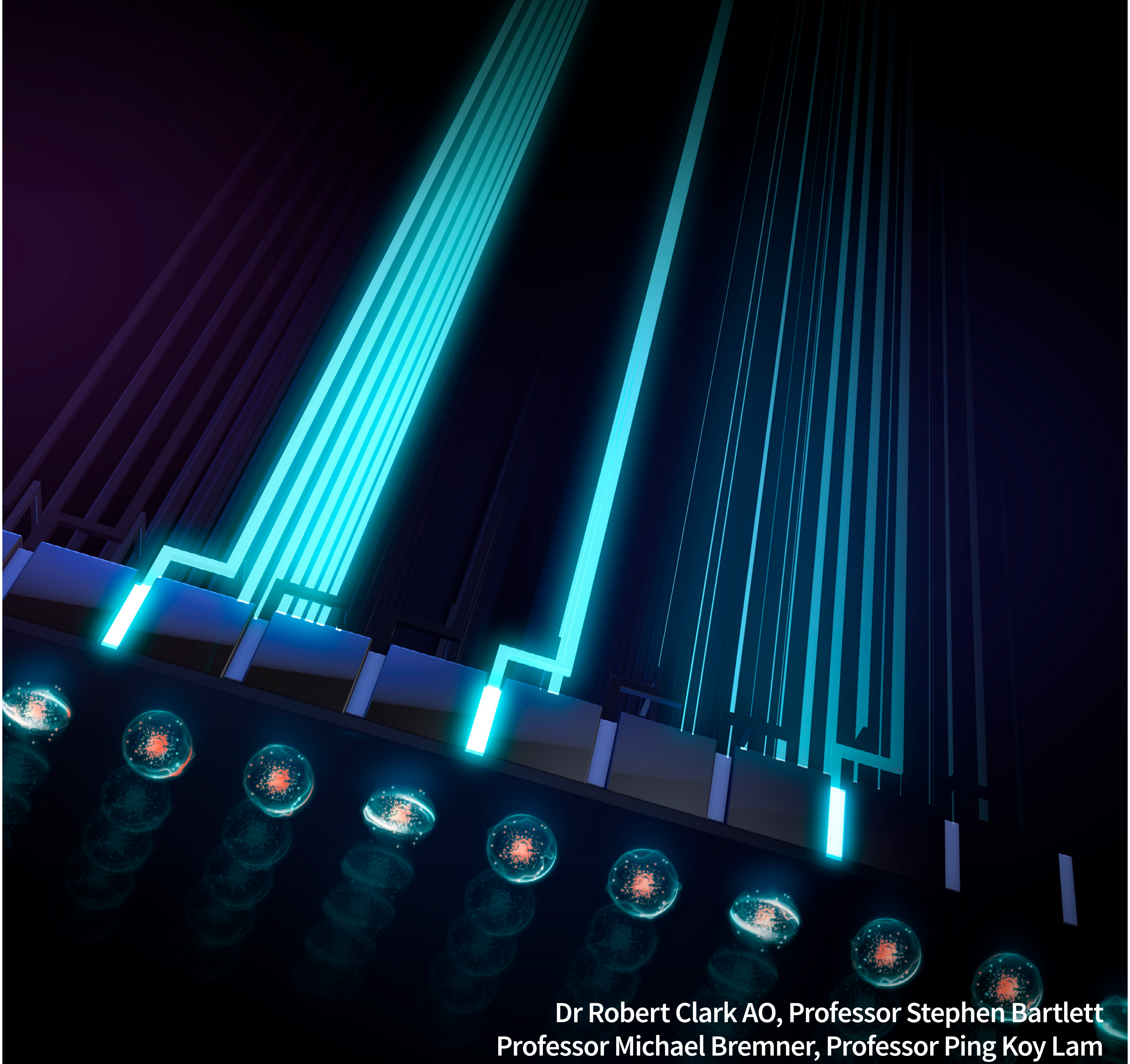
ASPI

SPECIAL REPORT

The impact of quantum technologies on secure communications



Dr Robert Clark AO, Professor Stephen Bartlett
Professor Michael Bremner, Professor Ping Koy Lam
and Professor Timothy Ralph

April 2021

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

TWENTY YEARS OF ASPI STRATEGY 2001 - 2021

About the authors

Dr Robert Clark AO, Project Chair, Australian Strategic Policy Institute

Professor Stephen Bartlett, University of Sydney

Professor Michael Bremner, University of Technology Sydney

Professor Ping Koy Lam, Australian National University

Professor Timothy Ralph, University of Queensland

See page 38 for biographies.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. 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.

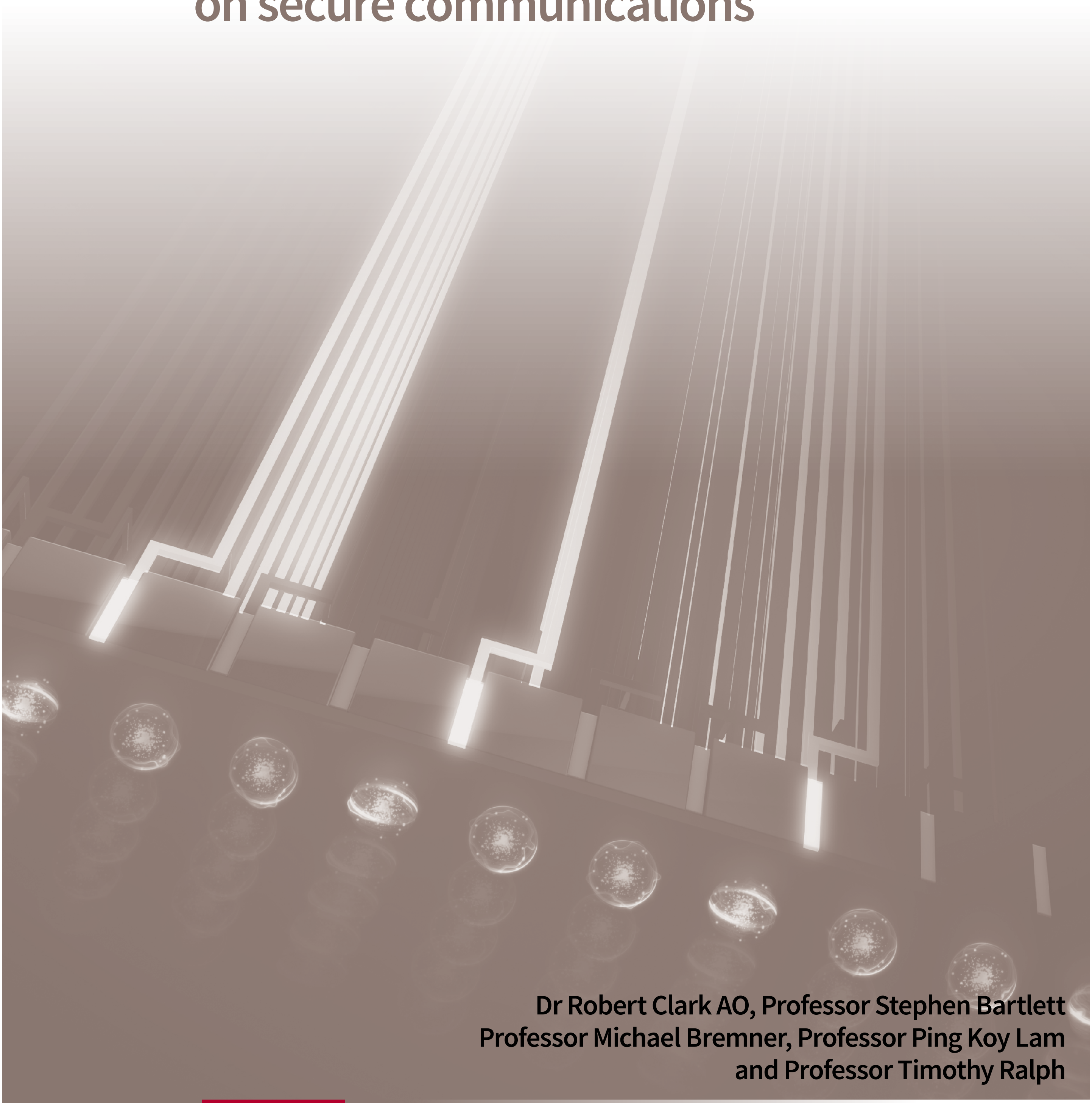
ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal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

Important disclaimer
This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

This report was produced with funding support from the Department of Defence.

Cover image: Artist impression of a proposed quantum chip using a lattice of connected qubits controlled by vertically arranged receivers, iStockphoto/Tony Melov.

The impact of quantum technologies on secure communications



Dr Robert Clark AO, Professor Stephen Bartlett
Professor Michael Bremner, Professor Ping Koy Lam
and Professor Timothy Ralph

April 2021

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021

First published April 2021

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

FOREWORD

Quantum information science (QIS), which ‘applies the best understanding of the sub-atomic world—quantum theory—to generate new knowledge and technologies’, is, according to the US National Strategy for QIS, ‘the next technological revolution’.[1] The prospect of relatively near-term breakthroughs in quantum research offers the possibility of enhancing national industrial capabilities, boosting economic productivity and providing substantial benefits to national security. It is not surprising that the US, China, the UK and other countries are investing heavily into quantum research on the prospect of gaining substantial national benefits while mitigating QIS risks to current technology.

This report by the former Chief Defence Scientist Dr Robert Clark and an eminent expert working group of Australian quantum researchers highlights important opportunities available to Australia if our government is prepared to move quickly to boost QIS research—an area in which Australian science has important strengths.

The Defence Department commissioned ASPI to undertake this research, based on public sources, to examine the impact of quantum technologies on secure communications. Here, a substantial quantum breakthrough has the potential to put at risk ubiquitous public-key cryptography. The US QIS Strategy explains the dilemma:

> … one key quantum algorithm will be able to break public-key cryptography, which secures transactions over the internet. While employing this algorithm is far beyond the current level of technology, the need to protect sensitive data and provide a reliable infrastructure over the long-term requires moving to ‘post-quantum’ or ‘quantum-resistant’ forms of cryptography.[2]

Clark and his colleagues quote a Google research paper that closes with ‘We are only one creative algorithm away from valuable near-term applications.’ The risk is that we are only one creative algorithm away from quantum capabilities that might fundamentally undermine vital national defence and security advantages.

Given the potential of QIS, it is valuable that our government is beginning to focus on Australia’s interests and capabilities in this field. In a speech delivered on 1 February 2021, Prime Minister Scott Morrison said, ‘We need to work with close partners to develop and protect sensitive critical technologies, including quantum computing and artificial intelligence.’[3]

Time is of the essence. Clark et al. propose five immediate recommendations to boost our QIS capabilities and strengthen Australian security:

- Formalise, with the US, a defence and Intelligence community led bilateral research effort on quantum.
- Urgently develop an Australian sovereign capability in intermediate-scale quantum computing within five years.
- Build an international presence in quantum communications and establish critical national infrastructure and formal involvement in international space-based network programs.
- Follow the UK lead to establish a mathematical and theoretical sciences research institute.
- Cooperate with allies and partners to boost industry engagement on quantum research.

The cost of undertaking these steps is tiny relative to our $42.7 billion defence budget, and many existing research programs could support this national effort. The benefit would be to strengthen our defence capabilities against the potentially disruptive effects of quantum breakthroughs internationally, and to put Australia into a strong position to shape our sovereign and alliance interests in quantum technology.

A draft of this report was shared with Defence and valuable comments were incorporated, but, as with all our research, ASPI remains fully independent in the editorial judgements and policy recommendations made by our authors.

My thanks to Bob Clark and professors Stephen Bartlett, Michael Bremner, Ping Koy Lam and Timothy Ralph for their excellent paper and timely call to action.

Peter Jennings
Executive Director, ASPI
April 2021

EXECUTIVE SUMMARY

This ASPI report, which was commissioned by the Department of Defence and is based on publicly available research, examines the impact of quantum technologies on secure communications. It provides an overview of the key technologies and the status of the field in Australia and internationally (including escalating recent developments in both the US and China), and captures counterpart US, UK and Canadian reports and recommendations to those nations' defence departments that have recently been released publicly.

The report is structured into six sections: an introduction that provides a stand-alone overview and sets out both the threat and the opportunity of quantum technologies for communications security, and more detailed sections that span quantum computing, quantum encryption, the quantum internet, and post-quantum cryptography.

The last section of the report makes *five substantive recommendations* in the Australian context that are implementable and in the national interest:

The *first* is to formalise and prioritise Australia–US quantum cooperation within a bilateral framework, coordinated and led by the two countries' defence departments and intelligence communities, via a formal statement of cooperation on quantum technologies under the broader treaty-level agreement between Australia and the US on science and technology. This could be initiated via the 2021 AUSMIN dialogue. Mapping this recommendation to effective Defence Department project management would benefit from the initiation of an Australian model of the US Defense Advanced Research Projects Agency (DARPA).

The *second*, within the bilateral framework, is that it is imperative and urgent that the Australian DoD initiates a comprehensive program, interleaving hardware and software technologies, to attain a sovereign capability in intermediate-scale quantum computing within five years. The program should solicit several implementation pathways for a programmable quantum processor building from Australian strengths and be at a scale to demonstrate quantum advantage, ongoing scalability and adaptability to heavily exercise algorithm development for critical defence applications. The charters of the Defence Department focused Next Generation Technologies Fund and the Defence Innovation Hub are aligned to this recommendation.

