JRC SCIENCE FOR POLICY REPORT

Quantum Technologies: Implications for European Policy

Issues for debate

A M Lewis, M Krämer and M Travagnin

16 May 2016

EUR 27915 EN

Contact information
Name: Adam M Lewis
Address: Joint Research Centre, Via E. Fermi 2749, Ispra (VA),
E-mail:adam.lewis@jrc.ec.europa.eu
Tel.:0039 0332 785786

JRC Science Hub
https://ec.europa.eu/jrc

JRC101632

EUR 27915 EN

PDF ISBN 978-92-79-58276-9 ISSN 1831-9424 doi:10.2788/384376 LB-NA-27915-EN-N

How to cite: A M Lewis, M Krämer and M Travagnin;
Quantum Technologies: Implications for European Policy; EUR 27915;
doi:10.2788/384376

Abstract

Title Quantum Technologies: Implications for European Policy

New technologies for communications, computing, sensing and timing, which exploit quantum physics more deeply than heretofore, are expected to have high impact and to require a European policy response. This paper raises key discussion points, as a contribution to a wider EC initiative.

Table of contents

Acknowledgement

We wish to thank our JRC colleagues Naouma Kourti and Carlo Ferigato for helpful discussions during the writing of this paper and, in general, in the study.

The work was funded by the JRC's institutional work programme.

Executive summary

Quantum Technologies are being promoted as part of the EU's Future and Emerging Technologies (FET) programme that aims at turning Europe's excellent science basis into a competitive advantage. Recently, as part of its Communication on the European Cloud Initiative [COM(2016) 178], the European Commission has proposed reinforcing EU action in this area in line with recent initiatives at Member State level, such as the UK Quantum Technologies Programme and the establishment of the QuTech centre in the Netherlands. The Joint Research Centre (JRC), in pursuing its mission to support EU policies with independent evidence, has decided to study the implications of the emergence of quantum technologies on European policies. Through this study, the JRC seeks to indicate possible points of intervention to seize on opportunities and to respond to the new realities that the use of quantum technologies could bring along.

However there are many questions to answer before that can be done, such as: What is the maturity of the technologies? Which application ideas open promising prospects for economy and society? Who are possible pioneer users? Will quantum technologies be competitive and how do they fit into current and future industry landscapes? Which are the initiatives at international level that may pose challenges for Europe? Which are the leverage points and drivers to promote progress and achieve benefit?

Three generally-recognized application areas have been chosen as initial study cases:

- Secure communication
- Computing and simulation
- Sensing and timing

For each application area, the JRC is setting up interactive processes with stakeholders and experts to exchange views on the questions relevant to each area. Based on the obtained answers, the JRC will engage with policy Directorates General of the European Commission to discuss the nature and timing of potential policy interventions.

In this paper, the 3 application areas are discussed so as to formulate the questions to be addressed and to stimulate the ensuing debate. If you feel you can contribute to this discussion please send an e-mail to **jrc-quantum@jrc.ec.europa.eu** and indicate your application area of interest.

1. Introduction

Scientific and technological progress in the last decades has brought along an increasing ability to analyse and manipulate physical systems at quantum level. This has made it possible to experimentally investigate quantum physics phenomena that, although well-known from the theoretical point of view, had been extremely hard to explore in the laboratory. Phenomena such as entanglement are very different from anything we experience at a human scale, challenge our imagination and intuition, and offer exciting possibilities for technological advance. Quantum physics is fundamental to devices such as the transistor and the laser, which have had transformative effects in our lives. Now, the growing capability of controlling the quantum world at an even deeper level is opening up new perspectives for innovation.

Novel quantum technologies are emerging in a number of sectors, namely communication, computing, sensing and measuring. Technology readiness levels and timescales for development vary significantly. In some cases, the new devices are expected to offer enhanced performance, versatility, resilience or better handling with respect to existing solutions. In other cases, the improvements might be so great as to enable completely new solutions to a variety of problems, with possibly transformative effects. Also, further technologies or applications might emerge that have not even been thought of so far. A wealth of business opportunities may unfold, but there are demanding technical and commercial challenges to be met in order to take advantage of them. Moreover, some of the applications are directly relevant to the public sector, for example in defence, security, and health care. Consequently quantum technologies carry a social and economic significance which demands the attention of public authorities, to help realize their economic and societal potential and to adapt or introduce regulatory regimes and standards as the need arises.

Quantum Technologies have been promoted through the EU's research and innovation framework programmes, most prominently via the Future and Emerging Technologies (FET) actions that aim at turning Europe's excellent science basis into a competitive advantage. Recently, as part of its Communication on the European Cloud Initiative [COM(2016) 178], [SWD (2016) 107], the European Commission has suggested reinforcing EU action through a long-term flagship initiative together with the private sector. The reasoning underlying this is in line with initiatives at Member State level, such as the UK Quantum Technologies Programme and the Dutch QuTech centre. It also reflects the call put forward in the Quantum Manifesto, a document that has been endorsed by stakeholders from science, industry and from some Member State governments [Quantum Manifesto, 2016].

The Joint Research Centre (JRC), in pursuing its mission to support EU policies with independent evidence, has decided to study the implications of the emergence of quantum technologies on European policies. With the goal of giving the European institutions foresight to inform policy decisions, the JRC seeks to indicate possible points of intervention to seize on opportunities and to respond to the new realities that the use of quantum technologies could bring along.

To conduct the study, the JRC is setting up interactive processes with stakeholders and experts from research, industry and policy to exchange views on the questions relevant to the envisaged application areas of quantum technologies. Interlocutors include experts from quantum science and technologies, but also experts on related or competing technologies, industry representatives from relevant market sectors, potential users and policy makers.

Engaging in a fruitful and balanced dialogue serves to examine aspects like maturity, applicability, competitiveness and market uptake of quantum technologies in the envisaged application domains. Further aspects include the possible role and integration

in current and future industry landscapes as well as challenges posed by activities worldwide and the pull exerted by arising economic and societal needs.

Based on the obtained answers, the JRC will engage with policy Directorates General of the European Commission, to discuss the nature and timing of potential policy interventions. The need and possibility for European policy response in the short and medium term will thus be assessed and points of intervention will be indicated. Beyond research and growth, other policy implications such as in security, space, health, energy etc. will be given special attention.

Three generally-recognized application areas have been chosen as initial study cases:

- Secure communication
- Computing and simulation
- Sensing and timing

In this paper, these application areas are discussed so as to formulate the questions to be addressed and to stimulate the ensuing debate. The sections dedicated to the three areas have been authored respectively by M. Travagnin, M. Krämer, and A. M. Lewis.

If you feel you can contribute to the study, either in a workshop or by correspondence, please send an e-mail to **jrc-quantum@jrc.ec.europa.eu** and indicate your application area of interest.

