SPECIAL REPORT

ASPI

From little things

Quantum technologies and their application to defence

Andrew Davies and Patrick Kennedy

November 2017

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Andrew Davies

Dr Andrew Davies is the director of ASPI's Defence & Strategy Program.

Andrew has been with ASPI since 2006. He has written extensively on ADF capability and force structuring issues, including platform options for air and maritime combat, industry issues, and decision-making in the Department of Defence.

He has an ongoing interest in the future submarine and Joint Strike Fighter projects, and his work on both has made an important contribution to the public understanding of those projects here and abroad.

Before joining ASPI, Andrew was a post doctoral fellow in physics at Melbourne University and the ANU. He then spent twelve years in the Department of Defence in the areas of capability analysis and intelligence.

Patrick Kennedy

Patrick Kennedy was a research intern at ASPI in 2017. Patrick is a candidate for Masters of Science (Physics) at the University of Melbourne. His undergraduate research involved the prototyping of a cheap and accurate wavemeter, as well as the construction of an atomic clock suitable for use in undergraduate learning environments. His current research involves working with biologists to study and simulate the statistical mechanics of warring ant colonies.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Experiments in laser interferometry have provided laboratory demonstrations of subtle quantum effects. The setup shown here allows an object to be imaged by light that has never been in contact with it. (Source: Gabriela B. Lemos et al, *Quantum imaging with undetected photons*, available at https://arxiv.org/ftp/arxiv/papers/1401/1401.4318.pdf. Image by Martin Ackerl for Lammerhuber Photography, © Austrian Academy of Sciences.)

From little things

Quantum technologies and their application to defence

Andrew Davies and Patrick Kennedy

November 2017

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

First published November 2017

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

INTRODUCTION

This paper looks at the impacts that emerging quantum technologies might have on defence. Some of the technologies are relatively well known; for example, there are many popular articles on quantum computing and its possible implications. There's a growing technical literature on quantum radar, and there's been some breathless recent reporting about it negating the advantages of stealth technology.

You can't buy a quantum radar or computer yet, but there are practical applications of other new quantum technologies. China has announced that it has a working quantum communication satellite system. And it's worth noting that what we're talking about here is really the latest generation of quantum systems. Previous innovations based on quantum physics have already had a major impact on both military and civilian technologies. The invention in 1947 of the transistor, which relies on intrinsic quantum effects for its operation, led to the microelectronics that are now ubiquitous in communication, computing, sensor and navigation systems. The development of the atomic clock in the 1950s enabled high-precision timing in the laboratory. After the development of devices that could function in less benign environments, like those experienced in satellite launches, they were employed in systems such as GPS to generate positional information. The 'revolution in military affairs' that came to public attention so dramatically in the 1991 Gulf War had quantum technologies at its heart.

Note that there are multiple steps in turning a technological idea into a system that's sufficiently robust for widespread use. The typical path is from idea, to 'proof of concept', to an up-scaled but still laboratory-based device. While laboratory devices sometimes have real-world applications, such as the primitive computers used to break codes in World War II, for widespread use the system must be productionised, including whatever degree of 'ruggedisation' is needed for practical applications. This paper assesses the status of what we think are the four most significant emerging quantum technologies: computing, communications, radar and remote sensing.

WHAT IS A QUANTUM TECHNOLOGY?

By ‘quantum technology’, we mean any device the operation of which depends on non-classical physics—that is, anything that operates on the physical principles of quantum theory. This paper isn’t intended as a primer on quantum technologies, so we limit our explanation here to a broad description, and provide more details as required under each of the technology headings. (For the interested reader, there’s a reading list of popular and technical articles at the end of this paper.)

At the end of the 19th century, there was a school of thought that the laws of physics were mostly understood. Classical physics, most notably Newton’s laws of mechanics, the electromagnetic theory of Maxwell and thermodynamics, was the basis of machine and system design. But around the turn of the 20th century, a number of puzzling phenomena proved to be beyond the explanatory power of existing theories. What we now call quantum theory took most of the first half of the 20th century to elucidate. It proved to be a difficult birth, and quantum systems frequently defy easy description in words developed to describe a classical world. For our purposes, the most important of the quantum-specific concepts are ‘superposition’, ‘non-locality’, and ‘entanglement’. We won’t try to explain them in any detail, as it’s notoriously hard to do so, and others have done it better than we could. (See, for example, the book by Euan Squires listed in our further reading list.)

Superposition means that an object behaves as if it has more than one value of some measurable property at once. (Such as a ‘qubit’ in a quantum computer that acts as if it’s simultaneously a zero *and* a one.) But, unlike a classical object, the value that’s measured isn’t predictable, even in principle. The best we can do is to predict the probability of measuring different values. Measurement is at the heart of quantum theory.

Non-locality means that measurements on parts of a quantum system can tell us about properties that will be measured at some other place and time, no matter how far apart they are. Think, for example, of a decaying subatomic particle that splits into two particles that head off in opposite directions: each one will generally be in a superposition of states. But because they were once a single object, if we measure the physical properties of one, even though we can’t know in advance of what answer we’ll get, we’ll immediately know what answer will be produced by a measurement on the other one. The two objects in this example are said to be *entangled*.

One other concept that’s germane to this discussion is *decoherence*. The discussion above implies that superpositions endure until a deliberate measurement is made. But if a quantum system interacts with the external environment strongly enough, or for long enough, its quantum information becomes spread out among a large number of particles, effectively making that information impossible to recover.

QUANTUM COMMUNICATION

Quantum communication is probably the easiest quantum technology to describe—and it seems to be one of the easier ones to practically implement. A quantum communication system exploits superposition and the probabilistic nature of quantum measurements to create an information channel that's cryptographically secure. It has no classical analogue, because classical cryptographic systems require either a secure exchange of key material via some other channel (such as having codebooks for the key of the day) or rely on a mathematical operation that's extremely difficult to reverse engineer (such as the prime number factorisation problem that underlies RSA encryption). The former approach is vulnerable to compromise of the key to a third party, and the latter is potentially vulnerable to either a breakthrough in mathematical methods or a dramatic increase in computing power—one such possibility being quantum computing (discussed in the following section).