The *third* is to build an international presence in global quantum communication via the establishment of critical national infrastructure, and to establish a national quantum communication expert group led by the Defence Department that coordinates strategy and formal involvement in international space-based quantum network programs with key strategic partners. More specifically, establishing the backbone infrastructure of a national optical ground station network for quantum-capable satellite communications is strategically important.

The *fourth* is to establish a mathematical and theoretical sciences research institute, modelled on the UK's Heilbronn Institute for Mathematical Research, that will act as a bridge between the Australian Defence Department and security establishments and the academic community on future threats to communication networks.

The *fifth* is that the Defence Department's approach to prototype development and industry engagement in quantum technologies should also be conducted within a framework of cooperation with our allies and partner nations, in relation both to major corporates and start-ups and to national laboratory facilities.

A key message on quantum technologies relates to urgency. Escalating international progress is opening a widening gap in relation to Australia's status in this field. It is critical that, in addition to its own initiatives, the Defence Department transitions from a largely watching brief on progress across the university sector and start-up companies to a leadership role—to coordinate, resource and harness the full potential of a most capable Australian quantum technologies community to support Defence's objectives.

1. INTRODUCTION: QUANTUM TECHNOLOGY—AN OPPORTUNITY AND A THREAT

The terms of reference for this report from the ASPI Expert Working Group (EWG) focus on the implications of quantum technologies for communications security and call for recommendations to the Australian Department of Defence and national security institutions on how to approach those technologies in a cooperative way alongside our alliance partners.

Our report is consequently shaped by a strong Defence Department mission lens and is based on research using publicly available material. Its recommendations reflect the combined judgement of the EWG and should not be taken as a consensus across the breadth of the Australian quantum technology community, in which there are diverse opinions. Our guiding principle has been to put forward sharp and implementable recommendations that we believe are in the national interest.

1.1 International context: US, UK and Canadian defence focused reports

The EWG commenced its work in November 2020 and with that timing was most fortunate to have access to the US government's new publicly available online portal, *quantum|gov*.[4] The portal was officially launched in October 2020 as the 'home' of the US National Quantum Initiative, which was previously formalised by the December 2018 signing into law of the US National Quantum Initiative Act. This resource and its incorporation of the 2020 US *Quantum frontiers* report[5] additionally provides some 40 key reference papers. The international section of the US portal singularly documents a formal statement of quantum cooperation signed by the US and Japan in December 2019, which is of significance to our Australian recommendations in the context of the longstanding bilateral-treaty-level science and technology agreement between the US and Australia.[6]

Three recent papers in particular from the new US website are directly relevant to our terms of reference:

- *Overview of the status of quantum science and technology and recommendations for the DOD*, US Institute for Defense Analyses, June 2019
- *Applications of quantum technologies*, US Department of Defense, Defense Science Board Executive Summary (cleared for open publication), October 2019
- *Identifying research challenges in post quantum cryptography migration and cryptographic agility*, US Computing Community Consortium, 2019.

Those expert papers provide an international overview of technical status, astute findings and actionable recommendations for the US Defense Department, some of which map well to the Australian Defence Department. In relation to technical status, the US National Academy of Science's 2019 report on progress and prospects for quantum computing is also cited as a valuable and reliable assessment.[7] The post-quantum cryptography (PQC) paper captures the lead of the US National Institute of Standards and Technology since 2016 in developing and standardising the migration of public-key cryptography to new PQC algorithms that are 'quantum-resistant' or 'quantum-safe'[8] (a substantial undertaking; see below). It suffices to say, however, that US Government agencies' strategy and planning for quantum technologies clearly goes well beyond the recommendations in just a few publications, but has been shaped by more than two decades of detailed activity, considerable investment and proactive leadership.

In the US Defense Science Board Chairman's letter within the board's 2019 executive summary, the following statement is important:

> Quantum technologies exhibit remarkable potential to enhance or upend current warfighting capabilities. Fields such as sensing, computation, and communications are key mission areas. It is crucial that the Department of Defense (DOD), along with our allies and partners, maintain the leading edge in understanding these technologies. Industry and academia also play a vital role in the development of quantum technologies, and their collaboration with DOD could reap benefits for all parties. This is particularly pressing given adversarial investments being made towards quantum superiority, if not dominance.

An additional highly relevant publicly available resource is a UK Defence Science and Technology Laboratory (DSTL) research paper published by DSTL on behalf of the Ministry of Defence in collaboration with UK Strategic Command, *Quantum information processing landscape 2020: prospects for UK defence and security*,[9] which outlines how embracing quantum technology now could lead to enhanced pace, precision and pre-emption of decision-making by military commanders. In its detail, that work examines the potential for artificial intelligence (AI) software based on neural-net algorithms to run on commercially available quantum computers.

In January 2021, the Canadian Armed Forces and Department of National Defence also released a Quantum Science and Technology Strategy, the first of any Canadian federal department.[10] While that document gives broader guidance than the US reports, with an emphasis on quantum sensors, its content reinforces the central importance of the breadth of quantum technologies to the Defence mission and of Defence leadership in coordinating the national effort.

By way of introduction, we extract and summarise here key points from this literature, largely in the original wording of those authoritative sources.

1.2 The impact of quantum computing on communications security and status

The single most important reason that the *status quo* in secure communications cannot continue is the development of large-scale (fault-tolerant) quantum computers. Below, we outline this central issue, which provides objective context for our report's structure.

Modern information security is founded on public-key cryptography. This describes a class of encryption systems that is widely used in securing communications on the internet, for example, for financial transactions. Along with well-known consumer applications, it is also used extensively for commercial, government and military applications. The security of these systems is based on the presumed difficulty of solving certain mathematical problems; as long as those problems are impossible to solve, even with significant devoted supercomputer resources, the security of the communications is ensured. The most common such systems used today are based on mathematical problems that have resisted attack for many decades.

Quantum computing disrupts this *status quo*, as it has been demonstrated that algorithms executed on a quantum computer can efficiently solve many if not all of those mathematical problems. That is, a quantum computer will render public-key cryptography schemes insecure. Of particular concern is that a sufficiently powerful quantum computer will not only be able to crack most secure communications in future, but will also be able to decrypt all past communications that have been archived. As a result, the mere possibility that quantum computers may be built in the coming years has prompted a major re-evaluation of secure communication and the development of post-quantum cryptography.

Quantum technology itself offers another way forward, via quantum key distribution (QKD) and other encryption techniques. QKD utilises properties of quantum physics (entanglement and non-locality of distant parties, and quantum uncertainty—the unique feature that an unknown quantum state cannot be copied without disturbing it) to securely distribute a secret cryptographic key through an insecure channel, which can then be used for secure communications. While QKD is 'information-theoretic' secure, in practice, however, there are certification challenges in authentication between parties, susceptibilities of physical hardware, channel losses and denial of service that have precluded its adoption. QKD currently remains the subject of ongoing R&D to potentially overcome those issues. Europe and China are dominant players in QKD technologies.

We return to the central point about the availability of a large-scale quantum computer. The status of quantum computer development has been divided into three tiers:

- component quantum computers (a few 'physical' qubits)
- noisy intermediate-scale quantum computers, or NISQs (tens to thousands of 'physical' qubits)
- fault-tolerant quantum computers, or FTQCs (error-corrected 'logical' qubits each comprising thousands of physical qubits at currently achievable error rates).

The different approaches to building a digital quantum computer include trapped-ion, superconducting Josephson junction, semiconductor, photonic and topological qubits. Until most recently, the international situation was that superconducting and trapped-ion implementations had entered the NISQ phase and that no approaches were anywhere close to being in the FTQC phase. In particular, Google's 53-qubit Sycamore processor with programmable superconducting qubits has demonstrated 'quantum supremacy' over state-of-the-art classical computers in the task of sampling the output of a random quantum circuit (published in October 2019).[11] Estimating the classical computational cost via benchmarking comparison using the Oak Ridge National Laboratory's Summit supercomputer (the most powerful worldwide) and Google clusters, this specific computational task achieved on the Sycamore quantum processor in 200 seconds was estimated to take 10,000 years of classical simulation. An IBM paper later argued that classical simulation can be improved to cost a few days by leveraging secondary storage.[12] IBM has similarly pursued quantum computing based on superconducting qubits, and its 65-qubit NISQ processor is accessible to external users via a cloud platform. IBM's quantum computer road map cites a 1,000-qubit goal by 2023.[13]

In December 2020, shortly after our EWG convened, however, the University of Science and Technology of China (USTC) published a report of its development of an all-optical (photonic) quantum computer in the NISQ regime, built at sufficient scale and precision to also demonstrate quantum supremacy.[14] As for the Google Sycamore demonstration, this was for a specific task of sampling instances of a particular highly complex probability distribution, and the USTC paper claims the demonstration of a greater quantum advantage than the Google result, although the USTC photonic quantum computer is not in its present form programmable for other tasks. The USTC's benchmarking of quantum supremacy was via the Sunway TaihuLight supercomputer, from which the researchers estimated that the task achieved by the photonic quantum computer in 200 seconds would require 2.5 billion years of classical simulation. Being an all-optical configuration operating at telecommunications wavelength, the USTC device is directly compatible with quantum networks. Most recently, in February 2021, the USTC further reported (in an unrefereed research publication[15]) its design and fabrication of a programmable 62-qubit solid-state quantum processor composed of superconducting qubits in an 8 × 8 qubit array. The report details its demonstration of quantum walk functionality that is integral to enhanced search and other capabilities and cites its 2D processor architecture as opening a pathway to large-scale quantum computing. The USTC is based in Hefei, and in 2020 China announced its intention to build an $11 billion national quantum laboratory in that city.

Notwithstanding technical details, quantum computing has squarely moved on from two decades of component quantum computer R&D to enter the NISQ regime—an important stepping stone to FTQC—via at least three implementation pathways. Access to a NISQ machine will allow quantum-compatible software development to be heavily exercised and, as the closing sentence of the Google paper foreshadows: 'We are only one creative algorithm away from valuable near-term applications.' In this regard, the DSTL report provides an indication that AI/neural-net algorithms running on NISQ machines potentially provide a pathway to significantly improve important analysis tasks using real-time and near-real-time data feeds, to identify features of interest and instances of change of direct relevance to enhanced Defence Department leaders' 'data-to-decision' processes.

1.3 New opportunities from quantum networks: a quantum internet

The publicly available US quantum technology assessments strongly highlight the importance of quantum networking to securely pass quantum information across distant channels at high throughput and low loss, for which quantum entanglement distribution, teleportation, memory, repeaters and advanced photonic technologies generally are central to building the Holy Grail of a quantum internet. This also spans the networking of quantum computers (including quantum computers of different qubit types) for distributed quantum computing. Currently, entanglement distribution over more than 1,000 kilometres has been demonstrated, albeit at very slow rates. Over shorter distances (a few kilometres), entangled photon generation at tens of kilobits per second and quantum memory entanglement at 10 bits per second have been demonstrated. Quantum networks based on secure (trusted) nodes have been demonstrated in Europe and China.

In 1969, the entire internet connected UCLA, UCSB, the University of Utah and the Stanford Research Institute in California within the US—indicating just how quickly communications technology can escalate from humble beginnings. US Department of Energy's *America's blueprint for the quantum internet* report foreshadows a quantum network connecting the 17 Department of Energy laboratories—a similarly finite start that could equally disrupt and change the communications world as we know it.

Quantum sensors are judged to be a near-term application of quantum technologies. While this important category is outside of our terms of reference, we note here for completeness that entanglement distribution and quantum networks can be used to develop high-accuracy, large-aperture networked sensors with significantly enhanced resolution and coordination.

1.4 Australian perspective

With this brief introduction, in the context of secure communications, our report is structured to provide an overview of quantum computing, quantum encryption, quantum networking and post-quantum cryptography to assist government decisionmakers. It also outlines Australia's status in each of those areas and our judgement of how Australia might best contribute within its alliance and partner frameworks to both optimally support the Defence Department and to be a valued international contributor. The final section of our report contains timely, affordable and implementable recommendations on the central strategic and technological issues.

Australia has world-class credentials in quantum technology research with numerous US and international links. As in other nations, the dominant early contribution has come from the university sector, which includes a number of Australian Research Council Centres of Excellence and other significant university teams with an excellent publication record of exceptional quality. In particular, Australia has strengths, developed over two decades, across the span of necessary capabilities in semiconductor, superconductor, atomic and optical quantum devices with applications to computing, communication and sensing. Quantum computing technologies based on silicon, in particular, have underpinned a major national effort since 1998, with significant government and industry support. That support has brought success in the development of qubits with silicon donor atom, silicon quantum dot and hybrid systems, each of which have potentially independent manufacturing and commercialisation pathways. Similarly, many Australian firsts in optical quantum computing stand out internationally. Australian researchers have skills and knowledge in specific component-level technologies and specialised theoretical topics; however, the translation of their research into prototype development encompassing industry and government laboratory partnerships, both in Australia and with our allies, will be critical from a national security perspective. Internationally, over the past five years, commercial interests have entered this research domain with impact.