2. Secure Communications

2.1 Background

The possibility of transmitting at macroscopic distances the information encoded in quantum states has given rise to the field of quantum communications. Light is usually employed as the carrier, and optical quantum communications typically exploit phenomena such as photon entanglement (which means the quantum states of two photons are coupled in such a way that a measurement performed on one of them instantaneously affects the other's state, independently of the distance) or the no-cloning theorem (which states the impossibility of creating an identical copy of an unknown quantum state without affecting it). These peculiar phenomena lend themselves naturally to applications in the field of cryptography. Indeed, quantum states can be prepared in such a way to make it impossible to interact with them without modifying them. This means that an eavesdropper will unavoidably introduce a disturbance in the quantum states being transmitted among two interlocutors. Such a disturbance allows the revealing of the eavesdropper's activity to the two legitimate partners, as long as they devise and properly implement a suitable communication protocol. Quantum phenomena can therefore be exploited to share a cryptographic key whose confidentiality is guaranteed not by computational hardness but rather by fundamental physical laws, with a technique that has become widely known as Quantum Key Distribution (QKD). It must, however, be pointed out that the secure key exchange provided by QKD constitutes just a link in the chain of cryptographic primitives that are necessary to implement secure communications, and that the remaining links generally depend on mathematical algorithms and therefore remain prone to cyber-attacks. Such attacks become more effective as computational power increases, and could also take advantage of unexpected advances in mathematical analysis.

Indeed, a powerful driver for the development of new cryptographic techniques is progress in the development of a quantum computer, which would break the most common algorithms presently employed in public-key cryptography, and weaken the security of symmetric cryptography. Cryptography-breaking quantum algorithms have already been experimentally demonstrated in some small-scale quantum computing platforms, but the time horizon necessary to actually build a quantum computer that constitutes a real threat for present-day communication security is still unclear. In 2015 there has been a first policy response to this threat, with the announcement by the US National Security Agency that it "will initiate a transition to quantum resistant algorithms in a not too distant future". Standardization initiatives on post-quantum cryptography have been launched both by the European Telecommunications Standards Institute (ETSI) and by the US National Institute for Standards and Technology (NIST), respectively in 2015 and 2016.

Quantum Key Distribution was theoretically proposed in 1984, and the first experimental demonstration came in 1991. It has now reached, in some of its implementations, such a level of technological readiness that several commercial players are working on QKD systems at a pre-competitive level, testing system prototypes and field deployments. Standardization work started in 2009 (with a dedicated ETSI industry specification group), and a handful of SMEs are offering commercial products, typically to complement conventional cryptographic solutions. The necessity of focusing on policy issues going beyond research funding is therefore materializing. A policy option that is being pursued by several governments takes the form of technology push programmes, including in some cases substantial investments. These are needed in particular for long distance quantum links, since they are not compatible with the existing fibre-optics infrastructures. As an example, by the end of 2016 China will complete a 2000 km "quantum backbone" linking Beijing to Shanghai, and will launch a "quantum satellite" to connect it to Urumqi, the capital of Xinjiang.

Given the impact that a novel cryptographic technique such as QKD may have in several heavily-regulated areas of critical public interest, it could well be that the perspective of it becoming an effective communication security tool depends on policy initiatives not less than on market pull. However, a clear consensus among researchers and experts on the effectiveness of the role that QKD may have in responding to cyber-security threats, e.g. those caused by the development of quantum computers, has yet to emerge.

2.2 State of Research and Development

Research on secure quantum communications spans fundamental theoretical issues to the actual deployment of demonstrators and test-beds. It involves very diverse communities of scientists in fields ranging from information theory to material science, from quantum optics to telecom engineering, and from computer science to microelectronics. Several open questions remain. For example, the fact that some QKD protocols are actually information-secure is still being debated. But even a protocol which has been demonstrated to be information-secure can be attacked at the physical layer, given the non-ideal behaviour of the components employed to implement it. Research activity is therefore underway to devise new protocols that are less sensitive to implementation loopholes (e.g. device-independent QKD), to develop better components, and to integrate them in field deployable quantum chips [Scarani and Kurtsiefer, 2014]. A new "quantum hacking" specialization has emerged, with the mission of testing and challenging the solutions put forward by QKD developers [Lyderse et al., 2010].

Also, completely novel devices (e.g. quantum repeaters) must be developed to enable long distance quantum communications, and the time scale for their industrial availability is still debated. Hybrid solutions are meanwhile being deployed, that require intermediate nodes whose security has to be enforced by classical methods. Space-based relay systems are also being explored to circumvent the lack of quantum repeaters. However, the engineering is complex, the deployment cost high, and the performances severely constrained by optical losses [Elser et al., 2012].

Another important point to remember is that QKD presupposes the identification of the partners: this requires a public key infrastructure, which is presently based on cryptographic algorithms that could be easily attacked by future quantum computers. Therefore, fully quantum-resistant communications depend among others on the development of quantum signatures, a technique still in its infancy [Collins et al., 2014].

In addition to overcoming the existing technological limitations, the research community is working for the development of industrial standards that will cover aspects such as the implementation, evaluation, and certification of QKD components and systems [Alléaume et al, 2014]. Also, the interfacing with the existing communication infrastructure, as well as new metrology for performances and reliability are being addressed. The adoption of widely shared and accepted standards is commonly seen as a necessary step to build a market, by fostering awareness, confidence and trust of potential customer and final users.

2.3 Industrial trends

To assess the interest that Quantum Key Distribution is actually raising among commercial players, and gather some evidence on the industrial sectors that seem more active in this field, a patent analysis has been performed. With respect to already available publications [UK Intellectual Property Office, 2013], new information has been made available by attributing to each country the applications filed by applicants headquartered in it. The data are obtained from the Global Patent Index database of the European Patent Office (as per January 2016), manually filtering out the possible "false positives". The main results of this approach are plotted in Fig. 1.

