Responsible Innovation in Quantum Technologies applied to Defence and National Security

Philip Inglesant, Marina Jirotka, Mark Hartswood

NQIT Networked Quantum Information Technologies

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UK National Quantum Technology Hub Sensors and Metrology

QUANTUM COMMUNICATIONS HUB

QUANTIC

NQIT (Networked Quantum Information Technologies) is funded by the Engineering and Physical Sciences Research Council and is a part of the UK National Quantum Technologies Programme

EPSRC
Engineering and Physical Sciences
Research Council

UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME

Author: Dr Philip Inglesant, Professor Marina Jirotka & Dr Mark Hartswood
NQIT Responsible Research and Innovation (RRI)

Design & layout: Elle Styler, based on a design by Hunts

Contact: engage@nqit.ox.ac.uk

TABLE OF CONTENTS

Introduction

This Briefing is the outcome of a workshop held in Oxford in October 2016 and also draws on interviews and a review of the literature in defence, technology, and quantum technologies. It presents issues for consideration by policy makers and innovators responsible for applying quantum technologies to defence and national security. It addresses the challenges of adopting these technologies in a responsible way in a complex market economy and changing international operating environment.

Key Points

- Defence and national security are some of the main application areas of technology, including quantum technologies. Technology has an increasingly important role to play to meet the context of new and rapidly changing defence risks.

- There is increasing overlap between commercial and defence technologies. Defence no longer receives the lion's share of research funding, but defence is still a major customer of advanced technologies; at the same time, defence has often led the way in the development of new technologies which go on to be widely used in consumer devices and services: as we see today with the Internet and GPS.

- But society's increasing reliance on technology also opens up vulnerabilities, and could open them up for mis-use by terrorists or criminals.

- Quantum technology refers to emerging technologies which are harnessing the properties of quantum physics to enable new capabilities. Some of these capabilities are qualitatively new. For others, there already exist conventional technologies that can provide the functionality, but using quantum methods can give significant advantages - in some cases orders of magnitude in scale - in terms of sensitivity, accuracy, speed, or ease of use.

- Technology has been exploiting quantum effects for decades in applications such as lasers and semi-conductors. Quantum technology in the sense used here harnesses quantum properties directly, with the potential for new products which could change our lives profoundly. However, there is a spectrum rather than a clear distinction between these established and emerging quantum technologies.

- The user of the technology is interested in the capabilities rather than the underlying science. Moreover, there is a range of application areas (detailed below), of which the common feature is their innovative adoption, in different ways, of quantum physics.

Applications of potential interest for defence and national security include:

- Sensors, in particular, far more accurate gravity sensors, able to detect hidden objects or voids below ground;

- Applications to navigation, in places where GNSS[1] is not available, and to provide resilience against loss or jamming of GNSS;

- New forms of computing;

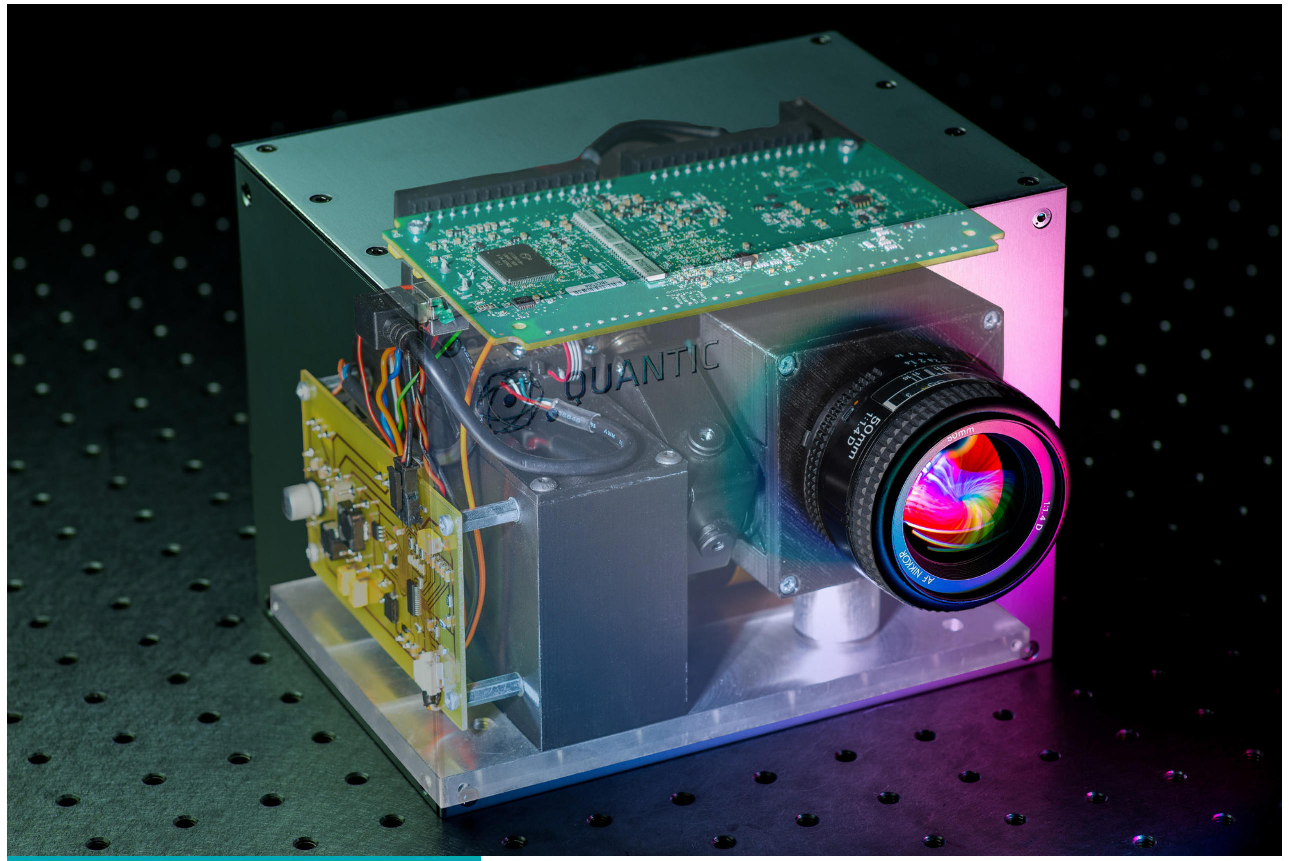
- New forms of secure communications; and

- Quantum imaging, able to detect gases, detect objects round corners. through buildings, fog, smoke or dust, or build images with very low light.

[1] Global Navigation Satellite Systems, for example GPS and Galileo

The UK is one of the world's leading investors in quantum technologies. The UK government is making a £270 million investment in a national quantum technologies programme, of which £120 million is invested in four quantum technology Hubs: quantum imaging - Glasgow, quantum communications - York, quantum sensors and metrology - Birmingham, and quantum computing - Oxford.

As these technologies emerge from the laboratory into civilian and defence applications, this is a privileged time to consider the Responsible Innovation (RI) implications; but it is also challenging to anticipate what these implications will be with technologies which are still far from widely deployed and adopted in society.



The Single Pixel Camera from QuantIC
in Glasgow, Scotland
Kevin Mitchell

Background

This Briefing has its origins in a workshop held at the Oxford Martin School in October 2016, attended by over thirty representatives of defence and security organisations, academia, and industry. The study also included desk research, literature review, and interviews. The authors are very grateful to the participants in the workshop and to others who took part in the case study.

