour of matter and light at the level of atoms to create, for example, the technologies that underpin lasers, cameras and computers.[1] Now, the ability to measure and manipulate individual atoms and other particles, is enhancing existing technologies and leading to a new generation of quantum technologies.[1]

The Government Office for Science has said that in the long term, quantum technologies could be comparable in size to the consumer electronics sector, currently worth an estimated £240bn a year globally.[1] The UK's quantum technologies community has suggested that the emerging quantum industry could create hundreds or thousands of high value jobs in the UK.[2]

Quantum technologies are being developed in the UK and internationally.[1,3] In 2013, the UK Government announced funding of £270m (over five years) to create the National Quantum Technologies Programme (Box 1).[4,5] Other funding has included £36m from the Ministry of Defence (MoD), and total investments from public and private sources now exceed £350m.[1,2] Quantum technologies were identified as a possible recipient of further funding in the Government's recent green paper: Building our Industrial Strategy.[6]

The UK's National Strategy for Quantum Technologies stated in 2015 that it is important for the UK to support international collaboration as a means to attract the best talent and inward investment, and to access a wider range of customers and markets.[7] In 2018, the EU aims to launch a ten-year, €1bn European Flagship programme to support the development of quantum technologies.[8,9] It is unclear if the UK will negotiate participation in the programme after leaving the EU. Existing Flagships include both EU and non-EU Members such as Turkey, Israel and Switzerland.[10,11]

Technologies

In the UK, the research and development of quantum technologies focuses on: timekeeping, sensing, imaging, communications and computing.

Timekeeping

Clocks use a periodic event (e.g. a swinging pendulum) to measure time. Atomic clocks use the oscillations of electrons within atoms as their fundamental ticking.[12] They

The Parliamentary Office of Science and Technology, Westminster, London SW1A 0AA; Tel: 020 7219 2840; email: post@parliament.uk www.parliament.uk/post

Box 1. The National Quantum Technologies Programme
The UK's National Quantum Technologies Programme aims to accelerate commercialisation by creating a coherent community across Government, industry and academia.[7] It involves over 130 companies, 17 universities and various government agencies. Four research hubs (led by four universities) have been created to support collaboration and to provide facilities and training.[5]

- **The Quantum Enhanced Imaging Hub** (University of Glasgow) is creating new types of cameras and optical sensors.
- **The Sensors and Metrology Hub** (University of Birmingham) is developing a range of quantum sensors, clocks, associated components (e.g. lasers) and manufacturing methods.
- **The Networked Quantum Information Technologies Hub** (University of Oxford) aims by 2020 to prototype the basic components of a quantum computer, which may eventually be scaled-up to produce a universal quantum computer (Box 3).
- **The Quantum Communications Hub** (University of York) is miniaturising transmitters and receivers, and is trialling secure quantum communications on fibre optic networks between Bristol and Cambridge. A further link is planned between Ipswich and Cambridge, to create a network spanning southern England.[13]

have been used since 1967 to determine Coordinated Universal Time (UTC), a standard timescale used world-wide.[14] Atomic clocks on-board satellites are also a crucial part of global navigation satellite systems such as GPS.[15] New techniques have been developed over the past decade to improve the accuracy of atomic clocks, for example involving different types of atoms, or the use of a quantum behaviour known as entanglement (Box 2).[12,16,17] The best atomic clocks lose or gain less than a hundred trillionth of a second per year.[18] Research is focusing on improving the performance and reducing the size, weight and cost of miniature atomic clocks (which cost about £1,200 and are the size of a matchbox).[2,19] The performance of the most accurate clocks is also being improved and verified.[20]

Sensing
Quantum sensors can measure gravity, magnetic fields, electric fields, and the acceleration and rotation of objects with greater sensitivity, accuracy and stability than conventional sensors.[1] Many of them utilise quantum behaviour such as superposition and the wave-like properties of atoms (Box 2).[21] Quantum gravity sensors are in the early stages of commercialisation; the first model was launched in 2010.[1,22] They can, for example, be used to map the location of tunnels or pipes underground. They could reduce survey times compared to conventional gravity sensors and could detect and characterise objects at ten times the depth possible at present.[1,23]