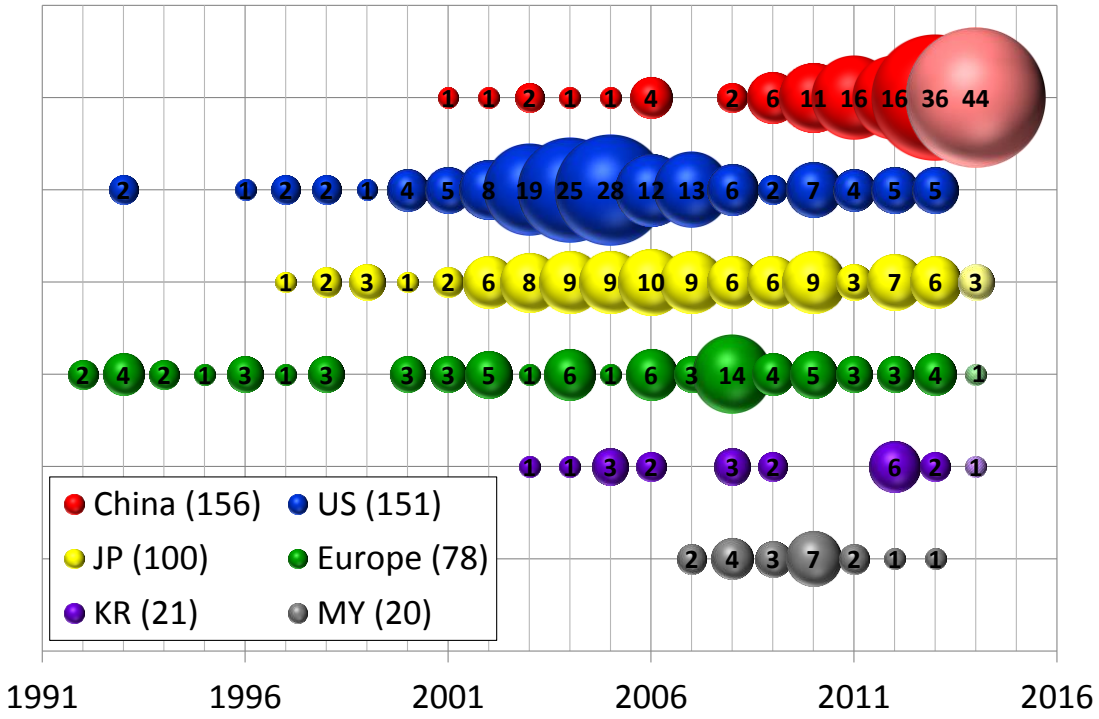

Fig. 1: Patent applications filed by applicants headquartered in different countries, for each priority date year. Europe comprehends UK (30 applications), FR (9), CH (7), DE (7), IT (6), ES (5), AT (4), FI (3), BE (2), GR (2), IE (1), LU (1), and RO (1). Applicants to the Chinese national patenting authority may renounce the 18-months non-disclosure period that is generally observed in all other countries, thus at least in part skewing the application counts for 2014.

The following trends have been identified:

- Overall patenting activity is still modest, and after an accelerating phase in the first ten years after inception in 1992, the global patenting pace has been constant. However, this apparent steadiness masks very different national trends. By inspecting Fig. 1, we can see that the number of Chinese applications rose markedly after 2010, and now tops the list. In the USA, the patenting activity peaked in 2003-2005, and has now stabilized on much lower levels. Japanese applicants started patenting somewhat later than in Europe and USA, but then maintained a very constant output. Also European applications have been more or less steady over the years: however, they seem to have somewhat peaked around 2006-2008.
- In most countries, applications by industrial players outnumber academic ones; the only exceptions are China (almost half of the applications are filed by universities), and Malaysia (all patents are filed by a single national research centre).
- In China, most of the patents have been filed by a couple of newly formed SMEs involved in the development of a national QKD infrastructure, with additional contributions by firms such as China Electric Power and China State Grid Corporation, which work on critical infrastructure protection.
- Most of patenting in the US and in Western Europe (led by UK) has been determined by firms active in the defence/security/aerospace sectors: MagiQ, BBN Raytheon, and Boeing in the US, Qinetiq in UK, Thales in FR, and Finmeccanica in IT. In the USA the Los Alamos National labs filed several applications on the use of QKD for critical infrastructure protection. The American telecom sector is strikingly absent, with only negligible contributions from big firms as Cisco, Nortel, and Verizon. Conversely, the industrial sectors more active

in Japan are telecommunications and electronics, and the same holds true for South Korea.

Looking at these findings, a question arises as to whether we can speak about "fashion waves" taking shape in different countries at different times, and involving different industrial sectors - some of which strongly depend on national policy programmes especially in defence, security, and space. It is evident that the technology push in China has spurred the formation of a completely new industrial capability. On the other side, at least in the western world, the interest from the defence sector seems to be ebbing, as can be confirmed also by documents such as the UK CESG White Paper [UK Government Communications Headquarters, 2016] and the USAF Scientific Advisory Board study [Utility of Quantum Systems for the Air Force, 2015]. Conversely, new applications seem to be emerging in other sectors: at the last QuCrypt conference (Tokyo, September 2015) Toshiba unveiled a QKD free-air pilot link to secure the transmission of genetic data. The Industrial and Commercial Bank of China successfully tested a QKD system in September 2015 [Industrial and Commercial Bank of China, 2015], and the possible interest by the financial sector has been discussed at a workshop organized by Plantagenet Systems, KTN, Innovate UK and the Innovation Forum (London, February 2016). In Europe, the first field deployment by a commercial user took place in 2010, when Siemens installed a QKD link between its data centres in The Hague and Zoetermeer.

However, a significant market for QKD systems has yet to materialize. According to some communications system manufacturers and cyber-security experts this technique has no future as a commercial product. This is for example the position expressed by Cisco in a 2012 presentation at a Royal Holloway University of London Information Security Colloquium, and confirmed in 2014 in a discussion held at the Crypto Forum Research Group, that is hosted by the Internet Research Task Force. They maintain that the key exchange, imperfect as it may be, is actually the strongest link in an information security chain which has several other more acute weaknesses (e.g. in networks, computers, and user interfaces), whose security should be prioritized. This view is shared also by the renowned cyber-security expert Bruce Schneier, who thinks that QKD is "as awesome as it is pointless" [Schneier, 2008]. These critical voices highlight the incompatibility of QKD with the existing optical fibre infrastructure, the difficulty of implementing a point to multipoint topology, and the impossibility to use it in wireless networks, and point at new quantum-safe protocols as the only viable mainstream solution for post-quantum cryptography. The issues affecting the potential of QKD as a successful technology in the marketplace have been discussed at a NEC Princeton Workshop on Quantum Cryptography already in 1999, originating a paper that is now available online [Hoi-Kwong Lo, 1999].

Because of technical complexity, novelty and cost, and also due to the difficulty of fully integrating it in the existing communication infrastructure, a common understanding about the future of QKD as a widespread commercial product has not yet consolidated, and there is no consensus about the importance of the role it will play in a hybrid environment that will progressively include quantum-safe algorithms. It is however clear that it holds the promise for important applications in sectors of prominent public interest such as space, defence, government, finance, and health [Jennewein and Choi, 2014]. It is therefore expected that policy decisions will have a great impact in the future progress of QKD as a viable cryptographic technique.

2.4 Policy Issues and Related Questions

Two very general trends should be considered when debating the policy implications of quantum-secured communications. On one side there is the phenomenon of an ever more interconnected society, where an increasing amount of critical information will be transmitted along a communication infrastructure. On the other, there are scientific

developments as the progress in computing power (due e.g. to artificial intelligence and cloud computing, or even to paradigmatic shifts like those entailed by quantum computation), that will threaten the reliability of cryptographic techniques based on computational hardness. These very general trends seem to highlight an evolutionary advantage for quantum-based cryptography, which relies on fundamental physical laws rather than on computational assumptions. But for such a process to really take hold, the development of an extremely diversified range of techniques would be required, some of which are still at a very early development stage. Even Quantum Key Distribution, although by far the most mature among the quantum cryptographic primitives, is presently still affected by several technical constraints, as described above, that prevent its applicability to a broad range of business cases.

An issue to be examined is therefore whether in these conditions it is reasonable to expect that market forces alone will exert the necessary pull for further growth and diffusion of QKD in the shorter term, and of other cryptographic primitives (e.g. quantum signatures, quantum non-repudiation) in the long run. If such forces do not materialize, it can be expected that applied research in this field will atrophy, carrying the risk of missed growth opportunities and increased dependence on a critical technology. A question therefore arises about the rationale for a public-funded technology push in this area.