The workshop addressed the ethical and social aspects of the application of quantum technologies to defence and national security. Its focus was on the overlap of three important areas of research: defence science and technology, quantum mechanics and emerging quantum technologies, and Responsible Innovation.

Technology has always played an important role in defence and warfare. Technology can give an advantage in the face of adversaries with greater numerical capacity or firepower; but countries also face an increasingly diverse range of threats. These threats involve not only military weapons, but also the adversarial application of readily available civilian technologies. There is a blurring of the distinction between civil and military technologies.

Quantum technologies are not, of course, the only sophisticated technologies with both civil and military applications; however, they deserve a particular focus, because of their potentially transformational properties. These transformations consist not only of making possible functions which are not possible by other means, but also in enabling improvements in the size, weight, power requirements, speed, or ease of use – in some cases, by orders of magnitude - over functionality provided by conventional technologies.

These powerful new technologies will bring changes to military as well as civilian applications. It is not possible to predict these with certainty, but if we do not try to look ahead and anticipate some of these implications, the disruptions will take us unawares. Once technology is widely deployed, it will be too late to change its trajectory; at best, the most negative impacts may be mitigated by regulation or international agreement [9].

Recognising this, Responsible Innovation [44, 52] is an emerging set of practices which brings together different groups of stakeholders, as was done in this workshop, to assess potential implications and to align the outcomes of science and technology with wider social needs and expectations.

The rest of this short paper will discuss the relevance of technology for defence and security, with a focus on the particular relevance of quantum technologies, leading into a discussion of the Responsible Innovation implications.

1. Technology for defence and national security

Technology is increasingly important for military and national security. On the one hand, advances in cyber, medical, materials science, and robotics technologies offer potential for our security and prosperity. At the same time, reliance on these technologies creates vulnerabilities to attack [23, 24]. A White Paper published by the UK Ministry of Defence [27] recognised that the widespread and rapid changes of technology bring new threats, which requires effective investment in defence and security science and technology.

1.1 The Changing Balance of Defence and Civil R&D

Technologies for defence can be seen as "offsetting" the advantages in terms of size or power held by an opponent. In the 1950's, the "New Look" policy built up the USA's nuclear deterrence; in the 1970's, a second offset strategy in the USA emphasised the development of intelligence, surveillance, precision-guided weapons and stealth aircraft. The US Department of Defense announced [31] in 2014 what has been called the Third Offset Strategy: new, long-term investments in innovation in the face of growing defence capabilities by other powers and a perceived falling behind by the USA and its allies. These investments are to focus on emerging technologies, including robotics, autonomous systems, miniaturisation, big data, and advanced manufacturing including 3D printing.

These technologies are emerging in a very different research and development environment from first and second technology offsets, however. The earlier offset strategies were built on technologies largely developed by and for defence; today, most investment in technology research and development is made by the private sector, and is overwhelmingly directed at civil technologies [36].

In the UK, government funded expenditure on civil R&D continues to outstrip government funding for defence R&D, while business funded R&D is much larger than either. Total defence spending is also declining: in the UK this stood at around 11.2% of GDP at the time of the Korean War, declined during the 1950's but was still around 7% GDP, and has fallen more or less steadily since the end of the 1960s (with a small rise following 9/11) to around 2.4 – 2.5% of GDP today [49].

At the same time, however, increasing use of open competition and off-the-shelf procurement, where possible, and focussed investments in technology and development are expected to reduce costs and overheads [27, 28]. However, since these technologies are also available to others, these technologies do not, in themselves, give an operational advantage, and there is also a need to maintain freedom of action, avoiding dependence on others [27].

Reflecting on this, a presenter at the workshop noted that the UK is well positioned to make a major contribution to the next generation of technology, including quantum technologies. The UK is a world leader in some aspects of these technologies, but the workshop heard that the total UK investment in quantum research and technology, around $US 500 million over five years, compares with a similar investment by the US Department of Defense and Google alone.

The UK is well positioned to make a major contribution to the next generation of technology, including quantum technologies.

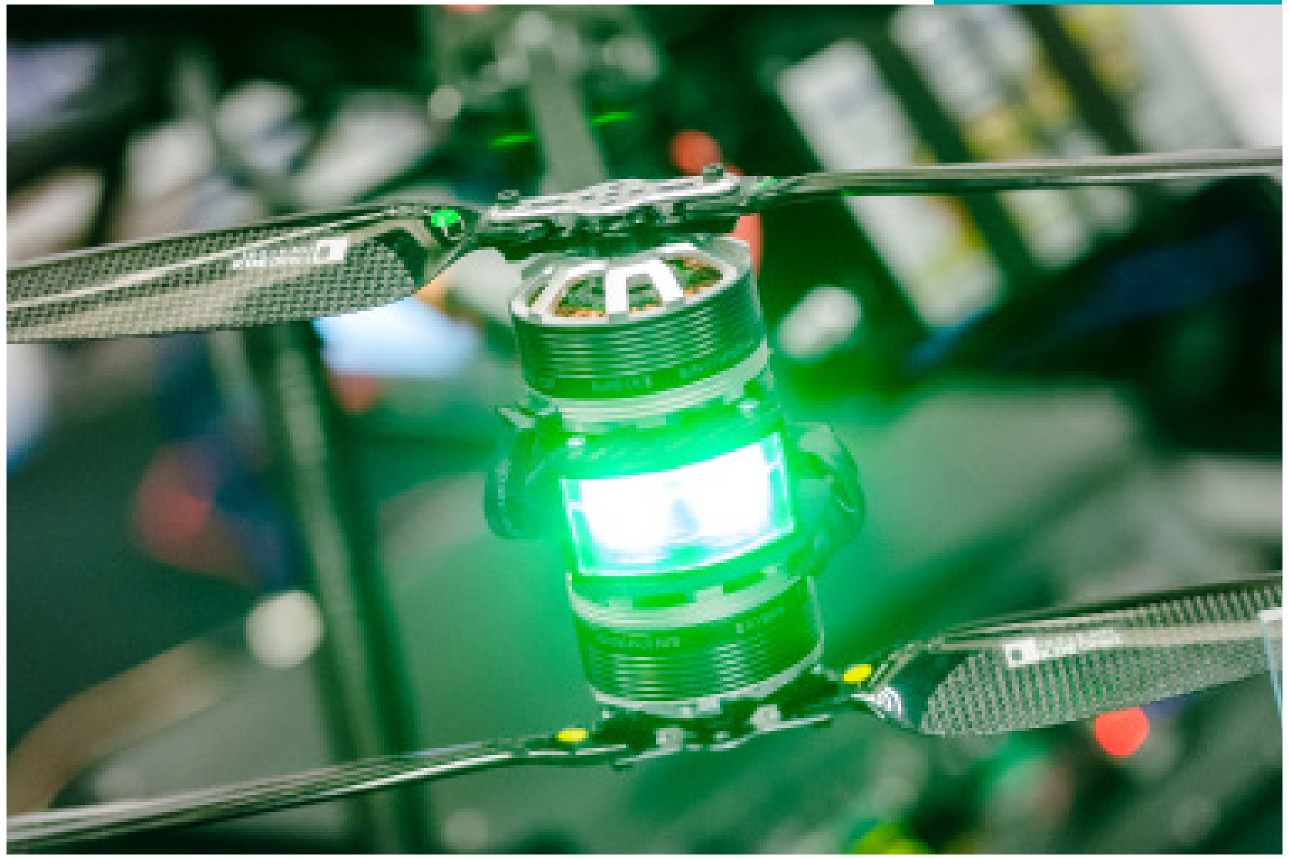
1.2 Dual use

Defence has often led the way in the development of new technologies which go on to be widely used in consumer devices and services [34]. Examples of non-quantum devices adapted for civilian use include thermal imagers for "seeing in the dark" and liquid crystal displays. The UK's defence science and technology laboratory, Dstl, has set up its own company to enable wider exploitation of technologies originally developed for defence applications[2].