Significant-scale start-up companies have formed in Australia (Silicon Quantum Computing, QuintessenceLabs, Q-CTRL) and in North America, centrally involving Australian researchers (for example, Silicon Valley-based PsiQuantum Corp, Xanadu in Canada) and Australian researchers have leading roles in major corporates conducting quantum research (such as Microsoft and IBM). The Australian quantum community has developed an initial road map, which while broad in its concept reflects a capable and vibrant community seeking to coordinate its activities. The recently launched Sydney Quantum Academy, collaborating across academia, government and industry, has a focus on developing diverse talent within that quantum ecosystem.

Notwithstanding this excellence, the step from research to development and impact in quantum technologies internationally is an extremely large one, requiring among other things sustained and significant resources for scale-up. Already, for example, the world has moved from component-scale to intermediate-scale quantum computing, and Australia is yet to enter the NISQ regime. It is with this calibration and escalating international progress in mind that the EWG, with its Defence focus, has gauged its recommendations.

In concluding these introductory remarks, it is important to emphasise the strategic importance of a national capability in quantum technologies, referred to in Prime Minister Morrison’s National Press Club speech of 1 February 2021, in which he said, ‘We need to work with close partners to develop and protect sensitive critical technologies, including quantum computing and artificial intelligence.’

2. QUANTUM COMPUTING

2.1 A new kind of computing—not just faster computers

As discussed above, in 2019 Google publicly revealed its newly developed Sycamore quantum processor and announced that it had successfully performed the first computation that was simple for a quantum computer but extraordinarily difficult for even the most powerful supercomputers.[16] Before then, the world's ever-increasing computing power had been driven by continual improvements in transistor fabrication technology. The past 50 years have seen extraordinary progress in computing power. Yet, despite those massive technological changes, the fundamental mathematical rules that drive computers have remained relatively unchanged. Google's demonstration of so-called 'quantum supremacy', also referred to as 'quantum advantage', was built on 30 years of breakthroughs in mathematics, computer science, physics and engineering and signalled the beginning of a new era that could potentially involve significant disruption in the technology landscape.

Conventional ('classical') computers manipulate information encoded in bits, usually represented by the presence (or not) of a small electrical current. Computational complexity theory tells us that this choice leads to problems that will be forever costly for classical computers. In simple terms, the classical cost of simulating complex physical or chemical systems doubles with the addition of every new particle. This led American Nobel Laureate Richard Feynman in the early 1980s to propose quantum computers as a way of circumventing this exponential cost. Quantum computers manipulate information encoded in quantum mechanical components, termed 'qubits'. For example, in Google's Sycamore processor, qubits are encoded by superconducting electrical currents that can be manipulated via carefully designed electrical componentry.

Quantum computing remained an academic curiosity until it was discovered that quantum computers could also be used to efficiently solve the 'factoring problem', in which a computer is tasked with discovering the prime factors of a large number. This key problem forms the basis of the RSA public-key cryptosystem, which is a cornerstone of internet security. With that discovery, a significant amount of research activity worldwide set out to establish whether quantum computers could be built and to determine their computational power.

2.2 Relationship to information security—the threat

Current RSA public-key (asymmetric) cryptography systems and other variants rely on trapdoor mathematical functions that allow the easy computation of a public key from a private key but make the inverse computation, of a private key from a public key, computationally infeasible. Specifically, widely used trapdoor functions rely on the difficulty of integer factorisation and elliptic curve variants of the discrete logarithm problem, both of which have no known solution for computing an inverse in polynomial time (that is, on a finite timescale). In short, this 'computational hardness' ensures security.

In 1994, however, Peter Shor outlined a quantum algorithm that could be used to perform integer factorisation in polynomial time on a sufficiently large-scale quantum computer.[17] That now-famous quantum algorithm has subsequently been shown to generalise to also solve the discrete logarithm and elliptic-curve logarithm problems in polynomial time.

The development of an FTQC coupled with this quantum algorithm consequently threatens the security of current asymmetric public-key cryptography. Moreover, Shor's algorithm provides a striking illustration of the potential for innovations in the mathematical and physical sciences to threaten secure communications more broadly.

In addition to Defence Department and critical cyber infrastructure systems, the digital transformation of the world involving some 4 billion internet users, 2 billion websites and more than $3 trillion in retail activity all have their security underpinned by current public-key cryptography at many layers. While the development of an FTQC has been assessed to be at least one or two decades away, there is nonetheless urgency to address this issue due to the 'record now, exploit later' threat, in which encrypted information is captured and stored for later decryption by an FTQC when it becomes available.

The development of new public-key algorithms that are 'quantum hard' is consequently of pressing importance for the US National Institute for Standards and Technology Post Quantum Cryptography Project, which involves international partners—a security 'patch' for the internet.

2.3 Applications of quantum computing—the opportunity

Notwithstanding the threat that the existence of a large-scale quantum computer (an FTQC) poses for information security, the potential of intermediate-scale (NISQ) processors to provide unprecedented computing power in the near future opens a wide opportunity space, particularly with regard to critical Defence Department applications and Defence's technology edge.[18] The recent availability of NISQ processors has significantly altered the quantum application development pathway. This has allowed for a heuristics-driven approach that has enabled much wider participation and industry involvement. Previously, quantum algorithm development was largely looking into a distant FTQC future and required highly specialised mathematical skills to determine the utility of a quantum application. We expect that in the near future that will no longer be necessary for practical quantum advantage. Consequently, it will be important for Australia, and in particular the Defence Department and government agencies, to have access to NISQ devices that we expect will allow for early mission-oriented applications to be developed.

While NISQ processors do not in themselves threaten communications security, this recently achieved intermediate regime allows, for the first time, quantum hardware and software development to be combined in the 'quantum advantage' regime, which could well lead to an acceleration of progress. That reinforces Australia's need for a sovereign NISQ capability.

2.4 Current status and timelines—the international landscape

The concept of the quantum computer took its modern form in 1995, when the basic architecture and design principles were developed. Almost immediately, researchers in universities, government laboratories and IT companies began advancing the technology behind it, and the US, Australia, the UK and Canada demonstrated early leadership. Research was primarily based in the university sector until around 2015. While the role of universities in quantum computing research continues to grow, investment from the private sector has expanded significantly in recent years. Several multinational technology companies have multibillion-dollar quantum computing programs, and there is a dynamic start-up community. Beyond technology development, there is also significant activity in data-intensive companies (in the finance, pharmaceutical, transport and energy sectors) pursuing quantum computing as end users.

Various technologies are being pursued for quantum computers: superconductor, semiconductor, atomic and photonic. Superconductor and semiconductor technologies are most compatible with a 'chip-based' design and can build on the nanofabrication capabilities of the computer industry; however, those approaches present several challenges in materials and control. Atomic and photonic approaches use the remarkable precision of atomic clocks and the coherence of the telecommunications industry but will be challenging to build at scale beyond the NISQ regime. There is no clear leading technology for quantum computer design, and corporates and governments are choosing platforms largely based on the expertise of their resident scientists.

A number of prototype quantum devices consisting of tens to hundreds of components have been fabricated on a range of different platforms. The scale of those devices (around 50 qubits) is of interest because a quantum device of that size is capable of performing operations that are beyond the reach of conventional supercomputers.[19] However, the devices suffer from high error rates, making it challenging to execute quantum algorithms of interest. The NISQ regime is expected to encompass the hardware development for the field until at least 2025. During the five years from 2021 to 2025, it is expected that quantum computers with 100 to 1,000 components will become available, also across a range of platforms, and that error rates will improve.[20] The ability to scale up those different platforms, while also reducing error rates, will determine which technologies are the most promising to develop.

While it is encouraging that devices in this regime can 'outperform' conventional supercomputers at certain very specific tasks, the development of practical applications, notwithstanding the high error rates, is the subject of major international activity. There is considerable enthusiasm from the business and technology sectors to find useful applications for NISQ devices, but the development of applications beyond the highly constrained demonstrations to date is an open research area. One most promising direction for NISQ devices is in solving specific optimisation problems.

Much of the work to develop NISQ applications has been enabled by commercially produced prototypes available as cloud services. IBM was the first company to make quantum processors available in this way and has now developed its extensive IBMQ network, a node of which is based at the University of Melbourne. Limited access to some of IBM's processors is available as a free service for non-commercial research. Access to IBM's more powerful processors is available only to research partners of IBM, or as a paid service through the IBMQ network. Google has been slower to make its processors broadly available, granting cloud access only to close research and commercial partners. In 2020, Amazon Web Services and Microsoft both launched services enabling quantum processor vendors to connect to potential end users via the Amazon Web Services and Azure networks, respectively. Xanadu has recently made its optical processor available in the cloud.[21] Widespread access to premier quantum computing processors is available to Australian researchers only through paid services or through research partnerships with those companies. Notably, the design of these NISQ devices remains an active area of research, undertaken almost exclusively in large, coordinated efforts involving both algorithm and hardware design in tandem. The opportunities for innovative algorithm development through access only to remote devices in the cloud are limited, compared to those integrated efforts.

Notwithstanding the optimism about NISQ devices, it is widely expected that quantum hardware will need to correct for errors occurring throughout the computation in order to successfully execute the most powerful quantum algorithms, such as those that threaten communications security. Quantum computers that can operate robustly despite the occurrence of errors are said to be 'fault tolerant'. The essential operations required to correct for errors in a quantum computation have recently been demonstrated in testbed systems. However, building a fault-tolerant quantum computer at scale, using perhaps millions of components, is a daunting challenge. Fundamental scientific and engineering challenges must first be addressed. Predictions about when large-scale fault-tolerant quantum computing will be possible vary widely, but the most common view is that fault-tolerant quantum computers with thousands of components will be available in the time frame from 2025 to 2030, and that larger devices capable of executing quantum computations that impinge on communications security will be available after 2030. There is considerable opportunity for disruptive quantum technologies to compress that timeline.

The *Quantum threat timeline report 2020* commissioned by the Global Risk Institute recently surveyed 44 experts to assess potential timelines for the production of quantum processors that can threaten network communications systems.[22] Given a 10-year time frame, 11 respondents judged that that there was a greater than 50% chance of a such a device being developed. That proportion more than doubled when respondents considered a 15-year time frame (23/44). When survey participants considered a 20-year time frame, the number jumped again to 38 respondents, or 86% of participants.

In this setting, most developed countries have established national programs to encourage the development of quantum computer technologies and to explore the potential benefits. The most significant activities in most countries are meant to encourage commercial investment and attract research and business talent. The US, the UK, China and other countries have identified a need, connected with strategic priorities in defence and intelligence, for sovereign capability in this area. In the US, the intelligence community, through the Director of National Intelligence, has sponsored a very active unclassified research program in quantum computing through the National Security Agency's Laboratory for Physical Sciences since the late 1990s, and more recently through the Intelligence Advanced Research Projects Activity. There is early discussion on developing supporting technologies for the research community, such as the Qubits for Computing Foundry. In the UK, the National Quantum Technology Programme has been in place since 2014, and in 2019 included the creation of the National Quantum Computing Centre. Concurrently, in 2014, the UK DSTL launched a DARPA-like project to develop quantum technology at pace; although it originally focused on quantum sensors, in 2020 it released a new forecast and a list of recommendations that more directly targets quantum computing research.

2.5 Australian perspective

Australia has world-class capabilities in quantum technology R&D. It was a pioneer in the nascent years of quantum computing, establishing early global leadership in both semiconductor and photonic approaches to quantum technologies, as well as the theoretical foundations for the field. Australia now hosts a broad quantum technology research community across many universities, which is collaborating deeply with leading international research laboratories and multinational corporations and is complemented by a lively start-up sector.

While researchers in Australia contribute to the development of quantum computer technology in myriad ways, the scale of demonstrated Australian capability remains small, involving 10 or fewer operating components. In the US and China, intermediate-scale (NISQ) devices involving 100 or more integrated components are becoming common. Australia does not currently possess a sovereign platform for developing technology, operating systems and software in the NISQ regime. More broadly, while Australian quantum computing technology at component scale continues to be world class, the quantum computer areas in which Australian research is world leading have become increasingly limited.

It is becoming clear that the NISQ regime, in its own right, will be of strategic importance. Consequently, it is essential that Australia maintains broad access to the full span of NISQ development, from hardware-focused activities such as fabrication and control systems to software-heavy operating system design and application development. Consequently, a recalibration and opening up of opportunities for Australian component-scale capability to develop NISQ prototypes and applications via a coordinated program that spans more than one pathway will be a wise Defence Department-driven investment. We see this as an urgent de-risking issue.

3. QUANTUM ENCRYPTION

A direct impact of quantum technologies on the security of communications arises from the possibility of replacing current encryption methods with quantum encryption protocols.[23] In principle, quantum protocols have higher, sometimes unconditional, levels of security, and the practicality of their implementation is rapidly improving. The development of quantum encryption technologies is an active area worldwide, but especially in Europe and China.

3.1 Entanglement

Many different quantum protocols have been proposed. Some require only the local preparation and measurement of individual quantum systems. Others require the preparation and distribution of individual quantum systems. The most powerful require the distribution of correlated (that is, entangled) quantum systems.