Several countries have already started to move in this direction, as can be seen from the following overview:

- A comprehensive public programme for the deployment of a QKD infrastructure is being pursued by **China**, and comprises a ~2,000km Beijing-Shanghai quantum backbone, four metropolitan networks, a ~50km free air link, and a quantum satellite for intercontinental communications.
- The government of **South Korea** is funding the development of a ~250km quantum backbone connecting existing metropolitan quantum networks.
- **Australia** is implementing a Government Quantum Network for intra-governmental communications in Canberra.
- In **South Africa** a quantum communication security solution has been deployed in Durban's municipal fibre-optic network.
- In **Japan** several industrial and public partners have jointly developed an extensive quantum network in Tokyo.
- Besides China, satellite-based quantum communications are also currently investigated by Japan, **Canada**, and the USA; in 2007 the European Space Agency published a review paper on its activity in this field, comprising a feasibility study for the placement of an entangled photon source on the International Space Station.
- In the **USA**, a fibre-based QKD infrastructure is being developed since 2003 (with a DARPA-funded project), and several players both public (Department of Commerce with NIST, Department of Energy with Los Alamos Labs) and private (mostly from the defence and aerospace sectors, e.g. Magiq, BBN Raytheon, Boeing, Batelle) are accumulating intellectual property and know-how, in some cases complemented by field deployments.
- A real-world application of QKD was demonstrated in **Austria** in 2004. In 2007, in **Switzerland** the canton of Geneva transmitted ballot results using a QKD link.
- A high point in **European** research towards practical application of quantum cryptography was achieved in 2004-2008, with the **SECOQC FP6 project** that involved several academic as well as industrial partners. However, some European companies seem now to have reduced their engagement.

Presently the most advanced Quantum Communications deployments in Europe are being pursued in the **United Kingdom** and in the **Netherlands** with public-funded projects of quantum links connecting Bristol to Cambridge and Delft to Den Haag and Leiden, respectively, while the Austrian and Chinese Academies of Sciences are working

together on a Quantum Space test link. A European-wide strategy for infrastructural deployments is currently missing.

In most of these public programmes, a certain degree of private involvement has been sought, targeting business sectors in which a commercial interest is likely to emerge sooner rather than later. But overall, until now, most QKD deployments all around the world have been mostly financed outside commercial logic, and rather in the expectation that they will contribute to economic growth by helping the build-up of completely new markets. Experiments on a small scale serve as field pilots, essentially intended to demonstrate the potential of the technique, and therefore engage possible users, encourage other adopters, stimulate the interaction among different industries, test standards and procedures, and to help bridge the culture gap with conventional cyber-security. On a larger scale, these programmes may stimulate the creation of a new industry and a complete supply chain. For some governments, the intent is clearly to develop autonomous capabilities and avoid dependence on other countries in technologies that can have a big impact in sectors critical for national security. Indeed, some countries apply export restrictions to certain cryptographic technologies, because of their potential military use. In the case of China, the scale of the public investment is such that a national quantum infrastructure is being built. In the USA, the push for big QKD infrastructural investments seems to have lost momentum, and different instruments are being used to encourage industrial participation: several SMEs are receiving Small Business Innovation Research (SBIR) awards and Small Business Technology Transfer (STTR) funds to develop components like e.g. entangled photon sources and single photon detectors. In this way the technology push is intended to bring to the market a new generation of devices that can play an important role not only in QKD, but also in several other quantum applications.

The scale of the efforts going on all around the world for the development of quantum cryptography is such that the debate on policy options should now be enlarged to include a general discussion about the actions that would be required if quantum technologies will enjoy a widespread adoption in communications security. In other terms, can we envisage in the near future an emerging necessity for other policy actions, to be pursued alongside funding research and contributing to the build-up of a market? Discussing policy preparedness issues will require analysing the consequences of the spreading of these technologies, and identifying the policy areas that may be impacted.

Here we present a list of points to be debated to assess the status of R&D on QKD, the perspectives for its commercial exploitation, and the need for further policy initiatives. The discussion will involve QKD researchers and manufacturers, experts in information security and conventional cryptographic techniques, telecoms engineers, network providers, potential QKD customers and users, researchers who have participated in field deployments and tests, experts who have contributed to progress in standardization, proponents of business cases, market analysts, investors, policy makers, regulators, privacy and data protection experts, and a wide representation of civil society.

1. What are the unique strengths of this technology? Will the limitations which now affect it always be inherently present?

2. What are the strengths and weaknesses of alternatives, already present on the market or being researched?

3. To what extent will the future of QKD depend on the rise of quantum computing?

4. Are there real-world applications for which at the present development stage QKD may already represent a commercial alternative to conventional solutions?

5. Are there credible business models?

6. Are there more general business trends that can act as tailwinds or headwinds for the future of QKD as a commercial product?

7. Will market forces alone provide the growth and diffusion of QKD, or is there a need and justification for policy support initiatives?

8. Are there particular interest groups advocating or opposing the diffusion of QKD?

9. Is now the time for Europe to go beyond pure research funding? If yes, which are the right ways to support the progress and diffusion of this technology?

10. Is there a risk of fragmentation in Europe, given the programmes already adopted by some governments?

11. Given the initiatives of other countries, is there a necessity to start thinking about a common European infrastructure to be used as test-bed for researchers?

12. Could an European infrastructure contribute to build-up a new market, by identifying commercial opportunities and help develop business models?

13. If a technology push initiative is justified, which area should be addressed first (space, defence, government and public administration, infrastructure protection)?

14. Are there some legal frameworks that are hindering market forces?

15. Are there societal constraints that must be taken into account, or societal groups that will be particularly affected?

16. Can we envisage the long-term consequences of a widespread adoption of this technology, for example in international relations, or in the privacy/security balance?

3. Computing and simulation

Future computing, and more generally future IT, is a challenge of vital importance. Progress in semiconductor-based computing technology has been steady for several decades. During this period, constant increase in performance and decrease in size could be counted on. However, this is changing (see e.g. [Waldrop, 2016]]. It is an open question as to how future computing will evolve. In this context, new information technologies are more than a "Nice-to-have" or a subject for curiosity-driven research. Beyond specific technologies, there is a need for new integrated views of future IT landscapes. It is recognized that quantum computing and simulation could play a role in this, but it is uncertain how and to what extent.

3.1 Changing times for information technologies

One of the drivers behind the ongoing change is a worsening cost-to-performance ratio when it comes to cost of technology development, manufacturing and energy consumption related to further hardware miniaturization and performance increase. In contrast, in the past, increase in cost was effectively compensated by increase in performance. Yet, this is not the only reason why advances in computing cannot be achieved as before: The diffusion of the internet and of wireless mobile devices, the growth in data to be stored and turned into information as well as the trend towards an "internet of everything" are transforming the ecosystem of information technologies. As these trends continue, technology needs emerge that cannot be satisfied with existing capabilities, including the need to (see e.g. [Semiconductor Industry Association, 2015]):

- Increase energy-efficiency of computing and sensing,
- Increase high-speed wireless connectivity and communication capacity,
- Increase capability to store and analyse growing amounts of data,
- Increase ability to control and enhance safety, security and privacy in complex networked IT systems,
- Ensure cost-effective manufacturing of computing devices.

The ongoing change is becoming manifest in a slow-down of the rate of progress in the chip-manufacturing business. In research and development a trend towards diversification and specialization has become apparent. Pathways include new transistor designs, new materials beyond silicon and chip design (see e.g. [Cross, 2016]).