Conversely, technologies can also open up new vulnerabilities. "Dual use" can refer to military technologies adopted for civilian benefits, but also to the use of readily available technologies for aggressive applications by non-state as well as state actors; for this reason, some technologies are subject to trade restrictions [11, 27]. Well-known export control regimes for arms and dual-use technologies include the USA International Traffic in Arms (ITAR) Regulations [50], and the Wassenaar Arrangement [46], which aims to avoid arms proliferation and contribute to regional and international stability.

This dual face of technology, opening up new threats and new attack vectors from non-state as well as state actors, while also providing an important part of the defence against them, is part of the increasingly complex strategic context in which countries now find themselves [12]. A presentation to the workshop discussed how technology, in the broadest sense, opens out boundaries while in other ways constructing new boundaries, sometimes literally but also by conditioning social behaviour in more subtle ways. For example, consider how the deployment of tanks changed warfare.

Drone-mounted gravity sensor being developed by the Quantum Sensors & Metrology Hub
Dan Tsantilis, EPSRC



[2] http://www.ploughshareinnovations.com/

2. Quantum Technologies

This, then, is the background in which technologies assume an increasing importance for defence and national security. This section considers the role that quantum technologies, in particular, can play.

Quantum technology can be described as the use of some of the properties of quantum mechanics, such as quantum entanglement and quantum superposition, for practical applications. Applications currently identified are generally classified as: quantum computing, quantum sensors, quantum-secured communications, quantum metrology and sensing, and quantum imaging.

New developments in quantum technologies promise to harness the properties of quantum physics to enable new capabilities which will affect our lives profoundly [47]. Science and engineering are progressing rapidly towards making these technologies a reality. Workshops in 2013 and 2016 at the Royal Society's Chicheley Hall explored how the UK might exploit emerging quantum technologies for defence, security, and the wider UK economy; one of the outcomes is a very useful survey of the landscape of these technologies [10].

New developments in quantum technologies promise to harness the properties of quantum physics to enable new capabilities which will affect our lives profoundly.

Technology has been exploiting quantum effects for decades: quantum mechanics is the essential underpinning for many existing technologies such as lasers and semi-conductors. But quantum technology in the sense used here goes beyond these existing technologies because it makes direct use, and in some cases manipulates, these quantum properties [21]. These are sometimes called "the second quantum revolution" technologies [13]; but some participants in the workshop questioned this idea: rather than a clear separation from one generation to another, there has been a range of intermediate developments, and this is continuing with the gradual emergence of these new technologies.

The counter-intuitive properties of quantum offer enormous potential for exciting new products, for civil as well as defence applications; but there is still a great deal of uncertainty about what can be achieved and when we can expect to see fruition. Some of these technologies are close to market, while others are still very experimental. Moving from the laboratory to industry to widespread adoption presents engineering and manufacturing challenges, may be disruptive, and will require market confidence and the development of supply chains [21].

Another potential – but still quite theoretical – avenue of investigation could harness quantum biology. This, the focus of a keynote presentation in the workshop, explores phenomena in living creatures which are believed to make use of quantum effects. Quantum effects produced in a laboratory are very fragile, but living organisms seem to have found a way to use quantum in ways that we do not yet understand. If we could understand and replicate these effects, they could have many potential applications.

2.1 The UK national strategy for quantum technologies

The UK is one of the world's leading investors in quantum technologies, supported by a vibrant research community. Recognising the potential, the UK government is making a £270 million investment in the UK national quantum technologies programme [47], of which £120 million is invested in four national quantum technology Hubs (Glasgow, York, Birmingham, and Oxford), each focussing on a key topic in quantum technology: quantum imaging, quantum communications, quantum sensors and metrology, and quantum information technology.

The overall programme is a coordinated effort between the industry, led by Department for Business, Energy and Industrial Strategy (formerly BIS), Innovate UK, and the National Physical Laboratory, research funders such as the Engineering and Physical Sciences Research Council, and defence and national security led by the Ministry of Defence, the Defence Science and Technology Laboratory and Government Communications Headquarters.

2.2 Is quantum qualitatively different – or an enhancement of existing capabilities?

Quantum physics as an area of study is no longer particularly new, but originated in a burst of activity between 1900 and 1930. The kind of world described by quantum mechanics is hard to conceptualise in physical terms, but the mathematics that describes it is clear and consistent, and extraordinarily successful as a theory.

Rather than a big step-change, there is a spectrum of quantum technologies, and many of the applications of quantum can also be done in conventional ways. But even in these cases, methods based in quantum mechanics could enable applications which are faster, more accurate, smaller, cheaper, or in other ways better, in some cases by orders of magnitude [34, 45, 51].

A common theme throughout the workshop was a debate about the exceptionality of quantum technologies. The technologies are quite different from one another in their applications: is it helpful to categorise quantum technology as a whole, and is it qualitatively different from other technologies?

A common theme throughout the workshop was a debate about the exceptionality of quantum technologies.

For the user of the technology and for policy makers, it is the capabilities of the technology which are of interest. Often, users of the technology may be unaware of the quantum physics which underlies it. Conversely, raising awareness of the potential applications of quantum physics may help to overcome public fears, such as that quantum is very hard to understand or that it is not under control.

3. Defence and security applications of quantum technologies

Defence and national security are likely to be among the first domains to adopt these emerging technologies: particularly quantum-enabled clocks, quantum navigators, quantum gravity sensors and quantum imaging [48].

There are important potential applications, but this needs to be tempered by the fact that many quantum technologies are either still at a theoretical stage, or are still in early development [51]. The workshop considered in particular four quantum technologies which are relatively advanced, and one which is still some way distant.

Quantum gravity sensors, quantum navigation, and quantum imaging are available for early adopters but are not yet consumer products [48]; quantum secured communications is available commercially, but with limitations in terms of distance and usability [16, 32, 38]. Meanwhile, fully capable quantum computing is still some years away, but the theory which will make this possible is developing rapidly, and forms of quantum computing and quantum simulation are already available in early forms.

3.1 Quantum sensors, gravity meters and navigation

Quantum meters for measuring gravity are able to detect the local gravitational field. Gravimeters as such are not new and do not necessarily rely on quantum technologies; these already have applications for mineral prospecting, seismology, and detecting underground features in surveying. However, quantum-based gravimeters are now leaving the laboratory and promise greater sensitivity and reliability, and will potentially be easier and faster to use and more stable and robust against external noise sources [8].

Fast and accurate gravity sensing could, among other applications, enable detection of nuclear submarines by sensors of sufficient sensitivity, because, although, according to Archimedes' principle, a submarine has a mass nearly equivalent to the water it displaces, the mass of the submarine is not uniformly distributed. This is still theoretical and, as we discuss below, realising it would be a vast challenge, but methods of harnessing quantum effects to detect submarines have been proposed [26].

This not a new idea [30], but is part of the technological capability, which, in this and other ways, is changing the cat-and-mouse game, a race between detection and stealth which has continued ever since the sinking of British ships by German U-Boats in 1914 [26, 35]. The key point about gravity measurement is that it is fully passive, unlike (active) sonar, and hence not detectable by the object of interest. However, although plausible in the future, this would require levels of sensitivity that are currently beyond the state of the art, and there are also operational requirements (measurement speeds, noise removal, difficult marine environment, etc.) which would need to be overcome, so that realising this in practice would be a huge challenge.