Entanglement is a unique property of quantum mechanical systems that is characterised by correlations between communicating parties that are stronger than those allowed by classical communication systems.[24] Entanglement implies privacy and randomness. For an ensemble of maximally entangled subsystems, one held by a sender (Alice) and the other by a receiver (Bob), measurements of the subsystems will give Alice and Bob identical, completely random strings of outcomes that are unique. That is, it is guaranteed that the outcomes are random and that no other parties can have a copy of the string.

Those features of entanglement are the key ingredients for most quantum encryption protocols. Thus, the ability to distribute entanglement between distant parties is a key resource for secure quantum communications.

3.2 Random number generation

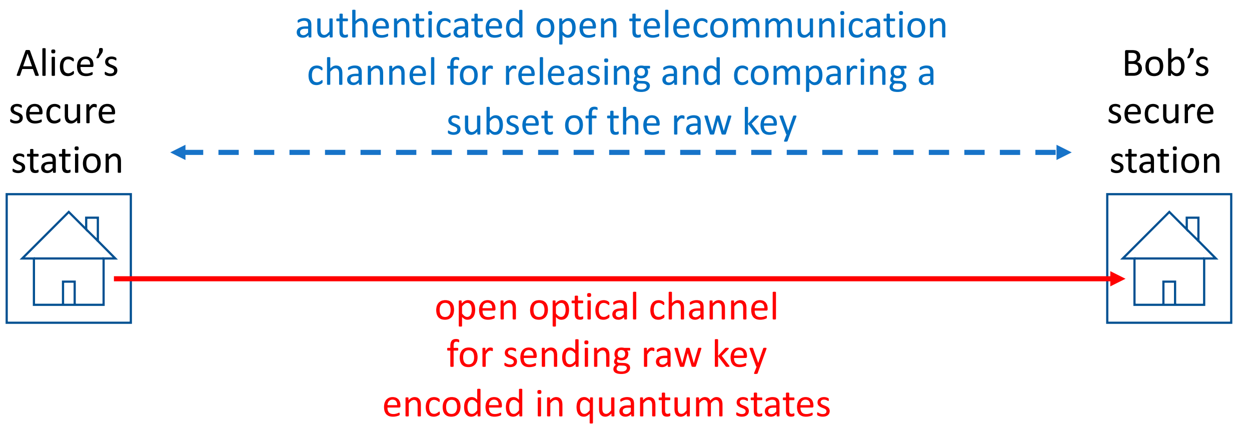
A simple application of those properties of entanglement is random number generation.[25] Consider a beam of light passing through a beam-splitter that transmits 50% of the light's intensity. It is possible to prepare such a beam as a string of individual photons. Quantum mechanics says that whether a photon is transmitted or reflected by the beam-splitter is a genuinely random event. Thus, if a photon counter is placed in the transmitted beam and photon arrivals are recorded as 1's and non-arrivals as 0's, then a binary random string will be generated. Such a string has many uses, including for secure encryption. Though conceptually simple, such a system has several technical challenges. Systems like that and also ones based on other quantum systems have been demonstrated. More sophisticated protocols employ the entanglement intrinsically generated by such systems to guarantee not only genuine randomness, but the absolute privacy of the random numbers generated.

3.3 Quantum key generation

Quantum key distribution (QKD) is arguably the most developed quantum encryption protocol. Simple systems that can operate over short distances are commercially available, and 'hero' experiments have demonstrated longer links and several field tests of simple networks. QKD is a method for securely distributing a secret cryptographic key through an insecure channel.[26] The secret key can then be used for secure communication, in most instances as a form of one-time pad. The privacy and randomness of the key are ultimately derived from the properties of entanglement.[27]

The basic set-up for a QKD protocol is shown in Figure 1.

Figure 1: Schematic of a QKD protocol


Alice's secure station
authenticated open telecommunication channel for releasing and comparing a subset of the raw key
Bob's secure station
open optical channel for sending raw key encoded in quantum states

A raw key (a sequence of random numbers) is encoded in quantum optical states sent via an open optical channel between secure stations (Alice and Bob). Using an authenticated open telecommunication channel, some of the raw key is revealed and compared by Alice and Bob. Applying quantum information analysis to the revealed key, Alice and Bob can determine the maximum possible information leakage to a third party (Eve, the eavesdropper). If that analysis concludes that Alice and Bob have an information advantage over Eve (that is, they know more about the key than Eve does), then they are able to distil a specific amount of secret key from the remaining raw key through error-correction and privacy-amplification algorithms. That secret key will be completely private to Alice and Bob.

The *strengths* of QKD are as follows:

- Few/no assumptions are made about the physical/computational power of potential eavesdroppers
- The protocol is future proof—future advances in technology do not compromise the security of current communications.

The in-principle *weaknesses* of QKD are that it:

- requires user authentication
- is subject to denial-of-service attacks.

For details about the current limitations of QKD and prospects, see box.

QKD details

Current limitations—hardware and software

The proportion of secret key that can be distilled from the raw key depends on the size of the information advantage over Eve that can be determined (the bigger, the better). The size of that information advantage depends on:

- the length and quality of the optical channel
- the quality of the quantum optical devices
- the tightness of the information bounds imposed by the quantum information analysis
- the quality of the error-correction and privacy-amplification algorithms.

In turn, the impact of those various conditions depends on the particular protocol being implemented, and there are trade-offs between different conditions for different protocols. The secret key rate then depends both on the information advantage and the rate at which raw key can be communicated. Again, between different protocols there can be trade-offs between the achievable raw key rates and information advantages. All things being equal, increasing optical channel length reduces both the raw key rate and the information advantage. Thus, there is a direct trade-off between the secret key rate and the distance between Alice and Bob: the greater the distance, the lower the key rate. If the distance is too large, no secret key can be exchanged.

A QKD protocol is said to be ‘robust’ if, under the typical ambient conditions for the optical channel, the secret key can be generated. A QKD protocol is said to be ‘device independent’ if it is unnecessary to trust the various quantum optical devices used in the protocol. It is currently very difficult to make a protocol both robust and device independent, so careful calibration of the quantum devices is necessary to eliminate security loopholes.

As shown in Figure 1, the archetype QKD system is point to point. Clearly, the ability to link up a secure network is highly desirable. Currently, that is very hard to do without introducing trusted (that is, secure, authenticated) nodes. Hence, the practical weaknesses of QKD, given current technology, are:

- slow key rates / limited distances
- security loopholes opened by non-ideal or compromised quantum devices
- key exchange that is only point to point.

Key rates can be greater than Mbits/second for distances of 50 kilometres or less but fall to Kbits/second levels by about 100 kilometres. A secret key can still be generated for distances out to a few hundred kilometres in fibre systems, but key rates fall to low levels. The current record in the field is 500 kilometres with a secret key rate of 3 bits/second.[28] The absolute record distance for secret key exchange is 1,120 kilometres achieved via a free space link involving a satellite, but the secret key rate was 0.1 bit/second.[29]

Prospects for relaxing current limitations

There are a number of avenues via which QKD systems may achieve enhanced performance and become more practical in the future:

- *Fields versus photons.* In principle, the highest secret key rates are achieved by QKD systems based on encoding information on field variables, such as amplitude and phase (also known as continuous variables), as opposed to single-photon degrees of freedom.[30] Unfortunately, technical limitations have so far not allowed field QKD systems to realise their full potential. That could change in the future.
- *Tighter bounds on eavesdropper information.* Security in QKD is based on bounding Eve’s information, but often those bounds are loose; that is, Eve is assumed to have much more information than she could physically access. If those bounds could be tightened, higher key rates would ensue.
- *Technological improvements.* Quantum optical technology is constantly improving, leading to constantly improving rates and distances for QKD.
- *Repeaters and networks.* The development of quantum repeaters (the quantum equivalent of amplifiers in telecommunications systems) and the subsequent deployment of quantum networks would allow QKD to be extended over arbitrary distances and between multiple users.

The *importance* of QKD and the development of QKD protocols has a number of aspects. First, there is the ability to deploy useful secure communication protocols. Initially, they are likely to be niche applications, including in high-security situations in which future proofing is crucial and in situations in which laser communications are already the preferred solution. As the technology matures, the applications are likely to expand. Second, we need to understand adversaries' capabilities for secure communications that are enabled by QKD. Such adversaries could include other nation-states as well as rogue or criminal elements within or outside Australia. Finally, the exacting requirements of QKD protocols act as a driver of quantum communication technology for more diverse future applications.

3.4 Entanglement distribution and quantum encryption

If high-quality entanglement can be communicated between distant locations, a number of other quantum cryptography protocols become possible in addition to QKD:

- *Quantum bit commitment.* Bit commitment is a cryptographic protocol whereby one party, Alice, generates, at some initial time, a bit that she wishes to keep secret from another party, Bob, until after a later time when it is revealed. Both parties wish to be assured of the other's honesty. While local protocols for secure quantum bit commitment are not possible, distributed protocols can be shown to be unconditionally secure due to fundamental properties of quantum mechanics and relativity.[31]
- *Quantum digital signatures.* Signatures are mainly used to confirm that the sender of a message is who they claim to be. The ability to distribute high-quality entanglement allows the deployment of quantum protocols for authenticating users via the distribution of quantum signatures.[32]
- *Distributed quantum computing.* If entanglement can be distributed, then quantum computing can also be distributed between distant subprocessors, for example by using teleportation to move quantum information between the subprocessors. The properties of entanglement mean that any information about the quantum computation may be extracted only through the correlations between the results of the subprocessors, requiring multiple parties to cooperate in a secret-sharing-like scenario. More sophisticated protocols can allow 'blind quantum computing', in which a party can have a quantum computation performed by a central 'mainframe' quantum computer, without revealing to the mainframe the nature or result of the computation.[33]

More generally, the existence of maximal distributed quantum entanglement between two stations allows quantum information to be moved between the stations as if an ideal quantum channel exists between them via the technique of quantum teleportation.

3.5 Australian perspective

Australia has a strong quantum optics community that has been involved in quantum encryption research for over two decades, both in experiment and in theory. Many research groups and centres of excellence are involved. In particular, Australia has pioneered research into approaches to quantum encryption that align better with current telecommunications infrastructure. The first QKD protocols of this kind were invented,[34] developed, demonstrated[35] and commercialised[36] in Australia. Quantum random number generation based on laser fields has also been developed and demonstrated here.

Looking to the future, our access to the southern sky makes Australia strategically valuable as part of a global quantum internet.[37] Australian groups have long been involved in research aimed at developing quantum communication between ground stations and satellites and developing the free-space protocols needed.

4. QUANTUM NETWORKING AND THE QUANTUM INTERNET

4.1 Distributing quantum information via a quantum internet

As quantum technologies develop, it can be expected that the capability will move beyond individual, specialised quantum devices to a networked structure. Small- and intermediate-scale quantum processors can be linked together through quantum communication networks to upscale their capabilities. Quantum sensor networks including quantum clocks can operate across space and time on national and global scales to provide vastly more data than individual components alone. And such a network can be used to provide secure communication links between many parties, both trusted and adversarial, beyond simple two-party links. That network will include quantum communication channels on land and through space (satellite) links, supported with existing conventional (non-quantum) communication channels. This vision of a large-scale interconnected quantum network is commonly referred to as the 'quantum internet'.

Several large-scale coordinated efforts to develop quantum networks have recently appeared internationally, most notably in the US, Europe and China. The primary focus of many of those activities is on the scientific applications of quantum networks, and the defence and intelligence research communities play a key role. Much as with the development of conventional networks, while ultimately the largest users may be civilian, it is in defence applications that the quantum internet may find its earliest drivers.

In the US, the Department of Energy has taken on a coordinating role in developing a strategy for the quantum internet through the Office for Advanced Scientific Computing Research. It is a large-scale program, also involving the National Science Foundation, the Department of Defense, the National Institute for Standards and Technology, the National Security Agency and NASA, along with national laboratories, academic institutions and industry. The Department of Energy blueprint identifies a number of priority research directions that will support quantum networks for sensor networks, upscaled quantum computing and secure communication. Current investment is at US$625 million over the 2020–2025 period in five national quantum research centres. A long-term ambition for the program is to connect all 17 Department of Energy national laboratories as the backbone of a US-based quantum internet.

In Europe, the Quantum Internet Alliance aims to develop a blueprint for a quantum internet. It is supported by the European Union's Horizon 2020 research and innovation program, and its primary focus is on the development of scientific and economic applications.

China has perhaps the most ambitious and advanced national effort in quantum networks. Its early activity in this area extends back to 2006. A series of trusted nodes links Beijing and Shanghai in a QKD network. In 2017, a major national R&D investment in quantum technology was initiated, focused on quantum networks and including quantum computing and secure quantum communication. The National Quantum Laboratory was established in Hefei, funded at US$11 billion. China has identified quantum technologies as an area in which it intends to be the global leader.