Also, among the symptoms of change are a number of notable recent decisions and strategic activities: The worldwide chip industry has restructured ITRS, the International Technology Roadmap for Semiconductors. ITRS had been used to coordinate technology advances among manufacturers, designers and suppliers since the 1990s. "ITRS 2.0" was launched in 2014 in collaboration with several IEEE societies. The 2014-2016 efforts have led to the transformation of ITRS 2.0 into the "International Roadmap for Devices and Systems" (IRDS) with the aim to deliver visions and roadmaps going beyond conventional paradigms[1]. Also, in the USA the Semiconductor Industry Association and the Semiconductor Research Corporation published a report in September 2015 which outlines research challenges and calls for additional national public investment to

[1] The launch of the International Roadmap for Devices and Systems (IRDS) was announced on May 4, 2016 as a new IEEE Standards Association (IEEE-SA) Industry Connections (IC) program to be sponsored by the IEEE Rebooting Computing (IEEE RC) Initiative in consultation with the IEEE Computer Society. The first meeting is scheduled for May 12/13, 2016 at IMEC, Belgium.

support growth and innovation in the IT sector [Semiconductor Industry Association, 2015]. Only 2 months earlier, the US president had ordered the creation of a National Strategic Computing Initiative (NSCI) with the strategic objective (among others) to establish "a viable path forward for future HPC [High Performance Computing] systems even after the limits of current semiconductor technology are reached (the "post-Moore's Law era")".

3.2 Advances in quantum computing and simulation

Quantum computing and simulation are among the approaches that are attracting attention in the face of the growing challenges to the IT industry. However, advances on quantum computing have so far been research rather than market driven, despite the fact that important contributions have been made by industrial R&D centres from the beginning (IBM Research, Bell Labs).

Scientific interest was actually sparked as early as the 1970s. It was boosted in the early 1990s by theoretical work showing that the efficiency of specific computational tasks is significantly improved when using quantum carriers of information (qubits) and processing them based on quantum physical laws. This included factoring, a task relevant to breaking a common encryption scheme (for further discussion, see section on secure communication) [Shor, 1994]. Experimental work was kicked-off at that time, enabled by the increasing ability to manipulate and analyse physical systems at quantum level. Research interest in quantum information and in quantum information processing generally increased from there.

Since then, significant progress has been made regarding initialization, processing and read-out of qubits in atomic, photonic and solid state systems. Several computing models have emerged and advances have been made on error correction as well as on quantum algorithms. Building universal quantum computers still poses significant challenges. Therefore, special purpose machines, in particular for simulation, have been targeted as promising ways to gain a performance advantage in the near future for specific tasks such as optimization or material analysis and material design. Also, successful steps have been made regarding the integration of processing elements on chips[2].

The first public sector driven research roadmap exercises date back ~10-15 years [Advanced Research and Development Activity, 2002], [Zoller, 2005]. Major challenges still lie ahead and include substantial scaling up, error correction, interfacing, integration with conventional components and development of architectures [Van Meter et al., 2013]. However, to this point no fundamental roadblocks to further experimental progress have emerged. On the software engineering side, more insights are needed regarding economically relevant applications for which quantum computing and simulation would bring a significant speed-up (see e.g. [Troyer, 2015]). Overall, there is a need for intensifying interdisciplinary research, bringing together computer and information science, physics and engineering. Time scale estimates tend towards the achievement of some science and engineering goals related to special purpose applications in less than or around 10 years while universal quantum computing is considered to be more than 10 years, possibly several decades away (see e.g. [Gil et al., 2015], [Quantum Manifesto, 2016]).

[2] For accounts of the advances referred to in this paragraph, see for example [Ladd et al., 2010], [Buluta et al., 2011], [Van Meter et al., 2013], [Monroe et al., 2013], [Devoret et al., 2013], [Stern et al., 2013], [Georgescu et al., 2014], [Carolan et al., 2015], [Montanaro, 2016].

In terms of private R&D investment[3], it is interesting to note that a number of targeted private and public-private R&D activities have been promoted steadily on a long term time scale of one and more decades[4]. Further activities have been launched recently[5]. Also, a first analogue machine promising a quantum speed-up in optimization tasks has become commercially available and has been acquired by private and public-private customers as part of their R&D investment[6]. On the software engineering side, some start-ups have emerged with activities related to systematic software development and to the evaluation of future quantum computing needs for customers in e.g. the finance sector.

These activities point to a growing interest. However, apart from the cases of a few high-risk start-ups and private sponsorships, corporate investments seem to remain at a small fraction of total R&D spending of the respective companies and hence do not entail a high risk[7]. This indicates that the activities have exploratory character and are being carried out in the pursuit of low-risk first mover advantages (the risk of not-exploring being higher than that of exploring with results of no or limited value). The investment reflects the need for new solutions rather than providing a measure of the likelihood of success.

Evidence from patent data is roughly in line with these observations[8]: Patenting activity started in the early 90s. It has persisted since then at a seemingly overall low or moderate level. Substantial portions of patent applicants can be associated with corporations headquartered in the USA and in Japan, as well as with D-Wave Systems in Canada and technology transfer activities connected with the University of New South Wales in Australia.

Overall, developments in quantum computing and simulation over the last 20 years support the view that it is important to consider this work in addressing future challenges in computing.

3.3 Policy Issues and Related Questions

At the science-industry-policy interface, the challenge of future computing, including quantum computing, is associated with the following issues:

---

[3] The transition from quantum science to quantum technology R&D is continuous. It seems reasonable to link increase of interest in quantum technologies with increase of private funding. However, note that in countries such as Canada and the USA, private sponsorship for research is common for all types of research including fundamental. For example, private funding for the Institute for Quantum Science and Technology in Calgary, Canada does not necessarily map onto the proportion of exploitation oriented work of the institute. Also, note that some research groups, including European, carry out company sponsored research (e.g. for Microsoft) that is, eventually, exploitation oriented even though the group's primary orientation remains fundamental work.

[4] For example by: IBM Research, Bell Labs, NTT, Toshiba, Hitachi, D-Wave Systems, University of Waterloo/Quantum Valley Investments (Institute for Quantum Computing)

[5] For example by: Google, Google/NASA/Universities Space Research Association (QuAIL, Quantum Artificial Intelligence Lab), Microsoft, Alibaba/Chinese Academy of Sciences, Airbus Defence & Space, University of Delft/TNO (QuTech centre), UK NQIT Quantum Technology Hub, University of Oxford/Nokia/Lockheed Martin, University of Southern California/Lockheed Martin, Rigetti, 1Qbit, QxBranch, Atos/CEA, Niels Bohr Institute/DTU/Aarhus University (Qubiz center), IBM/Samsung/Honda/JSR (IBM Research Frontiers Institute)

[6] D-Wave machines have been acquired by Lockheed Martin and the QuAIL consortium from 2011 on, including subsequent upgrades. Note that D-Wave Systems has now started selling computing time on their machine, in analogy to early business models with main frame computers in the 1950s and 60s.

[7] For example: Intel is investing 50 million USD in a 10-year collaborative relationship with the Qutech centre in Delft. The total annual R&D budget of Intel is of the order ~10 billion USD.

[8] See section 2.3 above for comments on the way patent data was analysed. For quantum computing, a narrow query containing "quantum computer" was employed. A large variety of key words would be needed to assess the overall intensity of patent activity. Yet, the observations made here appear consistent with the outcome of a broader query (For comparison, see the patent review of the UK Intellectual Property Office [UK Intellectual Property Office, 2013]).