Navigation is a related area of application since similar quantum techniques could provide precise inertial measurements such as of acceleration and rotation. Quantum navigation could be far more accurate than existing accelerometers and gyroscopes, and provide an alternative to global navigation satellite systems (GNSS), such as GPS, if GPS fails or in places where GPS is not available.

Again, this could transform the operational capabilities of submarines, which, being under water, are generally unable to use GNSS; it would also enable other new applications by providing navigation in indoor or subterranean locations. There is also concern that GNSS are vulnerable to failure or interference; many systems are now dependent on them, not only for navigation but also for timing - quantum clocks are another rapidly developing area [21]. As with some other quantum technologies, there are still challenges to be overcome, such as accumulation of errors over a long time scale.

3.2 Quantum imaging

There are other quantum technologies widely discussed in the literature and presented at showcases. Quantum imaging — the focus of Glasgow-based QuantIC, the UK Quantum Technology Hub in Quantum Enhanced Imaging in the UK National Quantum Technologies Programme — takes advantage of the quantum nature of light to record and enhance an image, or record light which has its behaviour altered on a quantum scale [42]. This can involve combining measurement and computational methods with the aim of forming images even when the measurement conditions are weak, few in number, or highly indirect [3, 29]. QuantIC's imaging technologies have applications across many industry sectors including defence[3]. The QuantIC Hub's "Hidden Object Tracker", a camera system developed with Thales, enables the detection of objects and movement outside the line of sight ("seeing round corners"). This has obvious defence applications if an enemy combatant could be revealed, as well as in civil applications such as making autonomous vehicles safer.

The ability to see through scattering or obscurant media – such as fog, smoke, dust or clouds - has safety applications in a number of defence scenarios, for example in a brownout where there is a loss in pilot visibility associated with the dust cloud created by a helicopter landing in a sandy environment. Many of these accidents could have been avoided had the pilot's vision not been compromised, or if an effective on-board imaging system had been deployed. Working with Sikorsky and Lockheed Martin, researchers at QuantIC are developing technologies to see through scattering media using the latest quantum technologies. These cameras can provide accurate and reliable visualisation in these scenarios and have the potential to significantly reduce the number of accidents [14].

[3] QuantIC hosted a workshop aimed at the Defence and Security sector, at QinetiQ in April 2016 [37].

3.3 Quantum computing and quantum secure communications

Quantum communication technologies enable new forms of secure communications, such as Quantum Key Distribution (QKD)-enabled cryptography, which could provide theoretically unbreakable "information in transit" security. These technologies are quite well advanced and commercially available, albeit with some limitations in practice [16, 21, 32]. Quantum Key Distribution has been demonstrated between ground and satellites (free space transmission), a technology in which China is now world-leading, having launched its own satellite in August 2016 [20, 38].

Quantum protocols such as QKD give unconditional, information-theoretic (that is, does not rely on assumptions about the resources available to an adversary), provably secure cryptography, protected by the laws of physics which guarantee that any interception would be detected (that is, it is resistant to eavesdropping on the communication channel). QKD has a theoretical proof of security against any future technologies. However, as with any cryptosystem, its practical security relies on correct implementation; known weaknesses in existing QKD implementations have been demonstrated since at least 2010 [19]; but quantum mechanics and various related techniques should enable attacks to be detected [16]. Careful analysis of the real security level of a cryptosystem, and development of techniques to detect intrusion and increase security, is an important area of study [16]. Note that QKD does not in itself solve other essential aspects of security such as verifying identities or access control [2, 32], although quantum communications does have potential in some of these areas, such as quantum signatures or quantum "tagging" [16, 21].

Meanwhile, a rather different set of applications of quantum computing to information processing is still some years distant, but already has important implications for simulations, logistics, and machine learning [43]. On the risk side and directly related to secure communications, there are already known quantum algorithms which would break existing forms of Internet encryption [15], although, so far, there are no quantum computers of sufficient power to implement them at more than a trivial level[4]. In response to this known threat, researchers are already developing what is known as "post-quantum" or quantum-safe cryptography [6], which uses classical (that is, non-quantum) mechanisms to replace the current public key schemes which will become insecure if sufficiently powerful quantum computers become a reality. The US National Institute of Standards and Technology's (NIST) Computer Security Resource Center has initiated a process to evaluate and standardise quantum-resistant public-key cryptographic algorithms [33].

Although distinct, there are obvious overlaps between post-quantum cryptography and QKD, since both are concerned to ensure security into the future. The UK government's review of quantum technologies [21] recommends that quantum communications and cryptography research groups should work together leading to joint technical developments of both QKD and post-quantum cryptography as well as work on digital signatures and other uses of these technologies.

The current advice (which dates from October 2016) from the UK National Cyber Security Centre (NCSC) is that QKD is unlikely to be cost-effective, is hardware dependent, and opens a new set of possible avenues for attack, which are not yet well understood [32]. However, the NCSC and the UK government review both recommend that research and development of QKD systems should be actively pursued to ensure that the application of the technology becomes cost-effective, practical, and validated to explore the security of real-world QKD systems [21, 32].

As the NCSC notes, responsible innovation should be accompanied by independent validation, and indeed the UK government's review [21] recommends that NCSC and others form a partnership to test and accredit quantum communication equipment and services.

It is worth noting that the Quantum Communications Hub (York) currently has a Partnership Resource project working on exactly such validation for Quantum Random Number Generators, as a first step towards these recommendations. NPL is the independent validation body, underpinned by theoretical work from the University of York and overseen by NCSC. ETSI's White Paper is a good introduction to the challenges and solutions of quantum cryptography [16].

[4] However, when they do become available, powerful quantum computers will be able to break current communications which could be stored and decrypted in the future, so this is already a serious concern [16].

4. Responsible Innovation

Responsible Innovation is an emerging set of practices which have been developed to help all stakeholders to consider the social and ethical issues of new technologies, to ensure that new technologies are developed in the public interest, are ethically acceptable, economically, socially and environmentally sustainable, and socially desirable [52]. A framework to encapsulate the principles of Responsible Innovation (the Anticipate – Reflect – Engage – Act "AREA" framework, adopted by EPSRC) was presented to the workshop (A framework for Responsible Innovation, appendix below).

The UK national strategy for quantum technologies, of which the quantum technologies programme is a part, views Responsible Innovation not only as a way to help ensure that products and outputs are more likely to be embraced by the public, but also as an opportunity to enrich the innovation process by enhancing creativity [47].

Responsible Innovation has a special place for technologies, such as quantum technologies, which are new and still emerging; it was argued in the workshop that this puts us in a privileged position, as "custodians of the future".

However, in considering the future impacts of a new technology, there is a dilemma, characterised by Collingridge [9]: it is difficult to predict the impacts of a new technology which has still not been extensively developed and widely used, but, conversely, change is difficult once the technology has become entrenched.

Quantum technologies are still very much "upstream" and therefore open to shaping by various groups of stakeholders. These technologies are still open to a range of possible futures, some more desirable than others. It is therefore timely to think about the potential impacts of quantum technologies and particularly their applications for defence and national security, using the tools of Responsible Innovation, before the applications become "locked-in".