4.2 Entanglement distribution for quantum networks

Protocols for the generation and distribution of strong entanglement are crucial for security applications (and other useful protocols, such as teleportation), but current protocols remain inefficient, slow and strictly limited in distance. Two approaches are currently under intense development to mitigate those problems: space-based distribution[38] and quantum repeaters.[39]

4.3 Space-based distribution of entanglement

The space industry is experiencing a renaissance in activity and growth due to the commodification of launch and satellite bus at significantly lower costs. The global space economy has also expanded through the augmentation of services and investment in the sector. In the past three decades, the number of satellites in space has been increasing exponentially. That growth is projected to be in the multitrillion dollar range over the next decades. In addition to the economic importance of the sector, developments in space technology are improving space and near-Earth situational awareness, enabling key terrestrial environment-monitoring services with wide coverage, exquisite precision and augmented capabilities. Underpinning all this growth is the necessity of reliable ground–satellite and intersatellite communications (satcom).

Current satcom relies mainly on radio or microwave channels. At those ‘non-optical’ frequencies, satcom has the following deficiencies:

- It has limited communication bandwidth due to the radio and microwave spectrum allocation available. Many nations have almost completely pre-allocated their communication spectrums.
- It has no directionality and is reliant on broadcasting across a wide extent of space. Interception and eavesdropping of satcom has to be assumed, so strong encryption of information is critical for many applications.

In contrast, laser communications offer many orders of magnitude more bandwidth and allow the focused transmission of information. Currently, many nations are upgrading their satcom to include laser links. Activities range from Norway’s world-first commercial optical ground stations[40] to Amazon Web Services’ Ground Station service.[41]

Laser satcom is highly quantum compatible due to the negligible transmission losses at high altitude and the directionality of laser beams. When supplemented by existing radio/microwave communication links, laser satcom can enable 24/7 quantum encryption of communication channels with adequate built-in redundancy and quantum key buffering.

Examples of advanced quantum satcom programs are the Chinese Micius satellite and Max Planck Institute / German Aerospace Center missions. (International programs on quantum communications and their status are tabulated in the appendix to this report).

In order to convert point-to-point satcom links into a quantum space network, entanglement distribution and quantum memory are required. Distribution of entanglement in space can extend quantum encryption between individual trusted satellites to a network of untrusted satellites. This is analogous to the distribution of entanglement in a terrestrial quantum repeater network described in the following section.

Beyond facilitating a quantum communication network via space repeaters, entanglement distribution also has the following scientific applications of potential relevance to Defence:

- *Distribution of clocks to achieve precision timing beyond the quantum limit.* This can potentially improve GPS and navigational precision.

- *Coherence and quantum entanglement between satellites for extended quantum sensing.* Currently, NASA is pursuing coherent optical links between its Gravity Recovery and Climate Experiment (GRACE) satellites. Future coherent optical links will increase the precision of measuring gravity (g). This has applications in determining underground and subsea structures and compositions.
- *Distributed coherent imaging between satellites to improve imaging resolution.* The James Webb Space Telescope will be the largest telescope in space, with a combined 6.5-metre diameter mirror. To extend that further, smaller satellites can be optically linked together to achieve a significantly larger effective mirror diameter. This ‘sparse-aperture’ imaging technique is already adopted in hand-held phones and cameras.
- *Test of quantum-gravity.* A number of missions have been proposed in the European Union and Canada to use distributed entanglement on satellites to test new models of quantum-gravity. One such experiment was reported by the Micius satellite team in 2019.

4.4 Quantum repeaters

Energy loss in transmission attenuates signals, whether classical or quantum, and inevitably limits the extent of quantum networks. In standard telecommunications, that problem is solved by having repeaters (amplifiers) at various points along the channel to amplify the signal. That solution cannot be employed for quantum communications because amplification tends to destroy the unique features of quantum states, such as entanglement. To overcome this challenge, a model of a quantum repeater has been proposed. The proposed solution is to segment the channel into smaller lengths, with repeater nodes connecting the smaller segments of channel. Specific quantum operations (such as entanglement swapping and entanglement purification) are performed at the nodes, enabling long-distance distribution of entanglement with an efficiency and/or quality surpassing that of direct transmission. An efficient, fast, global quantum internet will not be possible without the perfection of quantum repeater technologies.

The quantum repeater concept was first introduced in 1998,[42] and there have been significant theoretical and technological advances on repeater protocols and elements over the years. However, no complete, functional quantum repeater has so far been demonstrated. Repeater proposals can be placed into two classes: those based on establishing good entanglement at the intermediate nodes, which can then be used to teleport quantum states through the channel; and those based on performing error correction at the intermediate nodes. The former type is slow (as it requires a lot of back-and-forth classical communication) but can operate with reasonable distances between the nodes. The latter type is fast but requires shorter distances between the intermediate nodes.

We note that a quantum repeater is essentially an example of an intermediate-scale quantum (NISQ) technology, and its complexity has meant that no complete repeater protocol has yet been demonstrated. Nonetheless, many of the key elements of quantum repeaters have been implemented, including entanglement swapping, whereby entanglement between intermediate nodes can be teleported to the end points; entanglement purification, whereby many copies of corrupted entanglement can be combined to create fewer copies of high-quality entanglement; and quantum memory, whereby quantum states can be held without corruption while other operations and communications are performed.

4.5 Australian perspective

While plans were made to establish a demonstration quantum network in Canberra, the project did not proceed beyond initial point-to-point tests on the fibre infrastructure between UNSW at the Australian Defence Force Academy and the Australian National University (ANU). Emphasis has shifted to developing free-space quantum communication links, both terrestrially and with satellites.

Australian research on quantum repeaters is world class and has produced several of the best demonstrations of quantum memory[43] and entanglement purification techniques.[44] Australian groups are also active in the development of new repeater protocols. Key research efforts in this field are in the US, China, Europe and the UK.

Australia has a long tradition of collaborations with international groups aiming to establish space-based quantum experiments both for the investigation of fundamental science and for the establishment of quantum communication links such as Space QUEST.[45]

Current state-of-the-art quantum memory technology is looking very promising for extending the reach of satellite-based quantum communication. Both a quantum information recall efficiency of close to 90% and a six-hour-long memory have been demonstrated by the ANU. The hours-long memory, when mounted on low Earth orbit (LEO) satellites, will allow the global distribution of entanglement (LEO orbit has a period of 90–130 minutes).

An Australasian consortium including the ANU, the University of Western Australia (UWA), DST Group, the University of Auckland and CSIRO is leading the development of a proposal for an integrated optical satellite telecommunications research network to enable next-generation quantum secure satellite communication for Australia’s nation-critical capabilities. The proposal is to connect four optical ground stations in Western Australia, South Australia, the ACT and New Zealand. Two of the proposed sites are on university grounds (UWA and ANU), while the South Australian site is with DST Edinburgh. The New Zealand site is yet to be determined. The four sites are spread across a large area to provide site diversity and mitigate the impact of cloud cover and weather, for which advanced adaptive optics also plays a role.

It is clear that Australia has strong expertise and unique opportunities for development and engagement with the coming quantum internet, but that capacity is presently uncoordinated, and engagement is not at a national level.

5. POST-QUANTUM CRYPTOGRAPHY: A SECURITY PATCH FOR THE INTERNET

5.1 What it is: a replacement for RSA and other public-key cryptosystems

The realisation of a large-scale quantum computer would place many of the most widely used public-key cryptosystems at risk. RSA and other public-key cryptosystems are based on the presumed difficulty of certain mathematical problems, such as factoring integers into prime numbers, and quantum algorithms such as Shor's algorithm have been shown to efficiently break those cryptosystems. As a consequence, quantum computers would make the most widely used security on the internet insecure, enabling not only the decryption of present and future communications but also much of the stored encrypted information of past decades.

Post-quantum cryptography aims to develop new public-key cryptosystems that are resistant to attack by both conventional and quantum computers. Critically, post-quantum cryptosystems are intended to run on existing, conventional computers and networks—they are not themselves 'quantum'. Rather, they are public-key cryptosystems based on the presumed difficulty of certain mathematical problems even subject to quantum attack.

Developing post-quantum cryptosystems is a difficult challenge. Not only must they be resistant to conventional attack (no small feat in itself), but they must be designed to be resistant to quantum attack even though the full capabilities of a quantum computer are not yet known. Most approaches to post-quantum cryptography rely on the efforts of theoretical quantum computer scientists to identify mathematical problems that appear resistant to all possible quantum solutions.

The US NIST is in the final stages of a multi-year project to develop standards for post-quantum cryptography. As is common practice for all cryptographic standards, the NIST's PQC Program involves an open process for proposing candidates together with a rigorous, open, multi-round evaluation process to down-select preferred candidates. Given the prominence of both NIST and this program within the international cryptography community, it can reasonably be expected that the final selections from the PQC program will gain widespread acceptance globally.

5.2 The challenge of developing new cryptosystems

For decades now, the relative stability of public-key cryptography has enabled fast and secure internet communications. While the NIST-led PQC program is addressing the problem of identifying robust quantum-safe cryptographic protocols, that is only the first step towards securing the internet against quantum attacks. Once the NIST project is complete, a global effort to integrate new standards throughout the internet's infrastructure will be required. That is likely to require additional computational and communication costs beyond those of the current standards, potentially straining existing infrastructure.[46] At this point, we do not know the full extent of the impact of those changes.

Adding to the complexity of migration to PQC will be the desire to ensure that new infrastructure can be developed in a cryptographically agile way, so as to guard against potential future security risks. Current PQC standards are developed to be secure to the best knowledge available, but new breakthroughs in mathematics, or computer science, could threaten their security—just as Shor's algorithm has overthrown the security of RSA. Therefore, new infrastructure should ideally allow for interchangeable security standards to allow for security to be enhanced as new attacks are discovered.

The ongoing security and quality of internet-based communications will rely on productive collaboration across academia, industry and the Defence organisation.

5.3 Advantages and limitations of the approach

Utilising PQC to ensure ongoing network security remains the foremost option for ongoing internet security. That is the clear, publicly stated position of the US National Security Agency. Driving this recommendation is the potential for attacks on other alternatives, such as QKD, due to the relative immaturity of the technology. To maintain current levels of security and performance in networking and communications, PQC is likely to require enhanced computing and networking infrastructure due to the expected reduction in software efficiency. It is also expected that PQC will require significant software-level changes to existing communications applications. However, the NIST program is designed to minimise such challenges. Therefore, PQC is likely to require the upgrading of existing infrastructure, as opposed to the large-scale deployment of entirely new networking technologies.

Quantum computing remains the major limitation to the PQC approach to network security. While the NIST program has identified several potential replacements for RSA and elliptic-curve-based public-key schemes, we do not have a large amount of evidence that quantum computers cannot attack the specific implementations that are still under consideration. This remains a significant problem.

The threat of 'record now, exploit later' attacks against current communication standards poses a clear threat to sensitive communications. Unfortunately, the extreme variability in the predicted time frame for the construction of cryptographic-attack-capable quantum computers will affect the time frame for the testing and deployment of PQC. That problem is heightened due to the relatively small community of researchers capable of fully assessing this threat. The assessment of PQC schemes requires deep technical expertise in not only classical cryptography, but also quantum algorithms, complexity theory and architecture development. That overlap of expertise is extremely rare, heightening the risk.

5.4 Australian perspective

Australia has a small but influential community of academic researchers working specifically on PQC. Academic centres focused on cybersecurity have developed some expertise in this area, and Australian researchers are pursuing the development of new PQC schemes. Pleasingly, Australian Government agencies have given extensive support to the development of cybersecurity research, especially with regard to agility.

Likewise, Australia has an exceptional history of world-class research in quantum algorithms, complexity theory and architecture development. In Sydney alone, the concentration of expertise in this area rivals that of any of the major centres worldwide. However, as in the rest of the world, the interaction between the theoretical quantum computing community and the cybersecurity community remains limited, and there is little incentive to change the *status quo*. This remains a limitation: we must develop talent that is capable of fully assessing the threat that quantum computers pose to PQC, as this will remain an ongoing risk to secure communications.

6. RECOMMENDATIONS FOR THE AUSTRALIAN CONTEXT

Recommendation 1: Formalise and prioritise Australia–US quantum cooperation

A bilateral program with a mission focus, coordinated by the Defence Department and including the intelligence community

Given the central and accelerating importance of quantum technologies to our Defence organisation and those of our allies, and to national security and economic prosperity, it is urgent that consideration be given to prioritising a coordinated bilateral approach with the US, led by the Defence Department and intelligence community, including an appropriate Australian funding allocation for mission-critical projects, via a formal statement of cooperation under the broad Australia–US science and technology (S&T) agreement. Such cooperation could be initiated through the 2021 AUSMIN dialogue.

Mapping this recommendation to effective Defence project management would optimally benefit from an Australian DARPA model, as proposed and set out in a separate ASPI publication.[47]

More broadly, the Australian quantum technology community has numerous links to other nations in both the Five-Eyes and the Quadrilateral Security Dialogue frameworks, as well as with key European partners, particularly in quantum communications, for which increased coordination and prioritisation by the Defence Department is also important.

Background and context

Australia and the US have had a longstanding bilateral S&T relationship dating back to 1968. The most recent treaty-level formalisation of this relationship is the Agreement Relating to Scientific and Technical Cooperation between the Government of the United States of America and the Government of Australia signed in Washington in November 2016, which entered into force in December 2017. Under that framework, a US–Australia joint commission meeting on S&T is held every two years.