- How to promote advances in computing to achieve competitiveness and benefit for Europe? - What? How? When?
- How to respond to changes brought along by future computing? - What changes? What socio-economic impact? How to seize opportunities and mitigate risks?

With this in mind, the following questions have been identified:

1. What roles could quantum computing play in mastering the IT challenges outlined above?

2. What applications of quantum computing can be conceived that lie beyond the reach of conventional computing and would be associated with high economic, societal or ethical stakes (high benefit/risk)?

3. Building on the previous two questions, which are the leverage points and drivers to promote quantum computing as part of an integrated view on future IT that optimally exploits its potential and mitigates risks?

4. Building on the previous three questions, what are relevant uncertainties to keep track of in promoting quantum computing and how can they best be coped with?

4. Sensing and Timing

Advances in the precision, size, cost and robustness of advanced atomic-optical-physics based instrumentation are leading to new sensors for acceleration, rotation, and gravitational and magnetic fields, improved atomic clocks and new methods of imaging. Quantum devices for sensing chemical and biochemical species have also emerged, based on quantum dots, nuclear magnetic resonance and quantum cascade lasers.

Most of these sensors are already used in research, and in fundamental metrology but, as far as public policy is concerned, what matters is that they are increasingly being found useful for wider purposes. Applications are very varied, including in power and telecommunications networks, navigation, medicine and civil engineering. Some quantum based sensors have obvious applications in defence and security, and may find their first applications there, especially where it is worth paying a high price for a modest improvement in performance or where there are strong constraints preventing the use of alternatives.

In a few cases, quantum sensors have opened up the prospect of entirely new applications but mostly, where new quantum sensors are being developed, alternatives are available, and the motive for development is to seek an improvement, such as in sensitivity, cost, size and portability, or to remove the need for special operating conditions. In some cases, new quantum sensors are competing with older devices which are themselves based on quantum principles.

A patent analysis for quantum sensors was included in a second UK government report [UK Intellectual Property Office, 2014], according to which there were 1,953 patents worldwide, for the period 2004-2013, with a slight reduction of the rate of patenting over the period. Japanese organisations were dominant, and patents relating to quantum sensor technology formed a relatively high fraction of total Japanese patent submissions. The latter was true to an even greater extent, of Australia. The sensor technology where patenting activity was strongest was magnetometry (see section 4.3).

4.1 Gravitation, rotation and acceleration

New types of sensors for these quantities are being developed based on the quantum technique of cold atom interferometry [Barrett et al., 2016]. The advantage of using atoms is that they move relatively slowly, and interact with the quantity being sensed for a relatively long time, enhancing the sensitivity. This technology also exploits quantum properties to "cool" the atoms, i.e. slow them down by interaction with laser beams to remove noise.

High precision accelerometers and rotation sensors are important because of their application in inertial navigation: from the cumulative effect of all the changes in velocity undergone, it is possible to infer the position of an object with respect to a known starting point. The advantage of inertial navigation over satellite navigation (GNSS), is that it can be used in tunnels, urban canyons, underwater or where radio signals have been jammed. In the past, it was seen as an expensive technology mostly confined to military use, but it is now more widely available, even to the consumer market. Accelerometers and rotation sensors based on atom interferometry could substantially improve the precision. Stakeholders here are navigational equipment manufacturers, aerospace and maritime manufacturers and agencies. The potential user community could expand and perhaps, in the long term, it could even substitute GNSS in the consumer market.

Interferometry with laser-cooled atoms can be used to measure the local acceleration due to gravity, by putting the atoms in free-fall or trapping them in an "optical lattice" of laser beams [De Angelis et al., 2009]. Atom interferometric gravimeters already

compete in accuracy with conventional instruments based on macroscopic falling masses or springs and masses, and further improvements are believed possible. Instruments are now being developed for civil engineering and construction, to aid in the location of buried objects, especially infrastructure such as pipelines and underground service chambers. Significant improvements to gravimeters could revive their use in mineral exploration, where they have mostly been superseded by seismographic methods. Other possible geophysical applications are monitoring water levels in aquifers, detecting and monitoring earthquakes and volcanic eruptions, monitoring ocean circulation currents and ice-mass parameters, and the supervision of carbon sequestration.

So, it is apparent that quantum sensors could have applications in areas with large markets and societal significance, and possibly drive changes in regulation and standardization. However, the impact depends critically on the practical superiority of the new quantum sensors over alternative techniques, which has not been fully demonstrated for any of them.

4.2 Time

Atomic clocks are one of the best well-established quantum technologies (since 1949) and are used to define Coordinated Universal Time (UTC), via the network of national metrology laboratories. In fundamental time-metrology, optical atomic clocks i.e. using visible wavelengths, are surpassing in precision the current caesium fountain microwave standard clocks, so a revision of the fundamental standard for time is in prospect[9]. At this level of precision (up to 1 part in 10^{18}) a necessary infrastructure is a dedicated fibre distribution network, because the satellite links currently used to coordinate time standards from different national metrology labs themselves introduce small errors which would negate the advantage of more precise fundamental standards [Gibney, 2015]. Projects are underway to develop this. For example, in the EURAMET EMRP project SIB02 NEAT-FT, new techniques were investigated for phase-coherent comparison of remotely located optical clocks, separated by distances of up to 1500 km using optical fibre links. In April 2015, a study group of the Bureau International des Poids et Mesures (BIPM) was established to follow developments on the realization of optical fibre links for time and frequency transfer[10]. Europe is in a very strong position in this area because there are several European national metrology labs with state of the art optical clocks.

Users of precise time include telecommunications and power companies, for network synchronization, and the financial sector, for timestamping high-speed trading [Beddington et al., 2012]. The UK's National Physical Laboratory already offers its NPLTime® service, a certified precise time signal distributed over fibre, to users in the London financial district. Another goal of development is to reduce the equipment requirements to receive precise time via fibre optic link from this type of service, to the point where it will become a generally available commodity.

One of the most developed applications of atomic clocks is for Global Navigation Satellite Systems, such as Galileo and GPS. Although sophisticated in detail, the basic concept is simple: distances are inferred from the time taken for a radio signal to propagate between the receiver on the ground and the satellites. It is reasonable to expect that

[9] The caesium fountain clock also uses quantum principles, so this is an example of a new quantum technology competing with an older one.

[10] SGF, a Study Group focusing on Optical Fibre Links for UTC, under the CCTF Working Group on Coordination of the Development of Advanced Time and Frequency Transfer Techniques (WG-ATFT). SGF will focus on the developments and achievements in the field of frequency and time transfer using optical fibres, aiming at the comparison of atomic clocks, the comparison of timescale, the dissemination of time and frequency standards and of UTC to users.

atomic clocks will become smaller, lighter and cheaper over time, reducing some costs of replacement satellites for GNSS constellations[11].

It is also common practice to use the time signal from GNSS satellites for other timing applications, because it is cheap and readily available. So ubiquitous is this technique, that when experimental jamming of GNSS has been conducted in limited areas, it has sometimes caused unexpected failures in systems whose administrators were unaware that they depended on GNSS time.

4.3 Magnetic Fields

Magnetometry is another field where quantum sensor technology is already well-established, in the form of the superconducting quantum interference device (SQUID), alkali metal vapour, proton nuclear magnetic resonance and Overhauser-effect magnetometers. These instruments have geophysical applications, similar to the ones listed above for gravimeters, and for location of buried objects including bombs and unexploded ordnance.

Of current interest is a new solid state technology based on negatively charged nitrogen vacancy (NV^-) centres in diamond, which are defects in the crystal where one of the carbon atoms is absent and a neighbouring one is replaced by a nitrogen atom, and which can absorb and emit photons. This process is affected by magnetic fields and can be used to make very sensitive optically-based magnetometers [Rondin et al., 2014]. They have the potential to bring techniques involving measurements of extremely small magnetic fields, e.g. from human brain activity, or from single molecules, currently restricted to research environments, into more widespread use. SQUIDs can achieve both of these measurements, but they require cryogenic cooling, whereas NV^- centre magnetometers function at room temperature.

However, there are other methods of magnetometry, some of which are cheap simple and robust, and some which can achieve almost as high precision. Elimination of cryogenic cooling is not enough to allow one easily to exploit the maximum sensitivity in a clinical environment, or in a geophysical field survey, because extremely precise magnetometry also requires the careful exclusion of interference from stray fields. It is not yet known whether there are applications of nanoscale magnetic imaging outside research.

4.4 Chemical detection

Several chemical detection techniques exploit quantum effects which appear, or can be engineered to appear, in nanoscale semiconductor structures. The two most important are quantum dots and quantum cascade lasers.

Quantum dots are nanoscale semiconductor crystals with unique optical properties, including being excellent light emitters. The quantum physics underpinning this is a simple relationship between the size of the quantum dot and the energy levels. However, going beyond this, researchers have found that the fluorescence of the quantum dots is critically affected by the nature of the surface, and techniques have been devised to customize them to be sensitive to specific chemicals. They potentially offer a useful tool for law-enforcement, e.g. in detection of explosives and narcotics. They can also be customized to be sensitive to biochemicals including nucleic acids, proteins and enzymes, with potential applications in medicine. [Frasco and Chaniotakis, 2009]

[11] A public consultation on European Space Strategy, was launched by the Commission on 19th April 2016, to collect views on the objectives of the EU future space strategy, the main challenges and opportunities for the European space sector, as well as the future of EU space programmes, prominently including Galileo.
See https://ec.europa.eu/eusurvey/runner/SpaceStrategy

Quantum cascade lasers are mid-infrared lasers based on quantum wells created in stacks of layers of different semiconductors. They can achieve very high output power, tuneable over a wide range, and can be used for spectroscopic stand-off substance detection i.e. at a distance of many metres, again with high potential for security applications [Li et al., 2015].

Stakeholders here include police and border forces, airports and seaports, forensic services, and security equipment industry associations and manufacturers

4.5 Imaging

Quantum phenomenon can be used to overcome limits on imaging, enabling useful images to be generated in circumstances where it would otherwise be impossible [Genovese, 2016]. Classical optical techniques assume that light is mathematically continuous. Its true nature, consisting of discrete photons, manifests as "shot noise", which limits the performance. Quantum techniques, which take the existence of photons into account, can overcome the shot-noise limit. It is also possible, using entangled beams, to overcome limits caused by the presence of other types of noise, and by background light, which would make classical imaging impossible, referred to as quantum illumination. A quantum understanding of light has also been used to overcome the limit on microscope resolution set by the wave nature of light.

Ghost imaging is a technique using two light beams, one of which directly illuminates the object and one of which does not, the direct beam being measured using a detector with no spatial resolution. It was originally conceived as a quantum technique, but it has subsequently been shown that it may be achieved using classical light.

Quantum imaging has high potential for use in industry, and in defence and security, where there is a need to see through turbid media, or in the presence of noise or background light.[12]

4.6 Policy Issues and Related Questions

For this category, there are two central questions. The first is whether the markets will be sufficiently large to be economically significant. This will affect whether a policy response is required, and what form it might take, to foster the development of the sector and, in the longer term, to regulate or standardise it. The second question is whether there are specific opportunities or risks, such as in security or health. These questions are both arguably more urgent than the policy-related questions for quantum computing, and the more technologically ambitious forms of quantum communications, because the time to market for the sensors, imaging devices and clocks could be shorter. Some instances are:

1. What are the positive and negative implications for GNSS of improved clocks and inertial sensors? What does this mean for policy on development of GNSS systems?

2. Unlike GNSS, inertial navigation cannot be legitimately blocked for law-enforcement, for example, when intelligence had been obtained indicating that a terrorist group intended to use electronic navigation to detonate a bomb at a specific location. Does the potential security threat from cheap, simple-to-use

[12] We mention for completeness that quantum dots are now being applied in displays and televisions, by companies including Philips, Sony, Samsung, LG and TCL, for a potential market of the order of billions of euro. [Perry, 2015]. However, they are used as simple light-emitters and the devices are not an example of an exploitation of a subtle or deep quantum property.

inertial navigation outweigh the societal advantage? Would it be feasible or unfeasible to regulate its proliferation?

3. Will quantum sensors of acceleration, rotation, gravity and magnetic fields have practical advantages over existing technologies in more than a limited range of circumstances? Will the markets be large enough to justify the development investment, including possible public funding?

4. Will the drive towards ever greater precision of optical clocks have implications outside fundamental metrology?

5. Is improving the distribution and availability of ultraprecise time more important to society than further improving the precision?

6. Is there a need for a European, terrestrial, precise time distribution network, accessible by users without specialist laboratories, to guard against the possible non-availability of GNSS time?

5. Conclusions

In this report, we have identified policy-related issues arising from the emergence of quantum technologies. We consider quantum approaches to secure communications; computing and simulation; and sensing and timing. We give some contextual background for each of the application areas, and raise questions to stimulate a debate from which implications for European policy should emerge.

To address these questions, the Joint Research Centre is seeking input from those with professional knowledge of the actual and envisaged applications, of the devices and systems themselves, of new prospects arising from research, of conventional and competing technologies, of the markets, and of the relevant societal and public policy issues. As part of this, the JRC is holding a series of workshops, each focused on issues related to a specific application area.