> *It is therefore timely to think about the potential impacts of quantum technologies and particularly their applications for defence and national security, using the tools of Responsible Innovation, before the applications become "locked-in".*

4.1 Responsible Innovation and Technology Assessment

Traditionally, responsibility for the impacts of science and technology has relied on a post-hoc, "consequentialist" response [22]. Technology Assessment in various forms was an early attempt to set a more future-oriented, forward-looking direction, but it still maintains the division of labour between technology "push" from research at one end and "pull" in terms of accountability to societal needs at the other.

In the workshop discussion, it was noted that some countries, such as Germany, have formal government-backed Technology Assessment offices; the USA was the model for these but the USA OTA was disbanded in 1995, its work continuing to some extent as part of the Government Accountability Office.

Like Technology Assessment, Responsible Innovation attempts to anticipate and balance the positive and negative effects of new technologies. However, Responsible Innovation goes further because it aims to identify more profound social changes and to consider the purposes of emerging technologies. It recognises that the pathway to innovation is rarely simple or linear.

Responsible Innovation applies at each level in research and innovation even from the level of "basic" research. It operates at all levels: research teams and partnerships, funders, research policy-makers, investors and technology implementers, and engagement with the public. Individual researchers have a part to play, but responsibility is not all on their shoulders. In this respect, the workshop suggested two specific sets of stakeholders with responsibility in the defence industry: systems engineers building technology into systems, and operational analysts defining the ways in which technologies are used in practice.

4.2 Responsible Innovation in Defence and National Security

Keeping the focus on quantum technologies as they might be applied to defence and security, what might responsible innovation in these areas consist of, in practical terms?

Responsible Innovation aims for a "proper embedding" [52] of scientific and technological advances in society; but these fundamental principles and ethical concerns raise the question of how these principles should be established, what a "proper embedding" might consist of, how this should be decided and how it might be achieved, and how these can be balanced in the particular case of technologies for defence and national security.

There are also what can be called strategic issues for Responsible Innovation in defence and security, which depends upon maintaining technological advantage in an open, globalised knowledge economy.

4.3 Specific areas of concern in quantum technologies

The range of quantum technologies is broad – and the specific social and ethical concerns are correspondingly specific to particular technologies. These can be categorised as quantum sensing, metrology, and imaging; quantum computing and information processing; and quantum-enhanced communications.

Each of these raises specific areas of concern:

- Imaging may raise privacy concerns, if it becomes possible to conduct surveillance of spaces which are currently private (which could also be possible with non-quantum technologies).

- If much more practical and more accurate quantum sensors could be developed, this could have enormous impacts on international relations, as one of the presenters in the workshop pointed out. Quantum sensing technologies, and other means of detection of submarines or underground objects, for example, could upset the existing balance of power which depends on neither side having certainty about the activities of the other.

- On the other hand, far more accurate GNSS-independent navigation, based on a related quantum technology, could transform the operational capabilities of submarines.

- A possible threat to national security comes from the potential of QKD technologies to forestall legal intercept by security services. In practice, technical and socio-legal interventions may allow security services to continue to monitor suspicious communications with suitable judicial oversight. Currently,[5] the only way to extend QKD over longer distances is to "hop" through trusted relay nodes [16], and these could provide a point of legal intercept. On the other hand, currently-unbreakable encrypted communication using non-quantum methods is already available to anyone who needs it; subject to important caveats such as the risk from future quantum computers[6], an encrypted channel is the "strongest link" in most security chains [40], and links secured with QKD remain vulnerable to the same end-point attacks (such as Trojans or social engineering) as any other cryptography scheme, Denial of Service, as well as other forms of attack.

- This does not imply that research and early uses of QKD are not important. QKD might emerge as a practical form of cryptography not vulnerable to quantum algorithms, alongside post-quantum classical cryptography. If QKD becomes widely deployed, it will be important to understand potential attacks and how to defend QKD systems [21, 32]. QKD is provably secure against any future technologies; post-quantum classical cryptography is immune to known quantum algorithms and probably future ones too but does not provide provably future-proof security.

Even the apparent benefits of new capabilities bring new risks and new forms of attack; the workshop noted that there are now many more potential attack surfaces in existing and emerging (non-quantum) technologies: for example, a recent attack mounted from an Internet of Things "botnet" [18].

[5] Quantum repeaters [7] could overcome distance limitations, but are not yet technically implementable.

[6] Much of the existing Internet encryption is vulnerable to the eventual development of sufficiently powerful quantum computers; but by that time, post-quantum cryptography, or perhaps provably-secure QKD, is likely to be widely deployed. Another serious risk is that communications recorded today could become vulnerable in the future, so the need for QKD or post-quantum cryptography is already present.

4.4 Social transformations and quantum technologies

Technologies create futures, in both banal and profound ways. An example given in the workshop was how the first supermarkets needed to introduce customers to this novel way of shopping; now we are moving to self-checkout machines. Each creates a new, initially strange, way of doing familiar activities.

A presentation at the workshop discussed the ways in which technology has a "constitutionalising" role in shaping emerging conditions, crossing boundaries but also constructing new boundaries, empowering us but also opening up new vulnerabilities. Technologies are not infallible, evenly distributed, nor are they separate from the social space.

A round table workshop in March 2015 [17] discussed the "social constitution" of quantum technologies – the set of social, political and economic conditions which will shape public concerns and trust in the technologies. A crucial determinant will be who is seen to be benefitting from this research and innovation – in a research landscape dominated by private and public "giants" and surrounded by secrecy.

Geographical space, the physical environment, as an operating environment, raises questions of control and management, and of public safety and architecture. But now the rise of the network has created a new form of space, cyberspace, with new human and agent relations. We have to think differently about security in this space which is, arguably, ungovernable.

4.5 Universal principles

Alongside their constitutionalising role, the most advanced capabilities remain subject to fundamental principles such as human rights, privacy, data protection, and other laws. Quantum technologies should be no different, and should not require a completely different regulatory environment.

> *Advanced capabilities remain subject to fundamental principles such as human rights, privacy, data protection, and other laws. Quantum technologies should be no different.*

As was noted above, quantum technologies, in their applications, are in many cases enhancements over existing technologies, rather than qualitatively new, and the workshop compared quantum with other emerging technologies, such as synthetic biology and nanotechnologies. Many of these issues arise, not from quantum technology itself, but from enhancements that quantum might enable, working alongside other technologies – such as for navigation, motion sensing, or big data analysis.

Actualising these norms in a situation involving new technology, however, requires some action. A proposal which has been made elsewhere [4], and which was raised during the workshop, is that principles could be embedded into technological artefacts themselves. Indeed, a reference was made in the workshop to Asimov's Three Laws of Robotics, starting with: "A robot may not injure a human being or, through inaction, allow a human being to come to harm" [5][7]. However, the idea of embedding laws in artefacts is as a "straw man" to start discussion, rather than as a practical solution.

The appeal to universal principles begs the question to what extent they really are universal and to what extent they are specifically Western and liberal democratic values; but, while technology may extend or limit the possibilities of human behaviour, the principles of the European Convention on Human Rights[8] and the United Nations Universal Declaration of Human Rights will still apply.

[7] It is worth noting, however, that these Three Laws, while well-known, can lead to contradictions – in fact, the short story in which they are presented features a plot based around conflicts and "feedback loops" inherent in these Laws.

[8] http://www.un.org/en/universal-declaration-human-rights/index.html

4.6 Narratives of quantum technologies

In talking about emerging technologies, and quantum technologies in particular, one of the messages from discussion in the workshop is that it is important to be honest [37] about what we still cannot do, and about what quantum technologies will not be able to do, as well as about what we can and hope to be able to achieve.