Within that framework, Prime Minister Morrison announced during his 2019 meetings in Washington a $150 million investment in local Australian businesses, researchers and new technologies to support NASA's mission to return to the Moon and travel to Mars, expanding Australia–US cooperation in space and boosting the Australian space industry and workforce. The Prime Minister has also announced a number of other S&T initiatives that boost cooperation between Australia and the US, including a critical minerals action plan that increases trade in rare earths to support our high-technology future; work on reducing marine plastic debris and improving waste management; opportunities for Australian scientists to provide advice on lithium-ion recycling and hydrogen safety; and cooperation between Australian researchers and the US National Science Foundation on projects of mutual and strategic interest.

While the US made a formal statement on quantum cooperation with Japan in December 2019, Australia–US cooperation on quantum technologies has not been holistically prioritised, coordinated or formalised under the umbrella S&T agreement and largely remains in the academic research domain in the form of US funding of specific Australian projects, specific collaborations between Australian and US researchers and specific researcher–industry arrangements. The totality of this joint activity falls short of what could potentially be achieved through a strategic bilateral plan.

Whereas the US defence and intelligence communities have actively led and coordinated the US quantum technology field for some two decades or more, in Australia the Australian Research Council has been central to sustained support for the field. The Defence Department and government agencies largely maintain a watching brief, apart from their own activities, which in recent years have included some significant investments in specific areas, particularly silicon quantum computing. Quantum technology is cited only minimally in the 2020 Defence Strategic Update, but there is urgency that it is backed by detailed Defence strategic planning and policy.

Recommendation 2: Develop a sovereign capability in intermediate-scale quantum computing

A critical asset to keep pace with escalating advances in quantum technologies that affect defence capability

Within the framework of the partnership approach set out in Recommendation 1, we believe it is imperative and urgent that the Defence Department initiates a comprehensive program, across the span of hardware and software technologies, that harnesses the full strength of the nation's quantum technology community to attain programmable intermediate-scale quantum computer (NISQ) capability. The sovereign NISQ program should be at a scale to demonstrate a quantum advantage, have ongoing scalability and be adaptable for critical defence applications. The charters of the Defence-focused Next Generation Technologies Fund and Defence Innovation Hub are aligned to this recommendation.

By leveraging international state-of-the-art and existing national infrastructure, expertise and technology, sufficiently focused and resourced efforts could produce powerful and versatile devices within a time frame of five years. Such a targeted program would assess competitive options, including optical- and semiconductor-based quantum technologies, and various implementation approaches.

Background and context

Currently, only the US and China have demonstrated the capability to integrate large numbers of components into a rudimentary quantum processor that can outperform a conventional supercomputer at a specific computational task. In 2019, Google demonstrated such a quantum advantage using its Sycamore processor, based on superconducting technology. Subsequently, US-based programs in both superconducting and trapped-ion-based quantum technologies have demonstrated comparable capabilities. In 2020, researchers at the USTC in China published a demonstration of a limited, but still highly impressive, optical quantum processor that also demonstrates such a quantum advantage—the first demonstration by a group outside of the US. In February 2021, the USTC has also published its development of a NISQ processor based on superconducting technology and has demonstrated a quantum walk capability, which is integral to search functionality, on that platform.

From a defence and national security perspective, several considerations underscore the need for a sovereign capability in NISQ technology:

- Access to NISQ devices will allow for algorithm development and the testing of cybersecurity applications. The co-development of NISQ hardware and algorithms by sovereign teams, including partnerships with services provided by allied countries, will enable more rapid advances and mitigate concerns about continuity and security associated with dependency on cloud access to foreign hardware services.
- NISQ devices promise early applications of quantum computing advantage and are stepping stones to full-scale quantum computing, with manifold defence applications.
- NISQ technology is an enabling technology for advanced quantum communications applications, such as the development of quantum repeaters and sophisticated, error-corrected quantum sensors. In particular, optical NISQ technology is directly compatible with distributed quantum computing applications.
- NISQ technology can form the basis of a domestic quantum industry and research community that can attract and retain talent and expertise in Australia.

We assess that a targeted program by the Defence Department to develop a sovereign capability in this area could be achievable within three to five years. Australia's quantum research community, spanning universities, government and industry, has world-class expertise in quantum technologies at the component level, including a number of research efforts that are near the cusp of developing integrated, intermediate-scale quantum devices. Leadership by the Defence Department would coordinate and focus those efforts and keep essential capabilities within Australia.

Recommendation 3: Build an international presence in quantum communications

Establish critical national infrastructure and formal involvement in international space-based network programs

Capitalising on the deep and broad span of the nation's capabilities in quantum communications, Australia should build and formalise its international presence by participating in the Global Quantum Communication Network through substantive involvement in international space-based quantum network programs with key strategic partners.

More specifically, we recommend that Defence take a lead coordination role in establishing the key backbone infrastructure of a national optical ground station network for laser and quantum-capable satellite communications. In alignment with the Australian Space Agency's *Communications technologies and services roadmap 2021–2030*, the ground stations should be accessible to government organisations and industry, with built-in future-proofed compatibility with quantum memory, repeater and encryption capabilities. The network will establish a formative Australian capability in key quantum technologies with important defence applications and that are foreshadowed to underpin a global quantum internet.

In addition, we recommend the establishment of a national quantum communication expert group led by the Defence Department, and in liaison with CSIRO, that consolidates expertise around the country and across sectors (defence, government, industry and academia) to coordinate a national quantum communication strategy and vision. This would include the establishment of an appropriately resourced international presence by selective involvement in Global Quantum Communication Network programs such as the European Union's ETSI to establish quantum communication accreditations and standards; and multinational quantum networks such as those led by NASA, UK (RAL Space), Germany (German Aerospace Center, DLR) and Japan.

Background and context

Australia's future is dependent on reliable, fast and high-volume communication infrastructure to keep up with the increasing demands of Defence, communities, businesses and the rural sector, especially during natural disasters and health crises. Laser communication will complement radio and microwave satellite communications in providing global low-latency coverage and will play an increasingly important role due to its higher bandwidth. Laser communication has advantages in that it can support point-to-point communications and will not strain an already oversaturated radio spectrum. Laser's point-to-point specificity also offers increased security and, notwithstanding current limitations of quantum encryption schemes such as QKD, is compatible with quantum communication more generally, including the distribution of quantum information enabled by quantum memory and repeater devices, for distributed quantum computing and long baseline quantum sensing—and more broadly towards the future development of a quantum internet.

Australasia occupies a geographically unique position. Very low cloud cover makes the region an ideal location for optical ground stations to provide high-data-rate transmissions and real-time communications and enable the transmission of large volumes of data. In addition, Australia is the only country in the Southern Hemisphere (to date) with quantum capabilities, placing us in a unique position to implement a fully integrated network including advanced space-to-ground quantum communications.

An Australasian optical ground station network would interact with a number of space agencies (NASA, the Australian Space Agency, the European Space Agency, the New Zealand Space Agency, the German Aerospace Center and the Japan Aerospace Exploration Agency) and attract potential industry end users such as Airbus, Northrop Grumman, Boeing, Thales, the Swedish Space Corporation, Goonhilly, Capricorn, Transcelestial, Astrogate Labs and Arqit UK.

Recommendation 4: Establish a mathematical and theoretical sciences research institute

A bridge between the defence and security establishments and the academic community to research future threats to communication networks

We believe that there are significant opportunities to lift Australia's capacity to evaluate future threats to secure communications that emerge because of progress in the mathematical and theoretical sciences, in particular those posed by quantum computing, by a more formal collaboration between Defence and the academic research community. We recommend the establishment of a mathematical and theoretical science institute that will act as a bridge between the academic and defence communities. Its mission would be to use the significant strength of those communities working together to identify not only vulnerabilities to network security but also other emerging defence threats. Such an effort will both act as a nexus for such research and foster a talent pipeline to alleviate future threats in this space.

Background and context

The threat to key internet security protocols posed by the rapid development of quantum computers has spawned a worldwide re-evaluation of the underlying foundations of network security. The potential for 'record now, exploit later' attacks threatens sensitive communications now, despite the expected timelines for quantum computer development. In recognition of that threat, the US's NIST is conducting an international process to evaluate and standardise post-quantum cryptography schemes to replace the protocols under the most threat from quantum computers.

The security of modern networked communications schemes depends on the presumed difficulty of solving certain mathematical problems. Security has been established through years of research into the mathematical properties of those problems and thorough and open testing of the corresponding security protocols. The assessment of PQC schemes carries significant risk due to the worldwide scale of the deployment, rapid development timeline and breadth of expertise required to assess potential attacks. This requires input from an extremely broad set of experts in not only cybersecurity but also mathematics, computer science, quantum computing and other mathematically based disciplines. This is challenging, because the population of scientists and engineers with backgrounds in a cross-section of those disciplines is extremely small due to their highly specialised nature. NIST's approach has been to perform that evaluation as an open collaboration between the academic and security communities to develop trust in the eventual PQC standards. NIST has been well placed to lead the evaluation because of its capacity to draw on its own broad expertise, but also to act as an essential link between US defence and security agencies and the broader academic community.

In the UK, the risk posed by the continual advancement of mathematics is in part mitigated through the Heilbronn Institute for Mathematical Research, which is a collaboration between the UK Government Communications Headquarters and the academic community. The institute acts as a link between the Ministry of Defence and academia to harness the breadth of expertise available in the academic community.

In Australia, there is an opportunity to further leverage the capabilities that exist in the academic community for the evaluation of potential threats that emerge because of progress in the mathematical and theoretical sciences. While there are existing collaborations between Australian academics and Defence, Australia does not have an organisation comparable to either NIST or the Heilbronn Institute that is capable of acting as a bridge between the significant expertise that exists in Defence and academia. We believe it would be advantageous to establish such an organisation to focus research efforts on potential threats to network security, but also other emerging defence threats that are the result of progress in the mathematical and theoretical sciences.

Recommendation 5: Partnering towards Australian quantum technologies

Optimal industry suppliers for Defence from both Australia's and partner nations' quantum industry sectors

We recommend that the Defence Department's approach to prototype development and industry engagement in quantum technologies be conducted within a framework of cooperation with our allies and partner nations, in relation both to major corporates and start-up companies and to national laboratory facilities.

Background and context

The development of quantum technologies has the potential to reshape the existing technology industry landscape. This opportunity is driving sovereign and commercial investment to secure key intellectual property, supply chains and markets.

Over the past 20 years, Australia has developed significant concentrations of talent in quantum technologies through the competitive grants program, targeted federal and state government research support, US defence funding, university funding and, most recently, commercial investment. Much of that capability is in the university sector, where strong talent pipelines and leading academic research are found in locations across the country. In some cases, the talent concentration rivals that seen in other quantum technology destinations, such as the American strongholds in the San Francisco Bay area, greater Los Angeles, Chicago, Maryland and Boston, or the significant efforts underway in Europe and the UK in Delft, Oxford and Paris. Those geographical concentrations are the key for academic, industrial and start-up endeavours to interlink and share talent and resources. A nascent but nonetheless thriving quantum technology ecosystem is emerging in Australia and has produced a number of notable success stories. Most notable among them are a major initiative to develop a quantum processor based on phosphorus-doped silicon at Silicon Quantum Computing; the partnership between Microsoft and the University of Sydney on cryogenic digital control systems for quantum processors; the commercialisation of quantum encryption techniques by QuintessenceLabs; Q-CTRL; and Quantum Brilliance. Through partnerships with Defence, Australian quantum computing and communications research strengths can act as a catalyst for local industry growth or enhance opportunities for international partners. Beyond that, Australia has a large capacity to provide supply-chain capability across the quantum technology sector.

We emphasise that the strength and diversity of Australian quantum industries should not preclude partnerships with our allies and partner nations. In fact, it is a significant advantage to the Defence mission that many of Australia's key allies, including the US, Canada, the UK, Japan and European nations, have heavily invested in quantum technologies. Already, the Australian research community is making key contributions to both national and commercial activities in quantum technologies with those partner nations, and that should be both encouraged and leveraged.

APPENDIX: QUANTUM SATELLITE COMMUNICATIONS—INTERNATIONAL STATUS

Leading country / organisation	Participants	Satellite and orbit	Mission objectives	Status	Ref
USA / NASA Mission name: National Space Quantum Laboratory	NASA–MIT–LL Lasercom Collaboration, International Space Station (ISS)	LEO	Planned mission for generating entangled pairs of photons on ISS payload. Applications include quantum clock synchronisation, quantum sensing and distributed quantum computing.	Proposal	A1
Germany / German Aerospace Center (DLR) Mission name: QUOLLSat	Australian National University (ANU), Defence Science and Technology (DST) Group	LEO small satellite (300 kg)	20 cm diameter onboard telescope with high-speed adaptive optics communication link. Quantum light source on board to study quantum information decoherence in space.	Proposal	A2
China Mission name: QUESS	University of Science and Technology China, Hefei (UTSC), Chinese Academy of Sciences, Austrian Academy of Sciences	LEO medium-sized satellite (Micius 600 kg)	Demonstrated secure quantum links with single photons up to 7,600 km ground to ground, and entangled photons up to 1,120 km.	Launched in 2016 Achieved milestones since 2017	A3 A4 A5 A6
Italy	Universita degli Studi di Padova, e-GEOS, Agenzia Spaziale Italiana	LEO small satellites (Jason 2 510 kg, Larets 21 kg, Starlette/ Stella 48 kg)	Transmission of polarisation states for QKD between satellite and ground up to 2,000 km.	Achieved in 2014	A7
Germany	Max Planck Institute for the Science of Light, Institute of Optics, FAU, Tesat- Spacecomm, DLR	GEO large satellite (Alphasat I- XL 6,649 kg)	Quantum-limited coherent measurements of optical signals sent from geostationary satellite to ground up to 38,600 km.	Achieved in 2017	A8
China	UTSC, Chinese Academy of Sciences	LEO small satellite (CHAMP 500 kg)	Pre-QKD satellite-to-ground transmission of photons from quasi-single-photon source (up to 400 km).	Achieved in 2013	A9
Italy	Universita degli Studi di Padova, CNR, e-GEOS, Agenzia Spaziale Italiana	MEO small satellite (LAGEO-2 411 kg)	Single-photon exchange between satellite and ground up to 7,000 km.	Achieved in 2016	A10
Japan	National Institute of Information and Communications Technology (NICT), Japan Aerospace Exploration Agency	LEO medium-sized satellites (OICETS 570 kg)	Two ground stations used: one did standard radio communication while the other performed laser communications to measure the polarisation of the laser beam from the satellite to characterise the QKD link for future satellite missions (up to 650 km).	Achieved in 2009	A11

Leading country / organisation	Participants	Satellite and orbit	Mission objectives	Status	Ref
Japan	NICT	LEO micro-satellite (Socrates 48 kg)	Non-orthogonal linearly polarised states with pseudo-random binary sequences were transmitted (up to 650 km) at a 10 MHz repetition rate from the SOTA (small optical transponder) terminal aboard Socrates. On the ground, the polarised quantum states were received by the quantum receiver.	Achieved in 2017	A12
Singapore / National University of Singapore	University of Strathclyde (UK)	LEO 2U cubesat (Galassia—1.65 kg)	Generation of entangled-photon pairs and polarisation correlation measurements in orbit on the satellite up to 550 km.	Achieved in 2015	A13
France / Centre Spatial, Université de Grenoble Mission name: Nanobob	Université de Nice Sophia Antipolis, Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, University of Bristol	Sun-synchronised orbit (SSO) 12U cubesat	The entangled photon source, Alice, will be placed on the ground station and the detection system, Bob, on the satellite. In total, there will be two ground stations (ESA, OGS and MeO). The satellite will measure and time-tag the single photon polarisation states and communicate with the other ground station via an authenticated public communication channel.	Proposal	A14
ESA Mission name: Space QUEST	International Space Station (ISS)	LEO	Placing a module at the ISS that is capable of receiving single photons signals, removing background noise and time-tagging the arriving signals. Several ground stations will be used with the distance of communications being 400 km.	Proposal	A15
Austria and European Space Agency (ESA)	ISS	LEO	Performing quantum optics experiments up to 400 km where the transmitter is the optical ground station (OGS) and ISS is the receiver.	Proposal	A16
USA / University of Illinois	ISS	LEO	Carry out the super-dense teleportation experiment between ISS and OGS among three parties with a communication distance of up to 400 km.	Proposal	A17
Italy / University of Padova	Istituto Nazionale di Fisica Nucleare, Italian Space Agency Matera Laser Ranging Observatory (MLRO), e-GEOS SpA, International Laser Ranging Service, Center of Studies and Activities for Space	MEO large satellite (GLONASS 1,480 kg)	Exchange of single photons from GLONASS satellites using mounted retroreflector array detected by the MLRO telescope on the ground station with a distance of 20,000 km.	Achieved in 2019	A18
UK / University of Strathclyde Mission name: QUARC	University of Bristol	LEO 6U cubesat (12 kg)	To form a constellation of 6U-sized cubesats to demonstrate QKD over a channel of 400 km.	Proposal	A19

Leading country / organisation	Participants	Satellite and orbit	Mission objectives	Status	Ref
Singapore / Centre for Quantum Technologies Mission name: SpooQy-1	UK Space Agency	LEO 3U cubesat	Cubesat had a miniaturised polarisation entangled photon-pair source and the mission demonstrated Bell tests.	Launched, performed Bell type tests in 2019. Plans to demonstrate QKD by 2022	A20
Canada Mission name: NanoQEY	Institute for Quantum Computing, Space Flight Laboratory	LEO nanosatellite (NEMO 16 kg)	Satellite to be used as a trusted node that generates keys between two ground stations to demonstrate QKD experiments over a distance of 400–600 km.	Proposal	A21
UK and Italy / University of Strathclyde, University of Padova, Craft Prospect, Deimos Space Mission name: CQuCom	ISS	LEO 6U cubesat	The satellite will have a quantum source to generate single photons. The aim is to characterise the pointing performance, free-space channel, QKD as well as to distribute entanglement between space and ground station.	Proposal	A22
Canada / Canadian Space Agency Mission name: QEYSSat	Institute for Quantum Computing, and Honeywell	LEO	The satellite will have a primary payload to demonstrate QKD protocols with one or two ground stations, while the secondary payload will be used for classical communications and characterisation of optical links over 400 km.	To be launched in 2022	A23 A24 A25
UK / Arqit Mission name: QKDSat	BT, Fraunhofer UK, Toshiba Research labs, NU Quantum, ESA	LEO cubesat	Satellite to perform discrete variable based QKD experiments over 400–600 km link.	Contract signed between UK and ESA in 2018	A26 A27
ESA Mission name: QUARTZ	Austrian Institute of Technology GmbH, DLR, ID Quantique, itrust consulting, Ludwig-Maximilians-University, LuxTrust, Max Planck Institute for the Science of Light, Palacky University, Tesat-Spacecom, Netherlands Organisation for Applied Scientific Research	To be determined	To be determined.	Early stages	A28
UK–Singapore	RAL Space (UK) and Centre for Quantum Technologies (Singapore)	6U cubesat	Satellite to demonstrate QKD-based protocol.	To be launched in 2021	A29
Germany Mission name: QUBE	Center for Telematics, Ludwig Maximilian University, Max Planck Institute for the Science of Light, DLR	LEO 3U cubesat	A miniaturised QRNG source will be used to generate random bits and encoded on the polarisation states which will be sent to the OGS at DLR for detection. The experiment aims to establish a quantum link between the satellite and OGS as well as testing the performance of the QRNG source.	Early stages	A30

Leading country / organisation	Participants	Satellite and orbit	Mission objectives	Status	Ref
UK / Craft Prospect Mission Name: The Responsive Operations Key Services in Orbit Demonstration	Craft Prospect only	LEO 6U cubesat	The satellite will be a trusted node and discrete variable based QKD will be used for downlink.	Early stages	A31
ESA Mission name: Security and CryptoGrAphic Mission	ESA only	LEO/MEO/ GEO	Mission to demonstrate QKD experiments.	Under phase study, open to tender	A32 A33

References:

A1 Scott A Hamilton et al., ‘Overview of NASA’s National Space Quantum Laboratory Program’, presentation to 70th International Astronautical Congress, 2019, online.

A2 DLR–ANU Concurrent Design Engineering Session, Bremen (2017).

A3 Juan Yin et al., ‘Entanglement-based secure quantum cryptography over 1,120 kilometres, *Nature*, 2020, 582:501–505.

A4 Sheng-Kai Liao et al., ‘Satellite-relayed intercontinental quantum network’ *Physical Review Letters*, 19 January 2018, 120:030501.

A5 Sheng-Kai Liao et al., ‘Satellite-to-ground quantum key distribution’, *Nature*, 2017, 549:43.

A6 Ji-Gang Ren et al., ‘Ground-to-satellite quantum teleportation, *Nature*, 2017, 549:70.

A7 C Bonato et al., ‘Feasibility of satellite quantum key distribution’, *New Journal of Physics*, 2009, 11:045017.

A8 K Günthner et al., ‘Quantum-limited measurements of optical signals from a geostationary satellite’, *Optica*, 2017, 4:611.

A9 J Yin et al., ‘Experimental quasi-single-photon transmission from satellite to earth’, *Optics Express*, 2013, 21:20032.

A10 D Dequal at al., ‘Experimental single-photon exchange along a space link of 7000 km’, *Physical Review A*, 2016, 93:010301(R).

A11 M Toyoshima et al., ‘Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space’, *Optics Express*, 2009, 17:22333.

A12 H Takenaka et al., ‘Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite’, *Nature Photonics*, 2017, 11:502.

A13 Z Tang et al., ‘Generation and analysis of correlated pairs of photons aboard a nanosatellite’, *Physical Review Applied*, 2016. 5:054022.

A14 E Kerstel et al.,’Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration’, *EPJ Quantum Technology*, 2018, 5:6.

A15 SK Joshi et al., ‘Space QUEST mission proposal: experimentally testing decoherence due to gravity’, *New Journal of Physics*, 2019, 20:063016.

A16 T Scheidl et al., Quantum optics experiments using the international space station: a proposal’, *New Journal of Physics*, 2013, 15:043008.

A17 C Zeitler et al., ‘Super-dense teleportation for space applications’, *SPIE Proceedings*, 2016, 9739:973912.

A18 L Calderaro et al., ‘Towards quantum communication from global navigation satellite system’, *Quantum Science and Technology*, 2019, 4:015012.

A19 L Mazzarella et al., ‘QUARC: Quantum Research Cubesat—a constellation for quantum communication’, *Cryptography*, 2020, 4:7.

A20 A Villar et al., ‘Entanglement demonstration on board a nano-satellite, *Optica*, 2020, 7:734.

A21 T Jennewein et al., ‘The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite’, *SPIE Proceedings*, 2014, 9254:925402.

A22 DK Oi et al., ‘Cubesat quantum communications mission’, *EPJ Quantum Technology*, 2017, 4:6.

A23 H Podmore et al., ‘Optical terminal for Canada’s Quantum Encryption and Science Satellite (QEYSSat), IEEE International Conference on Space Optical Systems and Applications, Portland, 2019, 1.

A24 T Jennewein, ‘Towards quantum communications with satellites’, IEEE Photonics Society Summer Topical Meeting Series (SUM), Waikoloa Village, Hawaii, 2018, 217.

A25 A Scott et al., ‘The QEYSSAT mission: on-orbit demonstration of secure optical communications network technologies’, *SPIE Proceedings*, 2020, 11532H.

A26 ‘BT and Toshiba install UK’s first quantum-secure industrial network between key UK smart production facilities’, news release, 1 October 2020, online.

A27 ‘D/TIA partners with UK-based ArQit to develop first quantum encryption satellite’, news release, European Space Agency, 13 November 2018, online.

A28 ‘10 new business and research partners join Quartz’, news release, European Space Agency, 4 July 2018, online.

A29 ‘UK and Singapore collaborate on £10m project to develop next generation communications networks’, news release, Science and Technology Facilities Council, RAL Space, 27 September 2018, online.

A30 R Haber et al., ‘QUBE—a cubesat for quantum key distribution experiments’, 32nd Annual AIAA/USU Conference on Small Satellites SSC18-III-05, 2018.

A31 ‘ROKS: Responsive Operations for Key Services’, Craft Prospect, no date, online.

A32 ‘European quantum communications network takes shape’, European Space Agency, 9 April 2019, online.

A33 ‘SAGA Phase A study’, Romanian Space Agency, 14 July 2020, online.

TERMS OF REFERENCE, SCHEDULE AND BIOGRAPHIES

Terms of reference

From open-source research, produce a written report on the implications of quantum technologies for communications security, that identifies opportunities for Australian research and Australian technology firms to contribute and potentially bring these capabilities to the Australian Defence Force and our alliance partners in a cooperative way.

Scope of the report includes international status, judgements of technology maturity, early applications and capabilities, industry implications, capabilities and status within Australia, and recommendations for the Australian Department of Defence and national security institutions on how to approach these advances.

Schedule

Meeting 1: Tuesday 3 November 2020 10 am – 12 noon (by Zoom)

Meeting 2: Tuesday 17 November 2020 10 am – 12 noon (by Zoom)

Meeting 3: Tuesday 1 December 2020 10 am – 3 pm at ASPI, Canberra

Meeting 4: Tuesday 19 January 2021 10 am – 12 noon (by Zoom)

Meeting 5: Friday 5 February 2021 10 am – 3 pm at Sydney Nanoscience Hub

ASPI / Defence Department progress briefing by Project Chair: Tuesday 9 February 2021 at ASPI, Canberra

Meeting 6: Wednesday 17 February 2021 2 pm – 5 pm at Sydney Nanoscience Hub

Submission of exposure draft to ASPI / Defence Department: Friday 19 February 2021

Receipt of Defence Department feedback on exposure draft: Wednesday 17 March 2021

Meeting 7: Wednesday 24 March 2021 11 am – 12.30 pm (by Zoom)

Submission of final version of report to ASPI / Defence Department: Thursday 25 March 2021

Biographies

Dr Robert Clark AO FAA DistFRSN (Project Chair)

Robert Clark was formerly an officer in the Royal Australian Navy, a lecturer and Fellow of The Queen’s College at the University of Oxford, and Scientia Professor and Chair Professor of Experimental Physics at the University of NSW. As an Australian Government Federation Fellow, he was the founding Director of the ARC Centre of Excellence for Quantum Computer Technology over its first decade. More recently, he was Chief Defence Scientist in the Australian Department of Defence, CEO of the Defence Science and Technology Organisation and a member of Australia’s Defence Committee. In that role, he was the Australian Principal of the Technical Cooperation Program between Australia, the US, the UK, Canada and New Zealand and a member of the Prime Minister’s Science, Engineering and

Innovation Council. He is a Fellow of the Australian Academy of Science and a Distinguished Fellow of the Royal Society of New South Wales and is currently a Senior Fellow at the Australian Strategic Policy Institute. He has been privileged to receive a number of awards and honours, including the Eureka Prize for Leadership in Science, the Australian Centenary Medal, the Australian Defence Medal, the United States of America Secretary of Defence Medal and distinguished awards from US Government agencies and is an Officer in the Order of Australia.