To express your interest in participating in our study, please contact us at

jrc-quantum@jrc.ec.europa.eu

References

1. COM(2016) 178 Communication on the European Cloud Initiative - Building a competitive data and knowledge economy in Europe, 19 April 2016
2. SWD (2016) 107 Commission Staff Working Document on Quantum Technologies, 19 April 2016
3. "Quantum Manifesto: A New Era of Technology", Draft (2016)
4. V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems", Special Issue of Theoretical Computer Science to celebrate 30 years of BB84, Vol. 560, Part 1, p. 27 (2014)
5. L. Lyderse, C. Wiechers, C. Wittmann, D. Elaser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination", Nature Photonics, Vol. 4, p. 686 (2010)
6. D. Elser, S. Seel, F. Heine, T. Länger, M. Peev , D. Finocchiaro, R. Campo, A. Recchia, A. Le Pera, T. Scheidl, R. Ursin , and Z. Sodnik, "Network architectures for space optical quantum cryptography systems", Proceedings of the International Conference on Space Optical Systems and Applications (2012)
7. R.J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P.J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory", Phys. Rev. Lett. Vol. 113, p. 040502 (2014)
8. R. Alléaume, T.E. Chapuran, C.J. Chunnilall, I.P. Degiovanni, N. Lutkenhaus, V. Martin, A.Mink, M. Peev, M. Lucamarini, M. Ward, and A. Shields, "Worldwide standardization activity for Quantum Key Distribution", Globecom Workshop "Telecommunications Standards, from Research to Standards" (2014)
9. UK Intellectual Property Office, "Quantum Technologies: a patent review for the Engineering and Physical Sciences Research Council" (2013)
10. UK Government Communications Headquarters, "Quantum Key Distribution", White Paper by the Communications-Electronics Security Group (2016)
11. USAF Scientific Advisory Board Study, "Utility of Quantum Systems for the Air Force", Abstract (2015)
12. Industrial and Commercial Bank of China, "ICBC Leads Application of Quantum Technology in the Financial Field", press release (2015) http://www.icbc.com.cn/icbc/newsupdates/icbc%20news/ICBCLeadsApplicationofQuantumTechnologyinFinancialField.htm
13. B. Schneier, Blog "Schneier on Security" (2008) www.schneier.com/essays/archives/2008/10/quantum_cryptography.html
14. Hoi-Kwong Lo, "Will quantum cryptography ever become a successful technology in the marketplace?", arXiv:quant-ph/9912011v1 (1999)
15. T. Jennewein and E. Choi, "Quantum Cryptography market study and business opportunity assessment", Institute for Quantum Computing, University of Waterloo (2014)
16. M.M. Waldrop, "More than Moore", Nature Vol. 530, p. 144 (2016)
17. Semiconductor Industry Association and Semiconductor Research Corporation, "Rebooting the IT Revolution: A Call for Action", report based on the workshop "Rebooting the IT Revolution" held March 30-31, 2015 in Washington, DC (2015)

18. T. Cross, "After Moore's Law: Double, double, toil and trouble", The Economist, Technology Quarterly, Quarter 1 (2016)

19. P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20–22, 1994, IEEE Computer Society Press, p. 124 (1994)

20. T.D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe and J.L. O'Brien, "Quantum Computers", Nature Vol. 464, p. 45 (2010)

21. I. Buluta, S. Ashab, and F. Nori, "Natural and artificial atoms for quantum computation", Rep. Prog. Phys. Vol. 74, p. 104401 (2011)

22. R. Van Meter and C. Horsman, "A Blueprint for Building a Quantum Computer", Communications of the ACM Vol. 56, p. 84 (2013)

23. C. Monroe and J. Kim, "Scaling the Ion Trap Quantum Processor", Science Vol. 339, p. 1164 (2013)

24. M.H. Devoret and R.J. Schoelkopf, "Superconducting Circuits for Quantum Information: An Outlook", Science Vol. 339, p. 1169 (2013)

25. N. Stern and N.H. Lindner, "Topological Quantum Computation – From Basic Concepts to First Experiments", Science Vol. 339, p. 1179 (2013)

26. I.M. Georgescu, S. Ashhab and F. Nori, "Quantum simulation", Rev. Mod. Phys. Vol. 86, p. 153 (2014)

27. J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N.J. Russell, J.W. Silverstone, P.J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G.D. Marshall, M.G. Thompson, J.C.F. Matthews, T. Hashimoto, J. L. O'Brien and A. Laing, "Universal linear optics", Science Vol. 349, p. 711 (2015)

28. A. Montanaro, "Quantum algorithms: an overview", npj Quantum Information Vol. 5, p. 15023 (2016)

29. Advanced Research and Development Activity (ARDA), "A Quantum Information Science and Technology Roadmap: Part 1 Quantum Computation", Report of the Quantum Information Science and Technology Experts Panel, produced for ARDA, version 1.0 (2002); version 2.0 (2004)

30. P. Zoller (ed.), "Quantum Information Processing and Communication: Strategic report on current status, visions and goals for research in Europe", version 1.0 (2005)

31. M. Troyer, "High Performance Quantum Computing", lecture at QUTE-EUROPE Summer School (2015), http://www.chalmers.se/en/departments/mc2/education/Events/Quantum%20Simulation%20and%20Computation

32. D. Gil and C. Peranandam, "A quantum of possibilities: The business advantages of taking the quantum leap", IBM Center for Applied Insights, IBM Corporation (2015)

33. E. Gibney, "Hyper-precise atomic clocks face off to redefine time", Nature Vol. 522, p. 16 (2015), doi:10.1038/522016a

34. J. Beddington et al., "Foresight: The Future of Computer Trading in Financial Markets, Final Project Report", The Government Office for Science, London, (2012)

35. D. Barrett, A Bertoldi and P Bouyer, "Inertial quantum sensors using light and matter", arXiv: 160303246v1 [physics.atom-ph], (2016)

36. M. De Angelis et al., ”TOPICAL REVIEW Precision gravimetry with atomic sensors”, Meas. Sci. Technol. Vol. 20(2) 022001, (2009), doi:10.1088/0957-0233/20/2/022001

37. L. Rondin et al., ”Magnetometry with nitrogen-vacancy defects in diamond”, arXiv:1311.5214v3 [cond-mat.mes-hall] (2014)

38. M. F. Frasco and N. Chaniotakis, “Review: Semiconductor Quantum Dots in Chemical Sensors and Biosensors”, Sensors Vol 9(9), p. 7266 (2009), doi:10.3390/s90907266

39. J. S. Li et al., “Contributed Review: Quantum cascade laser based photoacoustic detection of explosives”, Rev. Sci. Instrum., Vol 86, p. 031501 (2015), http://dx.doi.org/10.1063/1.4916105

40. M. Genovese, “Real applications of quantum imaging”, ArXiv:1601.06066v1 [quant-phy] (2016)

41. T Perry, “CES 2015: Placing Bets on the New TV Technologies”, IEEE Spectrum, 7 Jan 2015

List of abbreviations and definitions

BIPM Bureau International des Poids et Mesures

CCTF Consultative Committee for Time and Frequency

CESG (originally) Communications-Electronics Security Group

DARPA Defense Advanced Research Projects Agency

EMRP European Metrology Research Programme

ETSI European Telecommunications Standards Institute

EURAMET European Association of National Metrology Institutes

FET Future and Emerging Technologies

GNSS Global navigation satellite system

GPS Global Positioning System

HPC High performance computing

IRDS International Roadmap for Devices and Systems

ITRS International Technology Roadmap for Semiconductors

JRC European Commission Joint Research Centre

NIST National Institute of Standards and Technology

NMR Nuclear magnetic resonance

NSCI National Strategic Computing Initiative

NV^- Negatively charged nitrogen vacancy

QKD Quantum key distribution

SBIR Small Business Innovation Research

STTR Small Business Technology Transfer

SECOQC Development of a Global Network for Secure Communication based on Quantum Cryptography

SQUID Superconducting quantum interference device

UTC Coordinated Universal Time

List of figures

Europe Direct is a service to help you find answers to your questions about the European Union
Free phone number (*): 00 800 6 7 8 9 10 11
(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server http://europa.eu

How to obtain EU publications

Our publications are available from EU Bookshop (http://bookshop.europa.eu),
where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.
You can obtain their contact details by sending a fax to (352) 29 29-42758.

LB-NA-27915-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/384376

ISBN 978-92-79-58276-9