One the one hand, “quantum” is widely seen as strange and hard to understand (a view also noted by Sciencewise [41]); on the other hand, exaggerated claims are made which show a lack of understanding of the fundamentals of quantum mechanics. The workshop considered the responsibility of scientists for public engagement, to correct overstated threats or opportunities in a two-way process of dialogue: learning from the public as well as educating.

Until recently, we knew very little about public understanding and public attitudes to quantum technologies, apart from a survey by Sciencewise [41], which found little evidence apart from some reporting on public media (newspapers, blogs, websites). More recently, a public dialogue exercise, commissioned by EPSRC, has produced a report based on workshops with a wide range of stakeholders[9].

The narratives, and ownership of the narratives, are key issues for maintaining public trust – avoiding misunderstandings, “spookiness” and hype, but realistically focussing on the applications and their potential benefits, to enable an informed engagement with the public. It is important and responsible to be honest in admitting what quantum technologies can and cannot achieve.

4.7 Defence, National Security and Responsible Innovation in a complex market economy

Constant change is a hallmark of the modern economy. The workshop discussed the way in which “disruptive innovation” has become almost a requirement in funding proposals. Disruption usually implies that existing markets are negatively affected, at least in the short term.

In an era of globalisation, privatisation, and democratisation of research and development, traditional processes of regulation seem out-dated. Moreover, regulation tries to take account of the specific risks and benefits of a technology, but the public might be equally concerned about the speed and direction of innovation, and issues of equity in access to the new technologies. Regulation struggles to keep up with innovation: there are potentially long time gaps – often between 30 and 100 years - between research and development, the impacts becoming apparent, and our response to it.

As one of the presenters discussed, moving from laboratory research to market readiness also means crossing the “valley of death” [25], attracting sufficient investment to technologies for which the future return on investment is highly uncertain. These large investors are likely to be corporations or defence companies, or other large-scale industries such as finance, oil or pharmaceuticals. The workshop noted that even with these big investments, technologies might still have fifty per cent failure rate.

The workshop noted that opportunities for direct government interventions in the innovation process are limited, and the scale of resources required is not likely to prioritise application areas – teaching and farming were mentioned – which do not have access to such resources.

The workshop identified the key role of universities in the democratisation of knowledge, as gatekeepers and fast-trackers. A well-resourced network of universities is able to provide access to quantum technologies for stakeholders who might not be able to make these upfront investments.

[9] https://epsrc.ukri.org/newsevents/news/epsrc-publishes-results-of-public-dialogue-on-quantum-technologies/

5. Issues for consideration by policy-makers

Policy-makers in science and technology must grasp the potential powers of the science and think through their implications in the short and long term. This concluding section brings together the messages in this short paper to summarise the implications for public policy.

5.1 Embed Responsible Innovation in the research process

Responsible Innovation is emerging to provide tools to support the policy process; but to do this effectively, Responsible Innovation needs to be embedded in the research and innovation process at all stages, and be properly resourced to do so. Responsible Innovation should be included in the structure of research programmes, as it is in the UK National Quantum Technologies; this applies equally to defence-focussed programmes and projects.

5.2 Conversation with stakeholders

In the workshop, technical experts, scientists, innovators in industry and Responsible Innovation specialists worked together to produce a new and productive set of ideas. This demonstrated that there is demand for a more structured conversation at the intersection of responsible innovation, quantum technologies, and the national security and defence sectors. As well as these direct stakeholders, it will be important to engage with the public not only in outreach but also in dialogue, recognising the mutual shaping of technology and society, and to avoid or correct common misunderstandings.

5.3 Learn from other technologies

Quantum technologies raise some new questions, but are also in continuity with existing technologies. The changes wrought by quantum technologies will be both quantitative – faster, cheaper, easier; and qualitative – enabling functionalities which were not previously possible and leading to social changes. But other technologies such as ICTs and nanotechnologies also have the potential for new capabilities and social transformations. We can learn from experiences with other technologies.

5.4 Disruption

Quantum technologies may be disruptive to existing industries and ways of doing things. While this may lead to long-term economic growth, there will be losers as well as winners; this needs to be planned for to minimise harmful social change. On the other hand, the workshop considered that many of the innovations from quantum are likely to be improvements (albeit in some cases by orders of magnitude) over existing technologies rather than wholly new capabilities. Some of these new or enhanced capabilities may be rapidly disruptive, as some existing quantum-based technologies have been, while other changes are likely to be gradual, or to co-exist with non-quantum technologies, rather than a sudden step-change.

5.5 Security threats

Although it is still some years distant, the threat from quantum computing to break existing Internet encryption is real. Understanding post-quantum cryptography at the technical level, and planning for its implementation, is a priority. Similarly, the new quantum technologies, taken as a whole and alongside other technologies, represent a new security attack surface. It will be important to research and study the impact on the overall security of systems as they integrate quantum technologies.

5.6 Maintaining advantage in a global world

The competition between quantum and classical technologies, and also the competition between power blocs to develop quantum computing, QKD, and other quantum technologies has been compared to an arms race [1]. These technologies are largely being developed for initially civil use, but advantage in these technologies will give major economic and military advantage. However, research today is open: most of the research conducted will be made public. The large public investment in quantum technologies should give the UK world-leading skills and knowledge; consider how this advantage can be maintained and strengthened in the globalised economy.

Appendices

Format of the workshop

Keynote: Professor Jim Al-Khalili, University of Surrey: Opportunities in Quantum Technology: Learning lessons from Nature

Presentation 1: Professor David Galbreath, University of Bath: The changing defence and security landscape

Presentation 2: Professor Neil Stansfield, Dstl: Technologies for defence and national security, and the third technology offset

Presentation 3: Professor Richard Owen, University of Exeter: Can quantum technologies be developed responsibly?

The presentations were followed by a plenary discussion addressing the issues raised in the keynotes.

The workshop then separated into six parallel working groups to discuss three sets of questions (two tables discussing each), around topics:

- “Access”
- “Social transformations”
- “Trust”

The workshop ended with feedback and next steps: what are the lessons for policy, strategy and tactics?

A framework for Responsible Innovation

Research and innovation of all kinds is generally conceived with good intentions; technology has transformed the quality of our lives in mostly positive ways. Responsible Innovation is not simply a collection of ideals and norms, but is also a practical response to the challenges of ensuring that research, innovation, and new products and services are properly embedded in our society (or any society), in the increasingly complex, globalised knowledge economy.

One way of encapsulating the tools of Responsible Innovation is the Anticipate – Reflect – Engage – Act (AREA) framework, originally developed for the UK EPSRC funding body in response to public disquiet – expressed in a series of public-engagement workshops - around a research direction in geo-engineering.

This framework has four dimensions:

- Anticipation envisages possible applications and implications of an innovation: anticipation does not attempt to predict the future, but it does build capacity to prepare for whatever the future may hold. Anticipation asks questions such as: “what if?...”, “what else might it do? ...”, opening up the space of possibilities.

- Whereas anticipation is outward and forward-looking, reflection invites us to consider the purposes and motivations of research, and the uncertainties, assumptions, framings, and dilemmas. It asks us to think about who may be the winners and losers, and the cultural, political, and ethical dimensions of an innovation.

- Engaging with a wide range of stakeholders introduces a broad range of perspectives and experiences. This allows us to see different viewpoints, to reframe issues and to identify possible areas of contestation. It is a dialogue, recognising the variety of skills and experience of different stakeholder, to help to create technologies that are socially desirable and widely accepted.

- Finally, these dimensions alone would not lead to responsible innovation unless we are prepared to act responsively to the outputs from the framework It involves a readiness to re-think goals and strategies and to adapt the trajectory and pace of innovation; it is dynamic and iterative.