Imaging
Advancements in imaging technology are improving the ability of cameras to detect individual photons (particles of light), increasing sensitivity and image quality.[1] This allows:

- **3D imaging** – by mapping the time that photons take to reach different parts of an object and return to the camera, it is possible to determine depth.[1]
- **imaging around corners** – by using light that bounces off walls, floors or other rough surfaces (as if a mirror), it is possible to track an object behind an obstacle.[1]
- **trans-wavelength imaging** – by using quantum entanglement (Box 2) to associate two different beams of light, it is possible to illuminate an object with one beam (which never reaches the camera), while capturing an image of that object using the other beam (which never interacts with the object).[24] This varies from conventional imaging, in which a single beam of light illuminates the object and is reflected back to the camera. If each beam has a different energy (colour), trans-wavelength imaging could be used to illuminate a biological sample with low energy light (to avoid damage) while making a high-resolution image of the sample with higher energy light (that is easily detected with conventional sensors).[24]

Communications
Quantum systems have characteristics that lend themselves to sending information securely. Typically, they encode information in individual photons, producing a binary sequence of data sent via conventional fibre optics.[25] The photons cannot be measured without disturbing their quantum state, which means that any eavesdropper would be detected.[26] In principle, information security is ensured by the laws of physics regardless of any technological advances (e.g. a quantum computer).[25] Quantum Key Distribution (QKD) is a technology used to establish the key required by the sender to encrypt (scramble) the message and by the recipient to decrypt (unscramble) it.[25,27] Research is focused on several areas, including: ensuring that implementation does not introduce vulnerabilities; increasing the speed of signals and the distance over which they are transmitted; authenticating users; and developing intercontinental satellite communications.[28] China launched a satellite in 2016 to test quantum communications, and aims to create a global quantum-secured network by 2030.[29]

Computing
Quantum computers (Box 3) could tackle certain tasks that would take conventional computers millions of years:[1]

- **Factorisation** – finding pairs of numbers that can be multiplied together to give a specific answer (e.g. the

Box 2. Quantum Behaviour
Quantum systems exhibit behaviour not seen in everyday life. Some properties, such as energy, become 'quantised' (they can only have certain discrete values). For example, atoms can have certain 'allowed' energies but cannot exist at energies in between these. Quantum systems are also inherently uncertain: it is impossible to predict the outcome of an experiment with certainty. Instead, predictions involve finding the probability of each of a range of possible outcomes. Quantum technologies exploit behaviours such as:

- **Wave-particle duality** – matter or light can simultaneously behave both as a discrete, localised particle (like a billiard ball) and a continuous wave (spreading out like ripples on a pond).
- **Superposition** – a particle can exist in a combination of different states at once. For example, it can behave as if it is spinning both clockwise and anticlockwise at the same time. Once it is measured or interacts with its environment, it settles into a single state, randomly adopting either a clockwise or anticlockwise spin.
- **Entanglement** – two (or more) particles can become intrinsically related, or entangled, so that they can no longer be described as separate entities. This means that a measurement made on one particle will determine the outcome of a similar measurement made on the other particle, even over great distances.

factors of 15 are 1x15 and 3x5). Factorisation of large numbers is very time consuming for conventional computers. Many encryption protocols (used to protect sensitive data) rely on the inability of conventional computers to factorise large numbers quickly.[30]
- **Searches** – for certain large unsorted datasets, a quantum computer could significantly speed up searches by exploring all entries simultaneously.[31]
- **Optimisation** – many problems involve finding the best option given certain constraints, e.g. the most efficient combination of routes for a fleet of delivery vehicles. Quantum computers could help to solve these types of complex problems.[32]
- **Simulation** – quantum behaviour within systems (such as molecules) could be mimicked using the quantum behaviour of a quantum computer, enabling more accurate modelling.[32,33]

Although quantum computers are expected to excel at certain tasks, there are some problems that would still be impossible to solve.[34]

Applications
Quantum technologies are leading to new products and services in many areas, such as infrastructure, navigation, medicine and underground mapping. Other unforeseen applications are also likely to emerge.[1]

Infrastructure
Timing of Networks
Telecommunication networks and power grids rely on clocks that are synchronised across the network with microsecond accuracy (a millionth of a second).[35-37] Timing is also important in finance.[38,39] To prevent fraud, changes to the EU Markets in Financial Instruments Directive will require computers used in automated trades to be synchronised to UTC with microsecond accuracy, from January 2018.[40,41]

Clocks on such networks can be synchronised via satellites.[35-38] Satellite signals are weak and vulnerable to interference and criminal disruption or falsification.[42-45] If a satellite signal becomes unavailable, clocks will gradually drift and require re-synchronisation. The MoD is funding the development of atomic clocks that could remain synchronised to within a few microseconds for over a year without satellite signals or other synchronisation methods.[2] These could increase network resilience and provide a key military advantage if satellite signals are lost (e.g. if disrupted by an adversary).[2] The Cabinet Office and the Government Office for Science are reviewing the dependence of critical services on satellite timing signals and how long these services should be able to operate in the absence of such signals.[1]

Sending Data Securely
Quantum communications systems can also be used to improve infrastructure resilience. For example, they have been used in Geneva to send ballot information for federal and regional elections from the central counting station to a government data centre.[52] They are also being adopted by banks and other firms as an extra layer of security.[53,54] A national laboratory in the US is looking to protect the power grid from cyberattack using quantum communications to send operational data.[55] In future, quantum communications might help to secure military communications against attacks using a quantum computer (Encryption, page 4).[56]

Box 3. Quantum Computers
Conventional computers store data in 'bits' that can exist in only one of two states (0 or 1); different combinations of 0s and 1s are used to represent letters and numbers. A quantum computer would store data in 'qubits', which due to quantum superposition (Box 2), could be both 0 and 1 at once. A group of qubits could occupy all possible combinations of 0s and 1s simultaneously, enabling the computer to explore multiple solutions simultaneously (in contrast to a conventional computer, where a group of bits performs one calculation at a time).[46]

Many states and multinational companies are funding research into quantum computers, using a range of approaches.[3,32,47] Canadian firm, D-Wave, has commercialised a machine that can tackle a specific class of problems. D-Wave says that its operation depends on quantum physics, but this is not yet accepted by all in the quantum computing community.[48] Estimates for developing a 'universal' quantum computer with the flexibility to run any type of algorithm (sequence of calculations) vary from within 15 to over 30 years.[2,49-51]

Navigation
Inertial navigation systems measure the rotation and acceleration of a vehicle to calculate its current location, based on its starting position. Errors accumulate over time, for example, high-performing marine navigation systems can gain a 1.8 km error for every three days at sea.[57] Quantum navigation systems could remain accurate for longer, with researchers predicting that an error of a few hundred metres per month may be possible.[2] The MoD is funding the development of a quantum navigation system, while the US Air Force Scientific Advisory Board says that prototype quantum navigation sensors could be tested in working environments in 5-10 years.[2,58]

Diagnosis and Medical Research
Magnetic fields produced by the brain can be measured to study the structure and function of the brain in real-time. Researchers in the USA have developed a quantum sensor that can operate at room temperature (unlike current equipment), which could lead to more portable devices in the future.[59] They could help in understanding diseases such as dementia.[1] Potential applications for quantum computers in medical research include:
- analysing large quantities of imaging data, for example to reveal the complex connections inside the brain[60]
- running faster simulations of biological processes such as protein folding, to understand better degenerative diseases such as Alzheimer's[32]
- accelerating drug discovery by improving predictions about the properties of new drugs.[32]

Underground Mapping
Conventional gravity sensors can map variations in density to detect, for example, a tunnel or pipe. They are used in

underground surveys prior to major infrastructure work, in oil and gas exploration, and on satellites (e.g. to monitor water levels in aquifers).[1,61] If used on satellites, they could image features in the Earth's surface with a higher (10-100 times) resolution than at present.[62] This could, for example, improve monitoring of river catchment areas to inform flood management (POSTnote 484).[62] Gravity sensors are also being developed to detect and image military facilities hidden underground (it is thought that there is no way of shielding gravity to protect facilities from detection).[2]

Societal Implications

While the Government is taking a variety of measures to foster the UK quantum technology industry (Box 4), there is little evidence available on wider public attitudes towards quantum technologies.[63] The Engineering and Physical Sciences Research Council is launching a public dialogue on quantum technologies in 2017, and the European Commission is running a project to identify and tackle the opportunities and challenges that quantum technologies may present.[64] A report from the UK Networked Quantum Information Technologies Hub has highlighted several issues that these technologies (especially quantum computers) could raise, which are discussed in the following sections.[65] Other implications may emerge as these technologies develop.

Privacy and Automation

A universal quantum computer would dramatically increase data analysis capabilities, while quantum sensors (if they eventually became widely-used) could enable the collection of more accurate data, for example relating to a person's location or health. This may exacerbate existing concerns about data collection and analysis leading to potential infringements of privacy (POSTnote 468).[65]

Quantum computing might also enhance the capabilities of artificial intelligence (computer systems that conduct tasks that otherwise require human intelligence).[32] Use of artificial intelligence could enable the automation of processes, increasing productivity, but may create challenges, such as for employment (POSTnote 534), privacy and attributing responsibility for actions arising from its use.[65-67]

Trade and Access to Technologies

Quantum Key Distribution (QKD) and parts of other quantum technologies are 'dual-use' (POSTnote 340), having both civilian and military applications. As with many technologies, they are subject to export controls, for example under the Wassenaar Arrangement, which may limit the trade of some products developed in the UK.[2,65] Further, high costs (particularly initially) could be a barrier to accessing quantum technologies.[65] The infrastructure needed for quantum computers is currently too expensive for all but large corporations and governments. Some suggest that unequal access to quantum technologies may cement or increase power imbalances between nations, or between these powerful actors and citizens.[65]

Box 4. Fostering the UK Quantum Technology Industry

An analysis of global patents by the UK Patent Office suggests that the UK is strong in quantum technologies.[68] Members of the UK quantum technology community have said that a more detailed international analysis of global markets and the UK's position would help to focus future efforts on areas where the UK is strong and has a realistic chance of large commercial return.[2] The Government Office for Science has said that there is a strong case for continuing the National Programme in order to maintain the UK's global position.[1] It, and the UK quantum technology community recommend:

- the creation of 'innovation centres' with a greater focus on industry and co-location of academic and industrial partners[1]
- more engagement between the quantum technology community, end-users and industry to ensure products meet market needs[2]
- private sector matched funding for future stages of the National Programme (Box 1), to increase commitment from industry[1]
- the establishment of a new body with the sole remit to coordinate National Programme activities[1]
- that regulators and standards bodies are aware of a technology's capabilities, so that regulations can be adapted accordingly.[1]

Encryption

Quantum computers would be able to break widely used encryption protocols, because of their ability to factorise large numbers.[25] Such protocols are a cornerstone of electronic security and undermining them could lead to the misuse of sensitive financial, identity or national security data.[25] New approaches are being developed that could be resistant against decryption by a quantum computer, such as QKD and quantum resistant algorithms (mathematical problems thought to be unsolvable with a quantum computer).[25] The European Telecommunication Standards Institute (ETSI) is developing standards for QKD. Both ETSI and the US National Institute of Standards and Technology have initiatives to establish standards for quantum resistant algorithms, although this could take over 5 years.[69-72]

A third party might intercept encrypted messages today and store them until a quantum computer became available.[25] ETSI recommends that organizations ensure that their current systems can be switched to use new cryptography approaches resistant against quantum computers, once specific schemes are recommended by standards bodies.[73] It suggests that legislation could be used to encourage adoption of quantum computer-resistant communications that might otherwise be slowed by:[25]

- security industry best practice that involves using well-established standards
- a perceived lack of urgency due to uncertainty about when a quantum computer will become available
- the potential for organizations to classify decryption by quantum computer as a high impact but low probability risk, which they do not prioritise.

Endnotes

1 Government Office for Science, The Quantum Age: Technological Opportunities, 2016
2 Defence Science and Technology Laboratory, UK Quantum Technology Landscape 2016, 2016
3 Netherlands Ministry of Economic Affairs, Global Developments in Quantum Technologies, 2015
4 HM Treasury, Autumn Statement 2013, 2013

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Amanda Diez Fernandez for researching this briefing, to the Engineering and Physical Sciences Research Council for funding her parliamentary fellowship, and to all contributors and reviewers. For further information, please contact the co-author, Lydia Harriss.

[5] UK National Quantum Technologies Programme, Quantum Technologies: A £1 Billion Future Industry for the UK, 2017
[6] HM Government, Building our Industrial Strategy, 2017
[7] Quantum Technologies Strategic Advisory Board, National Strategy for Quantum technologies, 2015
[8] European Commission, Quantum Technologies, 2017
[9] European Commission, Intermediate Report from the Quantum Flagship High-Level Expert Group, 2017
[10] European Commission, Future and Emerging Technologies Flagships, accessed 22/03/2017
[11] European Research Area Network, Members of FLAG-ERA, accessed 22/03/2017
[12] Massachusetts Institute of Technology News, Thousands of Atoms Entangled with a Single Photon: Result Could Make Atomic Clocks More Accurate, 2015
[13] BT and Toshiba Launch UK's First Quantum Communication Showcase, accessed 22/03/2017
[14] Bureau International des Poids et Measures, International Atomic Time, accessed 22/03/2017
[15] US National Coordination Office for Space-Based Positioning, Navigation, and Timing, How GPS Works, accessed 22/03/2017
[16] Nature News, Atomic Clocks use Quantum Timekeeping, 2010
[17] Reviews of Modern Physics, Optical Atomic Clocks, 2015
[18] The National Metrology Institute of Germany, World Record for Two Optical Clocks, 2016
[19] Sandia National Laboratories, World's Smallest Atomic Clock on Sale, 2011
[20] Nature News, Hyper-precise Atomic Clocks Face Off to Redefine Time, 2015
[21] Muller Group at University of California Berkeley, An Introduction to Atom Interferometry, accessed 22/03/2017
[22] AOSense, Gravimeter, accessed 22/03/2017
[23] University of Birmingham, Gravity Gradient Sensors, 2016
[24] Nature News, Entangled Photons Make a Picture from a Paradox, 2014
[25] European Telecommunications Standards Institute, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, 2015
[26] Institute of Physics, The Age of the Qubit, 2011
[27] POST, Data Encryption, POSTbrief 19, 2015
[28] Nature, Practical Challenges in Quantum Key Distribution, 2016
[29] Chinese Academy of Sciences, China's Space Satellites Make Quantum Leap, 2016
[30] Massachusetts Institute of Technology News, The Beginning of the End for Encryption Schemes?, 2016
[31] University of Michigan, Is Quantum Search Practical?, 2015
[32] Networked Quantum Information Technologies Hub, The Commercial Prospects for Quantum Computing, 2016
[33] Science Magazine, Quantum Simulators, 2009
[34] Scientific American, The Limits of Quantum, 2008
[35] US Government, Timing, accessed 22/03/2017
[36] Symmetricom, Power Utilities: Mitigating GPS Vulnerabilities and Protecting the Power Utility Network Timing, 2013
[37] Symmetricom, Ensure Mobile Service Availability with Rubidium Sync Holdover, 2012
[38] Journal of Research of the National Institute of Standards and Technology, Accurate, Traceable, and Verifiable Time Synchronization for World Financial Markets, 2016
[39] Government Office for Science, Future of Computer Trading in Financial Markets: an International Perspective, 2012
[40] Financial Conduct Authority, The Markets in Financial Instruments Directive, accessed 22/03/17
[41] European Commission, Annex to the Commission Delegated Regulation supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks, 2016
[42] Innovate UK Blog, Thinking Differently about Location and Time Data, 2016
[43] The Royal Academy of Engineering, Global Navigation Space Systems: Reliance and Vulnerabilities, 2011
[44] Chatham House, Space, the Final Frontier for Cybersecurity?, 2016
[45] Los Alamos National Laboratory, GPS Spoofing Countermeasures, accessed 22/03/2017
[46] Science Magazine, Scientists are Close to Building a Quantum Computer that can Beat a Conventional One, 2016
[47] Networked Quantum Information Technologies Hub, Technical Roadmap for Fault-Tolerant Quantum Computing, 2016
[48] Nature News, Computing: The Quantum Company, 2013
[49] The Optical Society, Quantum Computing: How Close Are We?, 2016
[50] Wired Magazine, The Quantum Clock is Ticking on Encryption – and Your Data is Under Threat, 2016
[51] US National Institute of Standards and Technology, Report on Post-Quantum Cryptography, 2016
[52] ID Quantique SA, Geneva Government: Secure Data Transfer for Elections, 2011
[53] ID Quantique SA, Financial Services: IDQ Secures Network for Disaster Recovery, 2011
[54] The Economist, Quantum Technology is Beginning to Come into its Own, 2017
[55] US Department of Energy, Office of Electricity Delivery and Energy Reliability, Practical Quantum Security for Grid Automation, 2013
[56] Joint Force Quarterly, 77, Cindy Hurst, The Quantum Leap into Computing and Communication: A Chinese Perspective, 2015
[57] iXblue, Marins Series: Military Strategic Grade INS, accessed 22/03/2017
[58] U.S. Air Force Scientific Advisory Board, USAF Scientific Advisory Board Study Utility of Quantum Systems for the Air Force, 2016
[59] US National Institute of Standards and Technology, Detecting Brain Waves with Atomic Vapor, 2016
[60] Massachusetts Institute of Technology News, A New Quantum Approach to Big Data, 2016
[61] NASA, Groundwater: Tracking Groundwater Changes Around the World, accessed, 22/03/2017
[62] Nature, Psi in the Sky, 2015
[63] Sciencewise, Public Attitudes to Quantum Technology, 2014
[64] European Commission, Quantum Technologies: Implications for European Policy, 2016
[65] Networked Quantum Information Technologies Hub, Thinking Ahead to a World with Quantum Computers, 2016
[66] Government Office for Science, Artificial Intelligence: Opportunities and Implications for the Future of Decision Making, 2016
[67] House of Commons Science and Technology Committee, Robotics and Artificial Intelligence, 2016
[68] Intellectual Property Office, Quantum Technologies: a Patent Review of the Engineering and Physical Sciences Research Council, 2013
[69] European Telecommunications Standards Institute, Quantum Safe Cryptography, accessed 22/03/2017
[70] US National Institute of Standards and Technology, NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat, 2016
[71] US National Institute of Standards and Technology, NIST Asks Public to Help Future-Proof Electronic Information, 2016
[72] US National Institute of Standards and Technology, Post-Quantum Cryptography: NIST's Plan for the Future, 2016
[73] European Telecommunications Standards Institute, Quantum Safe Cryptography: Case Studies and Deployment Scenarios, 2017