Professor Stephen Bartlett FAPS FRSN

Stephen Bartlett is a theoretical quantum physicist and professor in the School of Physics at the University of Sydney. He leads a team pursuing both fundamental and applied research in quantum information theory, including the theory of quantum computing. He is a Chief Investigator in the ARC Centre of Excellence in Engineered Quantum Systems (EQUS), where he leads a research program on designer quantum materials. He is the inaugural Lead Editor of the American Physical Society journal *PRX Quantum*. In 2020, he was elected as a Fellow of the American Physical Society and of the Royal Society of New South Wales.

Professor Michael Bremner

Michael Bremner is a quantum computer scientist and professor in the Centre for Quantum Software and Information and School of Computer Science at the University of Technology Sydney. Together with his team, he investigates how quantum algorithms can achieve a quantum advantage with near-term quantum computers. He is a Chief Investigator in the ARC Centre of Excellence in Quantum Computation and Communication Technology, where he leads the quantum Architectures and Algorithms work package. Michael was an ARC Future Fellow and is currently co-Editor in Chief of the *Nature* partner journal *Quantum Information*. He has served on the Editorial Board of the IOP journal *Quantum Science and Technology*. He is also a member of the Sydney Quantum Academy Executive Board.

Professor Ping Koy Lam FAA

Ping Koy Lam is an experimental quantum physicist at the ANU. He is currently an Australian Research Council Laureate Fellow, a Fellow of the Australian Academy of Science and the ANU node director for the Centre of Excellence for Quantum Computation and Communication Technology. Apart from his tenure at the ANU, he was an engineer for Sony Electronics and Hewlett-Packard (1990–1992), an Alexander von Humboldt Fellow at the Erlangen-Nürnberg Universität (2000), a CNRS visiting professor at Paris University (2007) and an adjunct professor at Tianjin University (2013–2015). He is currently also a visiting professor at Nanyang Technological University Singapore (from 2020). In 2007, he co-founded QuintessenceLabs—an Australian cybersecurity company productising quantum communication technology. For his contribution to science and industry, he was awarded the ANU Crawford Prize (2000), the AIP Bragg Medal (2000), the British Council Eureka Prize for inspiring science (2003), the UNSW Eureka Prize for scientific research (2006), and the AIP Alan Walsh Medal for significant contributions to industry (2014).

Professor Timothy Ralph FAA

Timothy Ralph is a professor of physics at the University of Queensland. He has extensive experience in quantum optics and has pioneered several key optical implementations of quantum information techniques. He has written more than 350 publications that have attracted more than 15,300 citations and has co-authored a popular textbook on quantum optics, now in its 3rd edition. He has an extensive network of national and international academic collaborators and is a member of the leadership executive and a node director in the Australian Centre of Excellence for Quantum Computation and Communication Technology. Timothy has industry and government collaborations with Xanadu Canada, QuintessenceLabs Australia, the Defence Science and Technology Group and Northrop Grumman USA. He is a Fellow of the Australian Academy of Science, was awarded the AIP Alan Walsh Medal in 2014 and has held three ARC Fellowships.

NOTES

[1] US National Science and Technology Council (US NSTC), *National Strategic Overview for Quantum Information Science*, September 2018, 2, online.

[2] US NSTC, *National Strategic Overview for Quantum Information Science*, 11.

[3] Scott Morrison, 'Address to the National Press Club', 1 February 2021, online.

[4] National Quantum Initiative, *quantum|gov*, online.

[5] National Quantum Coordination Office, *Quantum frontiers: report on community input to the nation's strategy for quantum information science*, The White House, Washington DC, October 2020, online.

[6] 'Agreement relating to scientific and technical cooperation between the Government of the United States of America and the Government of Australia', 29 November 2016, online.

[7] National Academies of Sciences, Engineering, and Medicine, *Quantum computing: progress and prospects*, National Academies Press, Washington DC, 2019.

[8] National Institute of Standards and Technology (NIST), 'NIST's Post Quantum Cryptography Program enters "selection round"', news release, US Department of Commerce, 22 July 2020, online.

[9] Defence Science and Technology Laboratory (DSTL), 'Dstl forecasts future quantum landscape for UK defence and security', news release, UK Government, 10 July 2020, online.

[10] Department of National Defence, Canadian Armed Forces, *DND/CAF Quantum S&T Strategy: preparing for technological disruptions in the future operating environment*, Canadian Government, no date, online.

[11] F Arute, K Arya, R Babbush et al., 'Quantum supremacy using a programmable superconducting processor', *Nature*, 2019, 574:505–510.

[12] Edwin Pednault, John Gunnels, Dmitri Maslov, Jay Gambetta, 'On "quantum supremacy"', *IBM Research Blog*, 21 October 2019, online.

[13] Karl Wehden, Ismael Faro, Jay Gambetta, 'IBM's roadmap for building an open quantum software ecosystem', *IBM Research Blog*, 4 February 2021, online.

[14] Han-Sen Zhong, Hui Wang, Yu-Hao Deng et al., 'Quantum computational advantage using photons', *Science*, 18 December 2020, 370(6523):1460–1463.

[15] Ming Gong, Shiyu Wang, Chen Zha et al., 'Quantum walks on a programmable two-dimensional 62-qubit superconducting processor', *Quantum Physics*, 5 February 2021, online.

[16] Arute et al., 'Quantum supremacy using a programmable superconducting processor'.

[17] Peter W Shor, 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM Journal on Computing*, 1997, 26(5):1484–1509.

[18] National Quantum Initiative, online; DSTL, 'Dstl forecasts future quantum landscape for UK defence and security'; Department of National Defence, Canadian Armed Forces, *DND/CAF Quantum S&T Strategy: preparing for technological disruptions in the future operating environment*.

[19] Arute et al., 'Quantum supremacy using a programmable superconducting processor'.

[20] Wehden et al., 'IBM's roadmap for building an open quantum software ecosystem'.

[21] JM Arrazola, V Bergholm, K Brádler et al., 'Quantum circuits with many photons on a programmable nanophotonic chip', *Nature*, 3 March 2021, 591:54–60.

[22] M Mosca, M Piani, *Quantum threat timeline report 2020*, Global Risk Institute, January 2021, online.

[23] S Pirandola, UL Andersen, L Banchi et al., 'Advances in quantum cryptography', *Advances in Optics and Photonics*, 2020, 12:1012–1236.

[24] M Nielen, I Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[25] Pirandola et al., 'Advances in quantum cryptography'.

[26] CH Bennett, G Brassard, 'Quantum cryptography: public key distribution and coin tossing', Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, 175.

[27] V Scarani, H Bechmann-Pasquinucci, NJ Cerf et al., 'The security of practical quantum key distribution', *Reviews of Modern Physics*, 2009, 81:1301.

[28] Jiu-Peng Chen, Chi Zhang, Yang Liu et al., 'Twin-field quantum key distribution over 511 km optical fiber linking two distant metropolitans', *Quantum Physics*, 2021, online.

29 Shen-Kai Liao, Wen-Qi Cai, Wei-Yue Liu et al., ‘Satellite-to-ground quantum key distribution’, *Nature*, 2017, 549:43.

30 Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón et al., ‘Gaussian quantum information’, *Reviews of Modern Physics*, 2012, 84:621; Pirandola et al., ‘Advances in quantum cryptography’.

31 Adrian Kent, ‘Unconditionally secure bit commitment with flying qudits’, *New Journal of Physics*, 2011, 13:113015.

32 Pirandola et al., ‘Advances in quantum cryptography’.

33 Joseph F Fitzsimons, Elham Kashefi, ‘Unconditionally verifiable blind computation’, *Physical Review A*, 2017, 96:012303.

34 TC Ralph, ‘Continuous variable quantum cryptography’, *Physical Review A*, 2000, 61:010303.

35 Andrew M Lance, Thomas Symul, Vikram Sharma et al., ‘No-switching quantum key distribution using broadband modulated coherent light’, *Physical Review Letters*, 2005, 95:180503.

36 QuintessenceLabs was established in 2007 to commercialise quantum encryption.

37 Australian Space Agency, *Advancing space: communications technologies and services roadmap 2021–2030*, Australian Government, 2020, online.

38 Juan Yin, Yuan Cao, Yu-Huai Li et al., ‘Satellite-based entanglement distribution over 1200 kilometers’, *Science*, 2017, 256:1140.

39 Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, Nicolas Gisin, ‘Quantum repeaters based on atomic ensembles and linear optics’, *Reviews of Modern Physics*, 2011, 83:33.

40 Konsberg Satellite Services (KSAT), online.

41 Amazon Web Services’ Ground Station service, online.

42 H-J Briegel, W Dür, JI Cirac, P Zoller, ‘Quantum repeaters: the role of imperfect local operations in quantum communication’, *Physical Review Letters*, 1998, 81:5932.

43 Miloš Rančić, Morgan P Hedges, Rose L Ahlefeldt, Matthew J Sellars, ‘Coherence time of over a second in a telecom-compatible quantum memory storage material’, *Nature Physics*, 2018, 14:50.

44 GY Xiang, TC Ralph, AP Lund, N Walk, GJ Pryde, ‘Heralded noiseless linear amplification and distillation of entanglement’, *Nature Photonics*, 2010, 4:316.

45 SK Joshi, J Pienaar, TC Ralph et al., ‘Space QUEST mission proposal: Experimentally testing decoherence due to gravity’, *New Journal of Physics*, 2018, 20:063016, online.

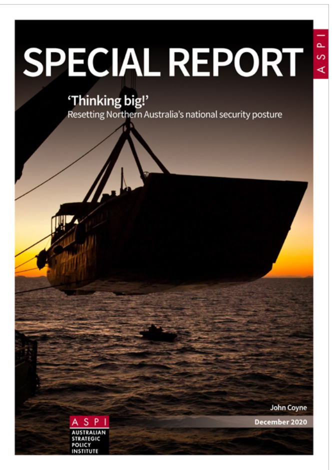
46 NIST, ‘NIST’s Post-Quantum Cryptography Program enters “selection round”’.

47 Malcolm Davis, *Speed, technology are more essential to survival in future war*, ASPI, Canberra, 25 February 2019, online.

ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
ANU	Australian National University
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DARPA	Defense Advanced Research Projects Agency (US)
DSTL	Defence Science and Technology Laboratory (UK)
EWG	expert working group
FTQC	fault-tolerant quantum computers
GPS	Global Positioning System
ISS	International Space Station
IT	information technology
LEO	low Earth orbit
NASA	National Aeronautics and Space Administration (US)
NISQ	noisy intermediate-scale quantum computers
NIST	National Institute for Standards and Technology (US)
OGS	optical ground station
PQC	post-quantum cryptography
QIS	quantum information science
QKD	quantum key distribution
R&D	research and development
S&T	science and technology
satcom	satellite communications
UCLA	University of California, Los Angeles
UCSB	University of California, Santa Barbara
USTC	University of Science and Technology of China
UWA	University of Western Australia

Some recent ASPI publications



SPECIAL REPORT

ASPI

‘Thinking big!’

Resetting Northern Australia’s national security posture

John Coyne

December 2020

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

After Covid-19

Volume 3

Voices from federal parliament

STRATEGY

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

Edited by Genevieve Feely and Peter Jennings

December 2020

SPECIAL REPORT

ASPI

Running on empty?

A case study of fuel security for civil and military air operations at Darwin Airport

John Coyne, Tony McCormack and Hal Crichton-Standish

May 2020

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT

ASPI

Accelerating autonomy

Autonomous systems and the Tiger helicopter replacement

Marcus Hellyer

December 2019

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT

ASPI

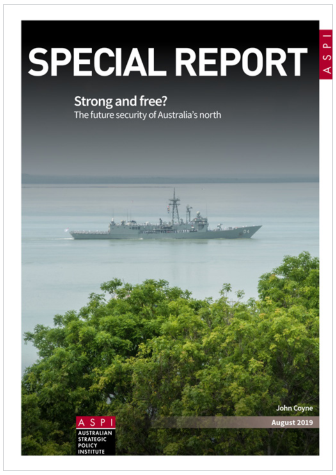
From concentrated vulnerability to distributed lethality—

or how to get more maritime bang for the buck with our offshore patrol vessels

Dr Marcus Hellyer

June 2020

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE



SPECIAL REPORT

ASPI

Strong and free?

The future security of Australia’s north

John Coyne

August 2019

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

The impact of quantum technologies on secure communications

ISSN 2200-6648