Putting the AREA framework into practice requires that the conversation is properly resourced. The framework, as it stands, is quite general, although it has been developed in response to real experiences in research projects. It requires tailoring and adaptation to be applied in specific new technologies; it demands a willingness to invest the time and energy to involve stakeholders and to enter into dialogue between research leaders, practitioners, Responsible Innovation researchers, and other groups.

Acknowledgments

We would like to thank all of those who attended the workshop in Oxford in October 2016, the presenters, and organisers; Florian Egloff who produced a summary of the discussion on which this report is based; and reviewers of earlier versions of this Briefing.

The participants, other than the presenters, are not named because the discussion part of the event (after the initial presentations) took place under the Chatham House Rule: “When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.”[10]

[10] https://www.chathamhouse.org/chatham-house-rule

References

1 Ahuja, A. Europe’s leap into the quantum computing arms race, 2016.

2 Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., . . . Zeilinger, A. Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 560(2014), 62-81.

3 Altmann, Y., McLaughlin, S., Padgett, M. J., Goyal, V. K., Hero, A. O. and Faccio, D. Quantum-inspired computational imaging. Science, 361, 6403 (2018), eaat2298.

4 Arkin, R. C. Governing lethal behavior: embedding ethics in a hybrid deliberative/reactive robot architecture. ACM, 2008.

5 Asimov, I. Runaround. Gnome Press, New York, NY, USA, 1950.

6 Bernstein, D. J. Introduction to post-quantum cryptography. Springer, 2009.

7 Briegel, H.-J., Dür, W., Cirac, J. I. and Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. Physical Review Letters, 81, 26 (1998), 5932 Available at: http://arXiv.org/abs/quant-ph/9803056v1 (Accessed on: 09/08/2018).

8 Brown, G., Ridley, K., Rodgers, A. and de Villiers, G. Bayesian signal processing techniques for the detection of highly localised gravity anomalies using quantum interferometry technology. International Society for Optics and Photonics, 2016.

9 Collingridge, D. The social control of technology. Pinter, London, 1980.

10 Defence Science and Technology Laboratory. A perspective of UK Quantum Technology prepared by and for the UK Quantum Technology Community. 2016. Available at: http://uknqt.epsrc.ac.uk/files/ukquantumtechnologylandscape2016/ (Accessed on: 28/03/2018).

11 Department for International Trade. UK Strategic Export Control Lists. 2017. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/593228/controllist20170222.pdf (Accessed on: 28/03/2018).

12 Development Concepts and Doctrines Centre - Ministry of Defence. Strategic Trends Programme: Future Operating Environment 2035. 2015. Available at: https://www.gov.uk/government/publications/future-operating-environment-2035 (Accessed on: 28/03/2018).

13 Dowling, J. P. and Milburn, G. J. Quantum technology: the second quantum revolution. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 361, 1809 (2003), 1655-1674.

14 Dutton, N. A., Parmesan, L., Gnecchi, S., Gyongy, I., Calder, N., Rae, B. R., . . . Henderson, R. K. Oversampled ITOF Imaging Techniques using SPAD-based Quanta Image Sensors. In Proceedings of the International Image Sensor Networks (Vaals, Netherlands, 08-11/06/2015, 2015), [insert City of Publication],[insert 2015 of Publication].

15 Ekert, A. and Jozsa, R. Quantum computation and Shor’s factoring algorithm. Reviews of Modern Physics, 68, 3 (1996), 733.

16 European Telecommunications Standards Institute. Implementation Security of Quantum Cryptography: Introduction, challenges, solutions. ETSI, 2018. Available at: https://www.etsi.org/technologies-clusters/white-papers-and-brochures/etsi-white-papers (Accessed on: 09/08/2018).

17 Faullimmel, N. and Stilgoe, J. Responsible Research and Innovation in Quantum Technologies: A briefing note, Report of interviews and round table workshop, March 2015.

18 Gallagher, S. Double-dip Internet-of-Things botnet attack felt across the Internet. Ars Technica, 21 October 2016. Available at: https://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/ (Accessed on: 28/03/2018).

19 Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C. and Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature communications, 2(2011), 349.

20 Gibney, E. One giant step for quantum internet. Nature News, 27 July 2016.

21 Government Office for Science. The Quantum Age: technological opportunities (The Blackett Review of quantum technologies). 2016. Available at: https://www.gov.uk/government/publications/quantum-technologies-blackett-review (Accessed on: 28/03/2018).

22 Grinbaum, A. and Groves, C. What Is “Responsible” about Responsible Innovation? Understanding the Ethical Issues. John Wiley & Sons Ltd, Chichester, UK, 2013.

23 HM Government. A Strong Britain in an Age of Uncertainty: The National Security Strategy. HM Government, London, UK, 2010. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Accessed on: 28/03/2018).

24 HM Government. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. HM Government, London, UK, 2015. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (Accessed on: 28/03/2018).

25 House of Commons Science and Technology Committee. Bridging the valley of death: improving the commercialisation of research. The Stationery Office London, London, UK, 2013. Available at: https://publications.parliament.uk/pa/cm201213/cmselect/cmsctech/348/348.pdf (Accessed on: 28/03/2018).

26 Lanzagorta, M., Uhlmann, J. and Venegas-Andraca, S. E. Quantum sensing in the maritime environment. IEEE, 2015.

27 Ministry of Defence. National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security. Ministry of Defence, London, UK, 2012. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf (Accessed on: 28/03/2018).

28 Ministry of Defence. Better Defence Acquisition: Improving how we procure and support Defence equipment. Ministry of Defence, London, UK, 2013. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206032/20130610_WP_Better_Def_Acquisition_screen_final.pdf (Accessed on: 28/03/2018).

29 Moreau, P. A., Toninelli, E., Gregory, T. and Padgett, M. J. Ghost imaging using optical correlations. Laser & Photonics Reviews, 12, 1 (2018), 1700143.

30 Moser, P. M. Gravitational Detection of Submarines. Pacific-Sierra Research Corporation Warminster United States, 1989.

31 Nagel, C. Keynote speech to Reagan National Defense Forum, Simi Valley, CA, USA, 15 November, 2014. Available at: https://www.defense.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=1&ModuleId=2575&Article=606635 (Accessed on: 28/03/2018).

32 National Cyber Security Centre Quantum key distribution, 2016. Available at: https://www.ncsc.gov.uk/information/quantum-key-distribution (Accessed on: 28/03/2018).

33 National Institute for Standards and Technology Post-Quantum Cryptography Standardization, 2017. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (Accessed on: 28/03/2018).

34 National Physical Laboratory Insights 06: Quantum edition. Available at: http://www.npl.co.uk/commercial-services/insights/issue-06/ (Accessed on: 28/03/2018).

35 Naval Technology Cat and Mouse: The Art of Submarine Detection. Naval Technology: News, views and contacts from the global Naval industry, Jun 14 2011. Available at: http://www.naval-technology.com/features/feature121453/ (Accessed on: 28/03/2018).

36 Penny, M., Hellgren, T. and Bassford, M. Future Technology Landscapes: Insights, analysis and implications for defence. RAND, Cambridge, UK, 2013.

37 Pielke Jr, R. A. The honest broker: making sense of science in policy and politics. Cambridge University Press, 2007.

38 Qiu, J. Quantum communications leap out of the lab: China begins work on super-secure network as ‘real-world’ trial successfully sends quantum keys and data. Nature, 508, 7497 (2014), 441-443.