'Quantum communication' is a misnomer—we're actually talking about 'quantum key exchange'. It works using a channel that allows the reliable passage of quantum bits or 'qubits' (not zeroes *or* ones, but superpositions of zeroes *and* ones). By carefully setting up measurements at both ends of the communication, the non-local nature of the quantum system lets you know whether a zero or one will be measured at one end, depending on the result observed at the other. Thus, the parties at both ends know the string of binary digits that was exchanged, and they can then use it as a key for enciphering sensitive messages. The security of the key is ensured because any eavesdropper who attempts to intercept the string has to do so by undoing the entanglement. And it turns out that it's impossible for the eavesdropper to reconstruct the string and send it on to the unsuspecting recipient. The 'no cloning' theorem for quantum systems says that there's no way to accurately reproduce an arbitrary qubit. The eavesdropper can interfere with the communication of the key, but can't steal it.

It turns out that engineering quantum communication is much less difficult (the word 'easy' probably shouldn't be applied to any of these techniques) than the technologies we discuss below. The transmission of qubits (in this case in the form of particles of light—'photons') along fibre-optic cables is now well established, and has been put to practical use. It's the basis of the Australian Government quantum network project set up in 2013 to link Parliament House with other government organisations in Canberra. A prototype system was running in the US several years before that, and China has ambitious plans for a secure internal network. Decoherence presents a practical challenge as distance increases, and a cable length of 250 kilometres still represents a significant achievement. But scientists are making steady progress; a German group has demonstrated the transmission of quantum signals from an aircraft to a ground station 20 kilometres away, and others have done the same between fixed ground stations 144 kilometres apart.

China seems to be ahead of the pack in fielding quantum key exchange systems, and announced the launch of the world's first quantum communication satellite in August 2016. While the distances involved are greater than other groups have managed so far (unless there are 'black' projects we don't know of, which is entirely possible), they aren't implausibly greater. Getting the claimed performance of the Chinese system by using high-power signals and large-aperture antennae is entirely credible. And the ability to uplink entangled states opens the possibility of communicating between widely dispersed ground stations through an intermediate satellite-to-satellite link. As noted above, a signal propagating through the atmosphere decoheres over distances under 150 kilometres, but

for communications between orbiting bodies there's little loss of coherence due to the near-absence of intervening matter. As announced in a technical paper in July this year, a ground-to-space-to-space-to-ground link was used to connect two ground stations over 1,400 kilometres apart in central and western China.

The upshot is that, in principle, quantum communication networks can be rolled out globally to form a 'quantum internet'. In practice, quantum links are more complex to set up than classical channels, and more delicate to maintain. High-volume fibre-optic cables currently carry large volumes of classically encoded traffic over global distances, greatly outweighing traffic carried by satellite links (although there have been efforts to increase the bandwidth of space-based links and hence the volumes of data carried over them). While repeater stations are required periodically to ensure signal integrity, the technology needed to do that is much simpler than for quantum systems, although so-called quantum repeaters are being investigated. A classical signal can be copied exactly and retransmitted, but a quantum one can't, so any long-distance quantum signal transiting fibre links must be re-enciphered multiple times using new keys. Because of those extra overheads, quantum communications are unlikely to replace existing classical communication channels any time soon, except for specialised applications where absolute security is required and relatively small volumes of data are involved—such as high-level military or diplomatic communications. The US Air Force Science Advisory Board reached the same conclusion—quantum communications add extra complexity for marginal gains.

For defence organisations, the maturation of quantum communication will ensure that secure communication channels will be available in the future, even if classical cryptographic methods become vulnerable to attack. That's obviously important, as the history of warfare is rich with examples of compromised communications leading to unhappy outcomes—all the way from tactical information betraying a position through to government-to-government messages betraying otherwise unknown contacts between nations.

But there are many cryptographic systems in use today that are secure to all intents and purposes, and some are thus far 'quantum' proof, so we don't see quantum communication as a game-changer. In a sense, it's a 'conservative' technology, in that it will help preserve existing practices by future-proofing them against developments in cryptography. It might be no coincidence that China is leading the push for operational quantum communication systems, as this allows it to offset the likely advantage the US has in cryptanalytic techniques.

QUANTUM COMPUTING

The concept of quantum computing dates to 1981, when Nobel Prize winning physicist Richard Feynman observed that classical computers couldn't efficiently deal with the complex dynamics of quantum systems. Rather than seeing that as a problem, Feynman turned the situation on its head, observing that setting up a quantum system and performing a measurement was therefore equivalent to executing many calculational steps on a classical computer. In principle at least, by carefully designing a quantum system and making a measurement, an answer that was practically unobtainable from a classical computer could be generated.

Once physicists and mathematicians started exploring the possibilities of such an approach, they found that there are some practically interesting problems for which suitable quantum systems can be designed. *Shor's algorithm* (1994) for factoring numbers into their prime factors ($15 = 3 \times 5$, for example) can be shown to be substantially more efficient than any known classical algorithm—and it's immediately applicable to cryptographic attacks on prime-number-based encryption, such as the RSA algorithm widely used in internet security. *Grover's algorithm* (1996) is a quantum technique for finding a specific record in an unstructured and unsorted database. The time taken by any classical search technique grows in proportion to the size of the database, while the quantum search grows only as the square root of the number of entries. Both take longer as the number of entries increases, but going from one to a trillion entries will take a trillion times longer for a classical machine, but only a million times more for a quantum computer. That said, it's not clear how useful that will be in practice. Every search of the trillion-entry database will require it to be reloaded, as observing the result of the previous search will collapse the superposition of database states that provides the quantum speed-up.

The discovery of those algorithms and the mathematical proof of their efficiency showed that useful quantum computing devices are possible—in principle. Perhaps of greater interest is the possibility of a *universal quantum computer*—a device that can be programmed to perform any computational task. That such a device is theoretically possible was established in 1985 by David Deutsch, who essentially generalised the classical theory of computers developed by Alan Turing. That's important because it means that a quantum computer can theoretically do everything that a classical computer can do, and potentially do it many times faster. There are also calculations and simulations that no classical computer can practically do but that are possible on a quantum computer. For example, being able to model quantum systems on a quantum computer could lead to breakthroughs in the design of exotic materials.

It's hard to overestimate the potential impact of large-scale quantum computing on virtually every aspect of modern life. The rapid growth of processing power in classical computing over the past few decades has been underpinned by technical advances in the ability to pack processors onto circuit boards (parameterised by Moore's Law, which says that the density of transistors doubles roughly every two years) and to move information between them. The net result has been an increase in the number of calculations that can be performed per second by a factor of a million in the past 30 years. Given the impact of that change on modern life, the potentially transformational nature of a sudden increase in computing power of a similar magnitude becomes immediately obvious.

Practical difficulties

But the potential of quantum computing might never be realised. Designing an algorithm and calculating its theoretical efficiency or proving that there's no fundamental law of nature preventing universal quantum computing is quite different from implementing it on practical hardware. Despite having over 30 years of theory and many person-years of experimental research and development effort behind it, there's still no commercial quantum computing technology on the market, nor any obvious sign of that happening soon.

Opinion remains divided regarding the prospects of a significant breakthrough to large-scale quantum computing. Optimists point to there being no fundamental impediment (in the sense that it's compatible with all known laws of nature), the existence of some promising prototype systems that have already performed some simple calculations, and a diverse range of technical approaches being pursued in labs around the world. Pessimists note that the laws of physics don't just have to allow something in theory: they must also align to make it possible in practice. They point to decoherence as the elephant in the room.

A programmable quantum computer needs to be able to interact strongly with the external world to allow the input of instructions and the output of results of computations. But, in between those interactions, it's necessary to quarantine the device from the external environment as much as possible, to prevent decoherence from spoiling the computation. The more steps in the computation, the greater the chance of decoherence intervening, so it could be that proof-of-concept demonstrations will be difficult to translate into systems for solving real problems. Because of unavoidable interactions with the environment, errors due to decoherence will need to be removed before they accumulate to prevent accurate longer calculations. Again, there's a theoretical proof that provides in-principle support in the form of what's called the 'threshold theorem'. The theorem says that if environmental noise can be kept below a certain level, it will always be possible to correct noise-induced errors faster than they're created. That means that fault-tolerant quantum computers of almost arbitrary size should be possible. It's a powerful finding, but error correction is notoriously difficult to implement. Current small-scale quantum computer demonstrations can get by without needing much error correction, but the amount required will grow sharply for more ambitious computers. There are experimental approaches designed to minimise the need for error correction (it can never be entirely avoided), or to confine it to subsystems small enough to make the process fast enough and reliable enough for practical applications. Ironically, it could be that the classical computing power needed to track and control the accumulation of errors will be a bottleneck for quantum computing.

We think that there's enough promise in current work on quantum computing to make its pursuit worthwhile (we review some important progress below), but we also note that there are no guarantees of success. For example, the generation of useful and controllable power from nuclear fusion is well understood from a theoretical point of view. There are no laws of nature that rule out the construction of a fusion reactor, and there have been proof-of-concept demonstrations of (fleeting) net energy generation in laboratories. But, despite a lot of effort and investment, it has proven to be prohibitively difficult to implement as a practical means of energy production. Fusion power has been 'a few decades away' for much more than a few decades now, and no fusion reactor has yet been able to generate more energy than is required to run it on a sustained basis. Despite some recent claims of breakthroughs, they remain unproven as commercially viable technology. Some engineering problems are just really hard. Quantum computing might be one of those.

Recent progress

We finish this section by noting that quantum computing has recently been nudging some important milestone achievements. One such is the practical implementation of 'quantum supremacy'. That means a clear demonstration of a 'quantum speed-up'—a quantum computer that outperforms the best classical supercomputer on a specific task. But 'outperforms' here is a qualified term. It doesn't mean that there's a quantum computer that can perform a useful real-world calculation faster than a classical one—just that the time required increases less steeply with the size of the inputs. Grover's algorithm (described above) is an example of a calculation for which

a quantum speed-up is possible. Doubling the size of a database doubles the classical computational time, but a quantum computer will take only 40% longer. The quantum computer could even be *slower* than a classical one and still pass the test, provided the 40% scaling is achieved.

That's still a significant step in computer science, even if the name tends to oversell it, and effectively shows that there are some things a quantum computer can do that a classical computer can't—at least on a practical timescale. A team working for Google expects to soon be able to demonstrate quantum supremacy.

If those developments were to lead to successful large-scale devices, then that would enable a range of practical applications, not just Grover's algorithm, but also the 'HHL algorithm' for linear equations, and quantum simulation. Most scientific fields have problems in which the ability to efficiently perform large calculations of those sorts would be very helpful. The HHL algorithm offers an even better performance boost than Grover's, providing an exponential speed-up of runtime compared to the best classical algorithm for solving a system of linear equations. That could allow for faster (and therefore more detailed) modelling in everything from weather forecasts to radar system simulations. And a quantum simulator would let us model atomic-scale interactions efficiently—something that a classical computer can't do. Areas such as medicine, chemistry and engineering now use advanced supercomputers to approximate the behaviour of drugs, organics and materials. Faster calculations of models with greater fidelity would be of great utility.

And certainly not least, most machine-learning techniques also involve linear equations. Using classical devices and the fruits of Moore's law, machines are already number one in chess, *go* and poker. And they're encroaching on jobs in industries traditionally occupied by highly trained (and well-paid) humans. A literal quantum leap in processing speed, especially in calculations of direct application to machine learning, could be a technological force multiplier of extraordinary impact.

The potential impact of large-scale quantum computing is huge, but there remain many unknowns in its practical implementation. That said, quantum computing experiments aren't especially expensive to support (and look positively cheap compared with 'big science' such as particle physics and large-array astronomy) and there are even some potentially useful small-scale devices that could operate on just a handful of qubits. We come back to the subject in a section on geopolitical implications at the end of this paper, but if a single nation were to make a big breakthrough first and establish a clear lead, catching up might not be so easy. For all those reasons, we think that continued investment in quantum computing research makes sense. But that shouldn't happen at the expense of research into other quantum technologies. As we see below, quantum sensing is very promising and is getting some runs on the board in terms of producing useful devices. That's not yet true of quantum computing.

QUANTUM RADAR

All radar systems aim to detect and track targets using electromagnetic energy. The name of the game is to bounce pulses of energy off targets; if the pulse hits a target, some energy reflects to a detector where it can be measured. But it's a challenging task. The echo is often very weak, and it must be measured against a background of noise. Quantum technologies can help to pick a weak signal out of the noise.

That idea underlies the two main approaches to quantum radar—based on *interferometric* and *entanglement* methods, respectively.

Interferometric quantum radar (also called *coherent state quantum radar*) is the more mature technology of the two. The basic idea is that a coherent—in the sense of not spreading as it propagates—waveform that behaves almost like a classical particle is transmitted. After reflection from a distant target, careful and precise measurements are made of the return signals. The net result is a system that is capable of greater resolution than classical radars. That means that targets can be imaged more clearly, or from farther away. Interferometric quantum-based detectors can make highly accurate readings even when the radar echo is very weak and wouldn't be visible above the noise floor in a classical radar. In practice, this means that the radar will help to track distant and rapidly moving objects at operationally meaningful ranges. Indeed, though there'll no doubt be kinks to iron out, the radar is feasible with today's technology and there are proposals to realise this kind of quantum radar with only minor changes to existing systems. Although the improved capabilities offered by the radar will be useful, they probably won't confer the required sensitivity to reliably detect and track stealth platforms—at least from beyond the weapon ranges of the offensive platforms.

The second technique, e*ntanglement quantum radar* (sometimes called *quantum illumination*), is potentially sensitive enough to offer practical counterstealth capability—but it's much harder to realise, even though it gets the lion's share of the spotlight in the popular press. In this scheme, entangled signals sent out by the radar are 'tagged' so that they can be distinguished from noise by comparing them with a 'stored' signal kept on hand (the 'tagging' is effected when transmitted signals are entangled with the stored signals). Even an extremely weak return, like we would see from a distant, stealthy target, can be detected if the signal signatures match.

An entanglement radar potentially offers several key capabilities in addition to counterstealth capabilities. At least in the dreams of various patent-holders, it could be possible to use radar returns to work out the material composition of the target. That should pique the interest of anybody interested in distinguishing between weapon types, or real and fake warheads, for example. Additionally, the only means to jam an entanglement-based radar would be to use brute-force power to ramp up the noise floor to the point where signals are hard to identify—the 'no cloning' theorem discussed above means that the transmissions themselves can't be faked. Finally, if the radar operates at low power, it would be very difficult for a target to tell whether or not it had been detected.

But there are significant engineering challenges to overcome. For the foreseeable future, entanglement quantum radars are likely to transmit only very low levels of power, and researchers are still trying to develop detectors that can pick up the extremely weak echoes. In addition, the tagged signals can be slow to generate, and that may limit the power and resolution of the radar. Finally, because we must compare the returning tagged signal with the stored

signal, which is subject to decoherence in whatever device is used to keep it, the measurement must be made soon after the tagged signal is generated, limiting the range of the radar. Technologies that might extend this window of time are still very experimental. One result from 2015 suggested that, with today's technology, the range of an entanglement radar might be limited to 11 kilometres.

As well as engineering challenges, there are more fundamental constraints on entanglement radars. The transmitted tagged signals are also prone to losing their unique signatures (their entanglement) as they travel, and that's likely to limit the range. In air, the record for that kind of transmission stands at 143 kilometres (corresponding to a best range of 70 kilometres, allowing for out and back travel). There are suggestions that the signals might still be useful even if the entanglement has been broken, but the prospect of atmospheric decoherence and attenuation remains deeply problematic. And to compare the tagged signals with the stored signal, we need to know the flight time of the tagged signal, *before* it's sent out. But that means we need to know the distance to the object being tracked in advance, suggesting that entanglement radars can only track targets, not initially detect them. If that's the case, entanglement radars would probably have to be used with an additional ranging system—which needs to be able to detect a stealth target, perhaps obviating the need for entanglement radar in the first place.

That's the theory behind technology that's still in the early stages of development; most of this theoretical groundwork was laid only in the 2000s. Research is driven by a small community, split between private, governmental and academic settings. The state of play for quantum radar is mostly evidenced in academic publications, and there's nothing like the broad base of engineering skill that supports classical radar development. As for the ultimate feasibility of the technology, there remains a base of scepticism in the broader scientific community.

That scepticism doesn't stop interested parties from hedging their bets. In the US, research has occurred within national laboratories and has been supported in open and closed settings by the Defense Advanced Research Projects Agency (DARPA). Several state-owned enterprises are researching quantum radar in China. And, given the large-scale funding in Europe for quantum technology, it's highly likely that additional classified research is also taking place there. Interestingly, several milestone publications have been authored by international groups—a trend common in modern scientific pursuits. That suggests there's a cooperative as well as competitive spirit, at least in academia.

Patents were granted to Lockheed Martin in 2008 and Raytheon in 2010; Chinese researchers and universities have also been granted patents. More recently, in 2014, an international collaboration sketched out how an interferometric radar could be built using existing technology. And, in 2015, a team of American and European scientists (working in part with Raytheon) demonstrated a proof of concept for some of the tricky techniques needed for entanglement quantum radar. Crucially, that group could entangle signals at the microwave frequencies necessary for tactically-useful radar, extending quantum illumination techniques that had previously been useful only for visible light.

Quantum radar and stealth technologies

In September 2016, China announced the demonstration of a prototype entanglement radar with a claimed range of 100 kilometres. If that's true, it's by far the most impressive publicly stated demonstration of the technology. But no information was communicated about its sensitivity or operating parameters—or how signals were 'stored' to produce ranges greater than 11 kilometres. That all makes it hard to get a precise read on what China may or may not have accomplished—and we note that China has a substantial incentive to undermine the perceived effectiveness of stealth platforms.

To get a handle on what developments in quantum radar might mean for stealth platforms, we need to look at some numbers. One of the key parameters is the signal-to-noise ratio (SNR). The SNR tells us how strong the signal is compared to the noise. Although the threshold for detection varies, a typical number for a classical system is that the signal must be around 30 times stronger than the noise baseline (equivalent to a signal excess of 15 decibels).

Quantum radar promises to lower the strength of the signal that's needed for a successful detection. That means that it could either see smaller targets at a given distance or see targets of a given size at greater distances.

A study in February 2017 suggested a reduction in the SNR threshold to around 12 decibels. That translates to a factor of two in performance. The return from a given target would be twice as large at a given distance. A target with a radar signature about the size of a golf ball will instead look like a bird. Alternatively, any given target would become detectable about 20% farther out.

Prospects

There's still a lot to be done to achieve a practical entanglement quantum radar in its strongest form. It'll take a lot of effort to get a working radar out of the lab and, even then, it may shape up more to be an evolution of existing capability, or a useful adjunct to it, rather than a direct replacement. And the costs and practical difficulties have to be weighed against concurrent advances in classical radars; networked, multistatic and VHF radar have all been touted for their potential counterstealth capabilities, and there are satellite detection techniques to throw into the mix. But there's enough at stake—and probably a great deal of activity behind closed doors—to admit the possibility that today's engineering challenges will be solved.

Interferometric quantum radar is a more realistic prospect in the short to medium term. Some designs could be implemented with only small tweaks to existing radar systems—although some of those designs would also need a separate ranging system. Like other improvements to classical radars, the gain in capability would probably be incremental, though useful.

Without the detailed, technical specifications of as yet non-existent quantum radars, it's hard to know how fatal the requirement for additional ranging systems will be. There's always the chance that, as new and better measurement systems develop, physicists will find a way around the need to 'store' signals for later comparison—that would obviate the need for the extra ranging systems. But even as it stands today, stealth is not a panacea, and stealthy platforms tend to be optimised for specific frequency bands. For example, stealth aircraft are typically X-band optimised—the frequency at which air-to-air radars and weapons operate. Existing radar systems at different frequencies can indicate the presence of stealth targets, even if that indication is inadequate for targeting purposes. One plausible application would be for a high-resolution quantum radar to be cued by a classical system able to give a 'ballpark' location. In our judgement, even that arrangement won't happen in the near term.

On an even more speculative note, it might be possible to deploy quantum radars without additional ranging systems. For example, if the system were calibrated to detect targets at a fixed distance, and could quickly sweep through many such fixed distances, there may be no need for advance knowledge of the target's range. Alternatively, quantum radar could form a 'trip-wire' sensor layer in a larger network by detecting stealthy targets as they pass a fixed perimeter, just as fixed arrays of seabed hydrophones help to detect submarines. Such a trip-wire could be established around important targets beyond the stand-off weapons range of an adversary's stealth aircraft. But the cost–benefit calculus for such operation is far from clear, and that technology is also likely to remain out of reach in the short to medium term.

In the long term, the greatest use-case for quantum radar might be found in space. As the need for space-based resilience increases, the need to track small, dark and fast objects will also grow—think floating rocks, or space junk that endangers satellites and future habitats. By almost eliminating decoherence as a problem, the space environment is particularly conducive to quantum systems.

QUANTUM SENSING

As described in the previous sections, the successful development of quantum computing, communication and radar is in no small way dependent on finding ways to avoiding decoherence—stopping, so far as is possible, the quantum system interacting with the environment outside. In those cases, the better isolated the quantum computer or signal, the better it will be at doing the job that it's designed to do.

When it comes to quantum sensing (also known as *quantum metrology*), that's true only sometimes. For some devices, that tendency to interact with the external world is a positive feature and makes possible quantum devices that are sensitive to tiny changes in magnetic, electric and gravitational fields, allowing them to make precise measurements of those quantities.

Quantum sensing as a field of research has a lot of moving parts, and it's difficult to survey them all. Around the world, many different research groups are pursuing a wide range of approaches. For our purposes, we describe here the possible outcomes and worry less about the detailed mechanisms underpinning them. For defence applications, that's relatively straightforward—the big three direct outcomes are improved atomic clocks, magnetometers and inertial navigation systems. But advances in quantum sensing will make it easier to build the quantum systems that underlie quantum computers and communication relays, so there will be second-order effects in the systems described earlier in this paper.

Other devices that rely on quantum phenomena will help make more accurate measurements of electric and gravitational fields, temperature, pressure, and pollutant or chemical levels. So, as well as the more obvious defence capability boosts listed for our 'big three', the gradual incursion of quantum devices into defence and national security circles will affect areas as diverse as airport security, hydrographic surveying, battlefield medicine and nonproliferation compliance.

Atomic clocks

When an atom is illuminated by a carefully calibrated laser beam, subcomponents of the atom oscillate, sometimes gaining energy and sometimes losing energy, but always in discrete amounts (the basis of the term 'quantum jump'). The frequency of those oscillations can be measured extremely precisely, and that idea underpins modern atomic clocks. In defence settings, atomic clocks provide the time standards that enable navigation, communication and many other sophisticated electronic systems. Atomic clocks were the first quantum-enabled measurement devices to find widespread use—the first was built by the US National Institute of Standards and Technology (NIST) in 1949. Since then, atomic timing systems have undergone a long series of iterative improvements and innovations, all aimed at making the clocks more accurate, stable, compact and rugged.

NIST is still a leader in the field today. In 2014, researchers there engineered a clock that would lose only a second over a five-billion-year period, and in October 2017 NIST scientists announced the most precise atomic clock ever built. But, as is the case with other quantum technologies, there's great interest around the world, and other groups are making significant advances. In September 2016, in a pioneering experiment, Chinese scientists launched the first space-based 'cold atom' clock into orbit on board the Tiangong-2 space station. The project is a scaled-down

version of a mission that has long been planned by the European Space Agency and its scientific collaborators. For our part, Australia will contribute to that larger European mission—researchers at the University of Western Australia are building one of the most accurate clocks in the Southern Hemisphere, ultimately to be synced with several aboard the International Space Station.

The science of atomic clocks is already very mature, even if that maturity is belied somewhat by the high intensity of developmental research around the world. Although there may come a time when there are only diminishing returns to be had (other than for fundamental science), our assessment is that such an inflection point remains firmly in the future. There are concrete reasons to dedicate resources towards improving and developing existing technology.

Every GPS satellite currently in orbit has four atomic clocks on board. Today's GPS satellites—each containing rubidium and caesium atomic clocks—provide positional signals that allow for an accuracy of within a few metres (typically between 1 and 10). That accuracy is sufficient for guided munitions and civilian navigation, but the need for sub-metre accuracy will grow as autonomous vehicles and drones become more widely used. And, as we get better at building ultra-accurate inertial navigation systems, we'll also need to be able to measure time increments ever more precisely. Finally, advances in atomic clocks will bolster existing military capabilities. A survey of quantum technology conducted by the US Air Force Science Advisory Board (see our further reading list) concluded that strong efforts should be made to prototype miniaturised laboratory clocks and to further improve their accuracy.

Smaller, laboratory standard clocks will enhance signals intelligence, electronic warfare and counter-radar jamming capabilities, while more accurate clocks will facilitate more robust communications. Some 'chip scale atomic clocks' that operate at low power (120 mW) and take up only a few cubic centimetres of volume are already commercially available. Having precise timing at this scale and power will enable a great many useful applications. They're not yet suitable for some of the more demanding tasks; a timing reference with a few orders of magnitude improvement over current commercial chip scale devices would be required for those. That improved level of performance is a focus of research in Australia and around the world.

Inertial measurement units

As quantum technology becomes more mainstream, there's an understandable tendency to prepend 'quantum' before the name of each novel application. That's a useful way to distinguish the old from the new, but it's not always helpful when it comes to understanding the technology in question. That's the case with the term 'quantum compasses'. The parallels you can draw with the familiar north-pointing needles are limited; a classical compass will always point in the same geographical direction, but the 'analogous' quantum system works differently and is more like a classical inertial navigation system.

All inertial navigation systems work by adding up accelerations. If we know where the system (the 'inertial measuring unit') is at the start, and if we know the magnitude, direction and duration of all the accelerations that the system is subject to, then we can calculate exactly where the system has ended up. Of course, 'exactly' is not quite right—there will always be some uncertainty in the measurement of the times and the forces. When many consecutive measurements need to be totalled—as is necessary when a submarine is submerged beyond the range of GPS for an extended period, for example—then the measurement uncertainties stack up. To get an idea of what a 'good' error rate is, we can note that the US Government regulates the export of inertial navigation systems if they tend to drift less than 0.8 nautical miles per hour. Even with top-end systems and hydrographic data, a submarine that's underwater for weeks will accumulate substantial positional uncertainty.

Inertial navigation systems that exploit quantum phenomena have a couple of distinct advantages over the classical alternatives. Certain quantum systems, such as gases of very cold atoms, are very sensitive to accelerations, making them well suited for inertial navigation applications. Their current accuracy is comparable or better than existing classical systems and, as the technology matures, will drastically improve. The quantum realisations are also startlingly compact; in 2015, European and US physicists demonstrated a proof-of-principle atomic gyroscope that could soon be as accurate as the most precise classical devices. But while the best classical systems have a footprint

of roughly 16 square metres, the quantum device covered just 40 square millimetres. In early 2017, German scientists demonstrated a related but more sophisticated technique in suborbital space. Crucially, that meant that the devices and auxiliary equipment had to be packed on board a sounding rocket and successfully launched.

These devices offer a way to compensate for the loss of GPS guidance if an adversary manages to degrade the service by jamming. Given the need for robust and precise navigational systems for precision targeting and other applications, it's not surprising that the US Air Force Science Advisory Board highlighted the potential for 'GPS-denied navigation' that the technology promises. The group identified the need to lead development in this field as the technology reaches prototype levels of readiness over the next five to 10 years.

Magnetometers

Underwater navigation isn't the only challenge for submariners—knowing where other submarines, surface vessels and aircraft are is mission critical. The traditional way for a submerged submarine to gather such 'situational awareness' data is by acoustic means. But, thanks to the prominent role that sonar has played in decades of submarine operations, classical devices have developed alongside quietening techniques to leave offensive and defensive capabilities in rough equilibrium. Worse, modern submarines and dedicated antisubmarine warfare vessels are so quiet that the rate of 'false contacts' in acoustic sensing has grown sharply. Other methods for finding submarines are required.

Magnetic anomaly detectors that pick up the magnetic signature of a submarine have been around for decades. They have never been long-range devices, and were mostly conceived as a way of localising a submarine the general position of which had been determined by other means. Today, the effective range is not more than a few hundred metres and, because the strength of the magnetic field diminishes with the inverse cube of the distance, much more accurate detectors will be needed to extend that range. There are some interesting quantum mechanical phenomena involving magnetic fields, so, perhaps unsurprisingly, quantum techniques have something to offer in that endeavour.

For precision measurement of magnetic fields, among the first quantum-enabled devices were superconducting quantum interference devices (SQUIDs). Originally developed in the 1960s, SQUIDs are extremely accurate devices capable of measuring tiny magnetic fields. To give a sense of what that means, the most sensitive of SQUIDs could detect a fridge magnet from 1.5 kilometres away if it was isolated from other stray fields. But although defence-based applications of SQUIDs are discussed in scientific and national security circles, the technology remains problematic from an operational point of view. The accuracy of the device comes at the cost of convenience; to detect the fridge magnet at that distance, you'd need to average measurements taken over several days. That's OK if the matter at hand is fundamental science—NASA's Gravity Probe B mission used SQUIDs in satellites to test Einstein's theory of general relativity, for example—but it's less useful if the device is intended to provide real-time tactical data. SQUIDs need to be cooled to extremely low temperatures, which is difficult to do outside of the laboratory. Earth's background magnetic field also needs to be filtered out—that's straightforward in magnetically shielded rooms, but harder if the fields to be detected originate from outside the controlled environment. That all gets yet more difficult when the measurement platform itself is moving.

For all those reasons, SQUIDs aren't the most promising of contemporary quantum technologies for detecting magnetic fields, although there was a recent flurry of interest in August 2017, when Chinese scientists announced a breakthrough that, at least at face value, is a solid step towards the successful operationalisation of the technology. The announcement (which was subsequently retracted after the military applications of the discovery were discussed by journalists) detailed plans for a networked array of SQUIDs. If the other (admittedly formidable) problems can be overcome, magnetic anomaly detectors using SQUIDs have the potential to detect submarines from 6 kilometres or more.

Other avenues of active research in quantum detection systems for magnetic fields hold the prospect of producing practical devices that are much less cumbersome than SQUIDs. In March 2017, DARPA announced the Atomic Magnetometer for Biological Imaging In Earth's Native Terrain (AMBIIENT) program. (Yes, we hate forced acronyms too.) That program will investigate new atom-based approaches to magnetometry and complement the Quantum-assisted Sensing And Readout (QuASAR) grant program, which has sponsored research on SQUIDs and other quantum sensors for the past decade or so. Biological magnetic signals are typically very weak, so a robust device able to detect them would have applications well outside the field of biology. Although the compact, rugged and cheap devices envisaged by DARPA won't come to fruition for many years, they could have a far-reaching impact; the grant communique speculates that such devices could facilitate areas such as battlefield medicine (think portable brain injury scanners) and 'magnetic navigation' (pathfinding by reference to the Earth's magnetic field).

There's a final approach to ultra-precise magnetometry that's still very much in its infancy, but worth mentioning because of its promise and the interest it commands around the world. At the microscopic level, the structure of diamonds is famously flawless. But if defects of a particular type—called 'nitrogen-vacancy centres'—are introduced, the resulting quantum system couples very strongly with the external environment and can be used to make sensitive measurements of magnetic fields and many other physical quantities. The advantage of nitrogen-vacancy-based sensors lies not just in their sensitivity, but in their relatively cheap cost and wide range of operating conditions (unlike SQUIDs, they can operate at room temperature). Several start-ups are already looking to commercialise 'NV diamonds' in the field of medical imaging—and that's the area that will very likely see the biggest initial take-up of such devices, although much is promised across a range of fields.

The wider setting

It's probably a fair rule of thumb to assume that, if a physical quantity such as electric field strength, pressure or temperature can be measured classically, there's a clever way to measure it that exploits quantum phenomena. The real question for users in the defence community is whether those measurement devices are practical and cost-effective outside of a laboratory. To the extent that they can be made to be, it's useful to consider their impact in general terms.

It's our general assessment that, except for a few niche exceptions such as magnetic navigation, quantum sensing will mostly improve existing capabilities without offering novel ones. But that doesn't mean they can't be significant, as the example of a potential countermeasure to GPS jamming as discussed above shows. And if very sensitive magnetometers can be successfully operationalised for use on aircraft or surface vessels—potentially including 'swarms' of small unmanned platforms—submarines would be at considerably greater risk of detection by antisubmarine warfare forces. However, it's worth remembering that that same effect could sometimes be produced through other means—in this case, by way of networked acoustic sensors, including submerged sensors, buoys and autonomous underwater vehicles. There's a lot of hype around quantum sensing—as varied as the field is—and some of that hype is justified. But our judgement is that it's improbable that any one technology will deliver a war-winning 'silver bullet' effect. And the measure–countermeasure battle will continue apace. For example, a swarm of small drones capable of generating a submarine-like magnetic signature could be deployed to mask the presence of a patrolling boat.

THE COMPETITION FOR QUANTUM TECHNOLOGY

Our summary of quantum technologies is necessarily 'once over lightly', but it's clear that there are some promising technologies at various stages of maturity. Our judgement is that most of them will be more accurately described as useful rather than revolutionary, with the possible exception of large-scale universal quantum computing. But there's always the chance that we're being overconservative and that an application of quantum technologies will make a profound difference to the world in general, or military affairs specifically. In that context, we should remind ourselves that, as late as the 1930s, a veritable 'who's who' of physicists, including Einstein, Bohr and Rutherford, was on the record saying that the harnessing of nuclear energy for practical applications was unlikely.

We should contemplate the possibility of one or more geopolitical actors getting ahead of the pack and coming up with the next 'revolution in military affairs', perhaps based on a combination of quantum and other technologies. To make a judgement of the likelihood of that, we can look at the history of the two most dramatic recent examples of significant technological ascendancy, both of which saw the US pull well ahead of potential adversaries.

The first—and most dramatic—example was the development of nuclear weapons. In that case, the US wasn't the first nation to realise the potential of nuclear fission to produce an enormously destructive weapon, but it had a unique combination of money, industrial resources and moral respectability—the last of those allowing the US to recruit many of the best scientists in the world for the Manhattan Project, in a way that Nazi Germany couldn't. The intellectual capital that was assembled has probably never been equalled, and the depth of US industry was able to convert the conceptual work into reality in the space of a few years (1942 to 1945).

The result was a lead in nuclear weapons that lasted well into the 1950s, which allowed the US to 'offset' the numerical superiority of Soviet forces in Europe. The monopoly on nuclear weapons was much less long-lived, as the first Soviet test occurred almost exactly four years after the first American test. The Soviets did that through a combination of espionage, being able to assemble their own talented team, and by knowing the 'art of the possible'. It's a point not widely appreciated, but it's often easier to figure out how to do something if you know that someone else has already done it. Just as crossword clues are much easier to solve once you have even only one letter, having a proof of concept and a technical hint or two is often enough to enable rapid progress.

The second offset achieved by the US was a combination of stealth, precision-guided weapon and night-vision technologies that were developed in the 1970s and 1980s. Displayed to the world during the 1991 Gulf War, the second offset built on the huge breadth and depth of the US military–industrial complex that had been assembled over the four decades of the Cold War. The advantage to the US lasted about 25 years and arguably still exists to an extent today, although China and Russia have both developed their own 'counter-offset' strategies to blunt American strengths.

The longevity of the second offset was to some extent a product of its timing. The collapse of the Soviet Union at the turn of the 1990s and the relatively unsophisticated state of the Chinese economy at the time meant that there were no serious competitors to Western military technologies. That's not the case today. In particular, a quarter of a century of rapid economic growth has allowed China to greatly expand its industrial capacity—a process augmented in no small way by widespread industrial espionage. The US is now looking for a 'third offset' that will again give it a decisive advantage over its strategic competition, but it seems less likely to succeed than was previously the case.

Taking the examples of quantum technology discussed in this paper, it's clear that there's extensive global interest, and that no one country has a clear lead across the board. There are groups of talented researchers working in many countries, often in multinational collaborations. The chance of any country being able to make a decisive technical breakthrough and then being able to productionise it as an operational system, all the while quarantining it from competitors, seems remote. In fact, if we look at the example of space-based quantum communication systems, the US might be lagging rather than leading. (With the caveat that we don't know what's in the Pentagon's portfolio of 'black projects'.)

Finally, the likely transformative technologies of the future, many of which are frequently mentioned in the context of the 'third offset', aren't held entirely—or even mainly—within government circles. Quantum technologies are under development in universities and commercial firms around the world. Of particular note are the significant investments being made through the UK's quantum technology initiative and by the EU. Those efforts are looking not only at bolstering fundamental research but at encouraging industry to participate in this new area. In some cases, such as quantum computing, the scale of investment by the global commercial IT industry swamps government efforts. And Chinese firms, many of which are in many ways state-coordinated enterprises as well, are making huge investments in quantum and other technologies. For example, Alibaba now has a portfolio of research projects of over US$15 billion. Because of the globalisation and commercialisation of research efforts, we judge that advantages that any player can generate will tend to be ephemeral, and the rate of diffusion of breakthrough technologies to other players could be quite rapid.

CONCLUSION

There's considerable uncertainty in evaluating the potential impact of the technologies examined in this paper. It's possible that some clever idea or an unexpected (to us) technical development will render some or all of the discussion here obsolete. But with our current understanding, we judge large-scale universal quantum computing as the technology with the greatest potential future impact—and with the biggest developmental challenges ahead of it.

The other quantum technologies we've looked at are all likely to be less difficult to implement but also less revolutionary in their impact. Quantum communication ensures that secure communication channels will be available in future, ironically negating one of the obvious first practical applications of quantum computing. Quantum radar may bring handy improvements in system performance, but it won't render stealth obsolete—being hard to detect will always be preferable to being easy to detect. By providing high-precision local positional and timing information, quantum sensing will help make navigational systems more resilient against interference with GPS and communication networks, reducing some of the vulnerabilities of classical high-tech military systems. Because those technologies are being actively developed by a wide range of groups around the world, we don't see any one nation being able to harvest the benefits at the expense of others, so we wouldn't bet on any quantum-technology-driven re-ascendency of the US. That said, there's enough promise (including commercial promise) in quantum technologies to warrant some additional R&D funding—especially in quantum sensing.

If we had to bet on technology that will really revolutionise military affairs, it would be artificial intelligence, whatever the underlying computing technology—but that's a discussion for another paper.

FURTHER READING

Physics

Because our language is shaped by our macroscopic world, quantum theory is difficult to describe in words. The natural language of quantum theory is the mathematics of Hilbert spaces, which requires university-level mathematics. However, there are a few good explanatory books around for the interested layperson. One we like is Euan Squires's *Mystery of the quantum world*. It's out of print now, but readily available second hand. (There are some other recommendations here.)

For readers willing to dive into mathematics, there's a wealth of more detailed material available online and in print.

Leonard Susskind and Art Friedman's *Quantum mechanics: the theoretical minimum* provides a general introduction to quantum physics; it doesn't shy away from equations, but it's the kind of book shelved in the popular science sections of most good bookshops.

If you've studied some linear algebra and calculus, David J Griffith's *Introduction to quantum mechanics* is a very gentle textbook that will help you understand the quantum world using mathematics rather than metaphor.

One technical resource that we found useful for describing the history of the development of quantum information systems is *The physics of quantum information (*Bouwmeester, Ekert and Zeilinger (eds.), Springer Verlag, 2000). It's still in print (though expensive) or available second hand, but it's also likely to be in most university physics libraries.

The international and strategic setting

A good recent popular piece on quantum technologies is 'Here, there and everywhere', by Jason Palmer, *The Economist,* 2017. The article includes a very good review of international research efforts and R&D spending.

The US Air Force Science Advisory Board's assessment of quantum technologies provides a concise, defence-oriented perspective of prospects, as of 2015. The main findings are available from the board's website.

Marco Lanzagorta is a physicist at the US Naval Research Laboratory who wrote the only current textbook on quantum radar. He's also the co-author of several technical discussion papers that consider quantum sensing, computing and communications in maritime environments, and a more speculative discussion centred on quantum radars in space. The reader can neglect the technical details in the papers and still get a handle on what some concrete use-cases for each technology may look like.

In 2016, the Joint Research Council for the European Commission filed an issues paper titled 'Quantum technologies: implications for European policy'. The discussion, available online, provides valuable insight into interlinked public and private efforts around the world and does a good job of framing the sorts of questions that help to evaluate these technologies.

The Jamestown Foundation has published a good series of articles on the Chinese effort in quantum technologies: *China's advances in quantum information science*, December 2016; *The strategic implications of quantum technologies*, December 2016; and *Disruption under the radar: Chinese advances in quantum sensing*, August 2017.

ACRONYMS AND ABBREVIATIONS

DARPA	Defense Advanced Research Projects Agency (US)
EU	European Union
GPS	Global Positioning System
IT	information technology
NIST	National Institute of Standards and Technology
R&D	research and development
SNR	signal-to-noise ratio
SQUID	superconducting quantum interference device

From little things
Quantum technologies and their application to defence

ISSN 2200-6648