39 QuantIC QuantIC hosts quantum enhanced imaging workshop for Defence and Security sector with industry partner QinetiQ, 2016. Available at: https://quantic.ac.uk/quantic-hosts-quantum-enhanced-imaging-workshop-for-defence-and-security-sector-with-industry-partner-qinetiq/ (Accessed on: 28/03/2018).

40 Schneier, B. Quantum Cryptography, 2008. Available at: https://www.schneier.com/blog/archives/2008/10/quantum_cryptog.html (Accessed on: 28/03/2018).

41 Sciencewise. Public attitudes to quantum technology. 2014. Available at: http://sciencewise-erc.org.uk/cms/assets/Uploads/Quantum-Technology-Social-IntelligenceFINAL.pdf (Accessed on: 22/07/2016).

42 Simon, D. S., Jaeger, G. and Sergienko, A. V. Quantum information in communication and imaging. International Journal of Quantum Information, 12, 04 (2014), 1430004.

43 Srivastava, R., Choi, I. and Cook, T. The Commercial Prospects for Quantum Computing: Networked Quantum Technologies (NQIT) User Engagement Team. 2017. Available at: http://nqit.ox.ac.uk/content/commercial-prospects-quantum-computing (Accessed on: 28/03/2018).

44 Stilgoe, J., Owen, R. and Macnaghten, P. Developing a framework for responsible innovation. Research Policy, 42, 9 (2013), 1568-1580.

45 Tannenbaum, E. D. Gravimetric Radar: Gravity-Based Detection of a Point-Mass Moving in a Static Background. arXiv preprint arXiv:1208.2377(2012).

46 The Wassenaar Arrangement The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Available at: http://www.wassenaar.org/.

47 UK National Quantum Technologies Programme Strategic Advisory Board National strategy for quantum technologies: A new era for the UK. Engineering and Physical Sciences Research Council, 2015. Available at: https://www.gov.uk/government/publications/national-strategy-for-quantum-technologies (Accessed on: 28/03/2018).

48 UK National Quantum Technologies Programme Strategic Advisory Board A roadmap for quantum technologies in the UK, 2015. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470243/InnovateUK_QuantumTech_CO004_final.pdf (Accessed on: 28/03/2018).

49 UKPublicSpending.co.uk What is the cost of UK National Defence? Available at: https://www.ukpublicspending.co.uk/uk_national_defence.php (Accessed on: 28/03/2018).

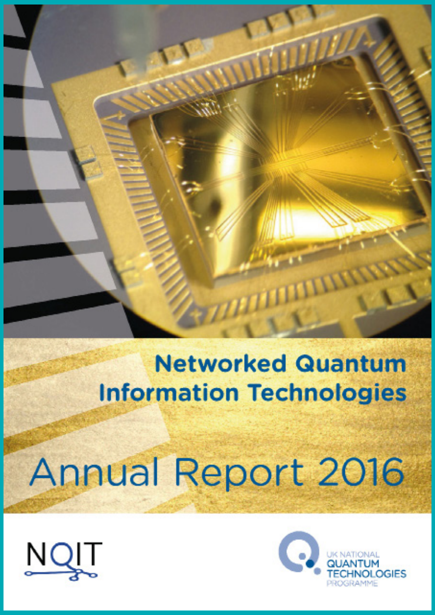
50 US Department of State Directorate of Defense Trade Controls The International Traffic in Arms Regulations. Available at: https://www.pmddtc.state.gov/regulations_laws/itar.html.

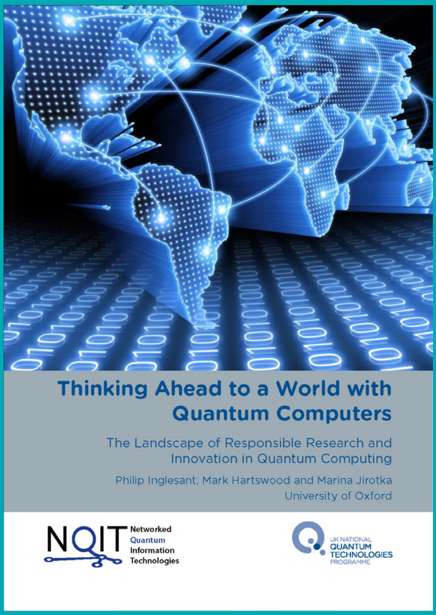
51 USAF Scientific Advisory Board. Utility of Quantum Systems for the Air Force: Study Abstract. 2015. Available at: http://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-151214-041.pdf?ver=2016-08-19-101445-230 (Accessed on: 28/03/2018).

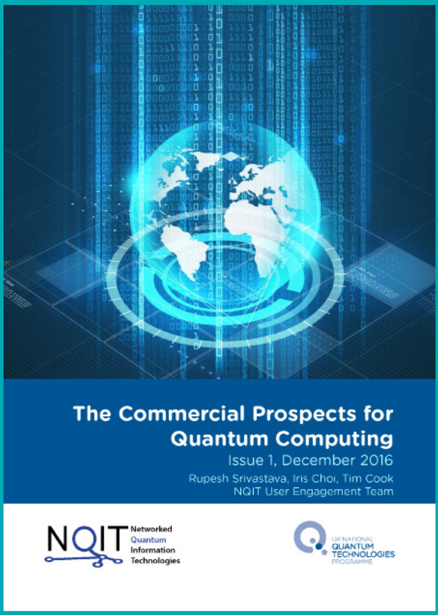
52 Von Schomberg, R. A vision of responsible research and innovation. John Wiley & Sons Ltd, Chichester, UK, 2013.

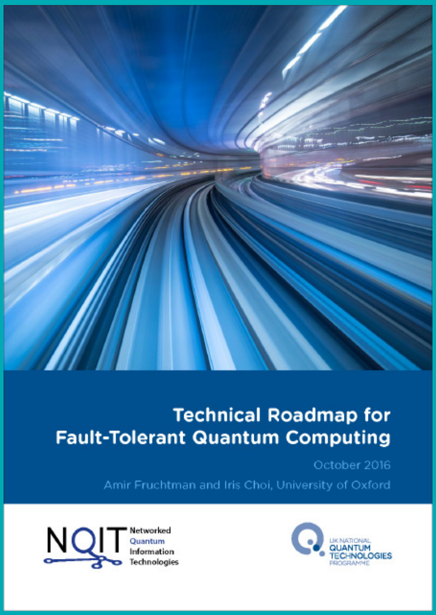
Annual Report 2018
NQIT Networked Quantum Information Technologies
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Annual Report 2017
NQIT Networked Quantum Information Technologies
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME


Networked Quantum Information Technologies
Annual Report 2016
NQIT
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME


Thinking Ahead to a World with Quantum Computers
The Landscape of Responsible Research and Innovation in Quantum Computing
Philip Inglesant, Mark Hartswood and Marina Jirotka
University of Oxford
NQIT Networked Quantum Information Technologies
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME


The Commercial Prospects for Quantum Computing
Issue 1, December 2016
Rupesh Srivastava, Iris Choi, Tim Cook
NQIT User Engagement Team
NQIT Networked Quantum Information Technologies
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME


Technical Roadmap for Fault-Tolerant Quantum Computing
October 2016
Amir Fruchtman and Iris Choi, University of Oxford
NQIT Networked Quantum Information Technologies
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

For more information about NQIT,
please visit our website:

http://www.nqit.ox.ac.uk

Or get in touch:
email: contact@nqit.org
@NQIT_QTHub

NQIT Networked Quantum Information Technologies

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME