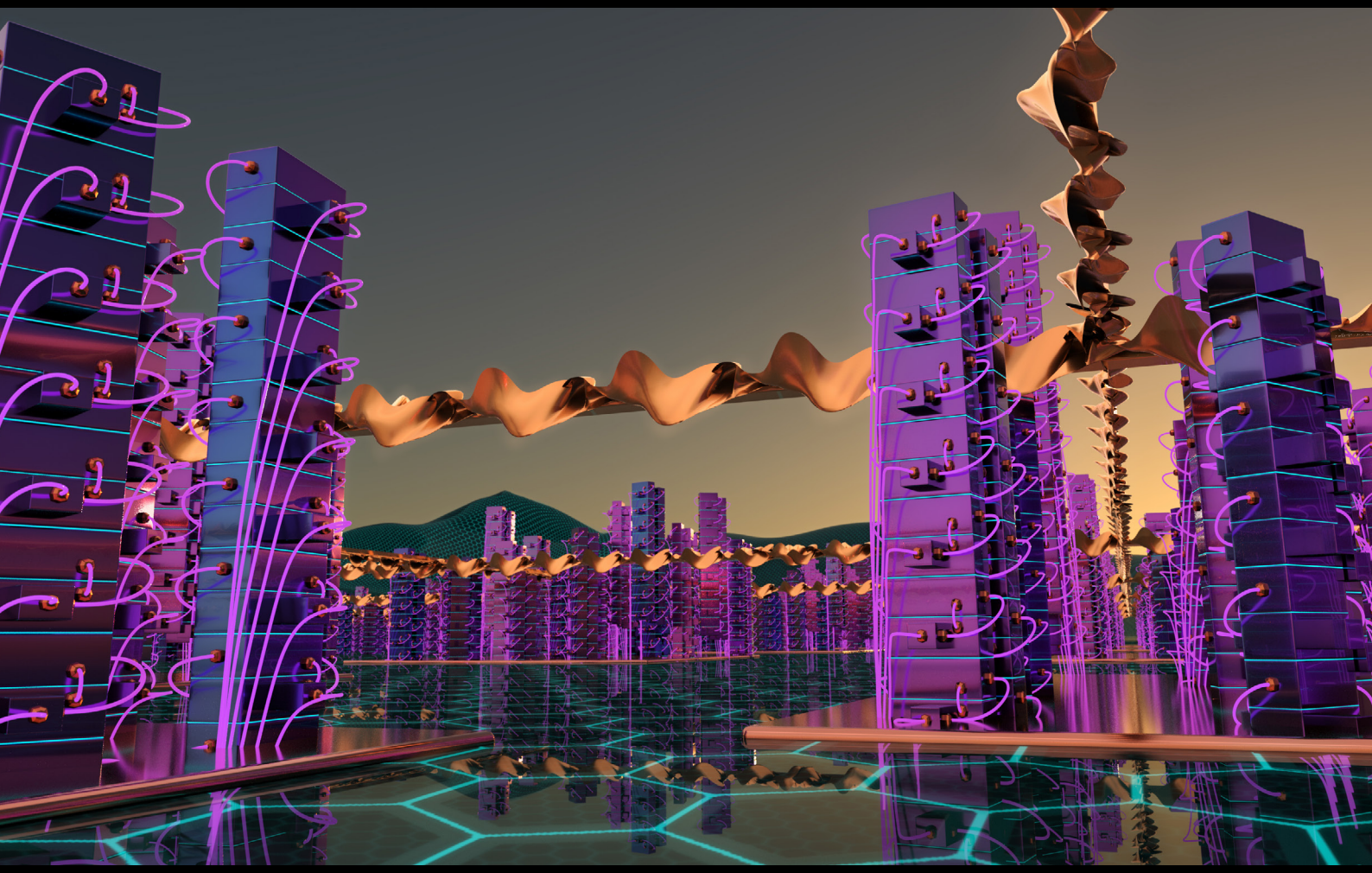
An Australian strategy for the quantum revolution

Gavin Brennen, Simon Devitt, Tara Roberson and Peter Rohde



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
TWENTY YEARS OF ASPI STRATEGY 2001 - 2021

Policy Brief
Report No. 43/2021

About the authors

Gavin Brennen is a professor of physics at Macquarie University working in quantum information theory. He is director of the Macquarie Centre for Quantum Engineering and a chief investigator in the ARC Centre of Excellence in Engineered Quantum Systems.

Simon Devitt is a senior lecturer at the Center for quantum software and information at the university of technology sydney and co-founder and managing director of the quantum consultancy firm, h-bar. Devitt is a recognised expert in the fields of scalable quantum systems architectures for quantum computing and communications systems, quantum error correction and compilation systems for large-scale quantum technologies.

Tara Roberson is a researcher in science communication and responsible innovation, working with the ARC Centre of Excellence for Engineered Quantum Systems and CSIRO. Tara's work will help pre-empt the societal impacts of quantum technologies. This will support the creation of technologies that are both socially desirable and created in the public interest.

Peter Rohde is a senior lecturer and ARC future fellow in the Centre for Quantum Software & Information at UTS. His research has focused on quantum computing, the quantum internet and quantum crypto-economics.

Acknowledgements

Thank you to Danielle Cave for all of her work on this project. Thank you also to all of those who peer reviewed this work and provided valuable feedback including Dr Lesley Seebeck, Lachlan Craigie, David Masters, Fergus Hanson, Ariel Bogle, Michael Shoebridge, Rebecca Coates, David Douglas and Justine Lacey. Finally, we are grateful for the valuable feedback we received from anonymous peer reviewers who work in the fields of quantum academia and policy. ASPI's International Cyber Policy Centre receives funding from a variety of sources including sponsorship, research and project support from across governments, industry and civil society. No specific funding was received to fund the production of this report.

What is 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.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published May 2021. ISSN 2209-9689 (online), ISSN 2209-9670 (print).
Cover image: Produced by Leslie Sharpe.

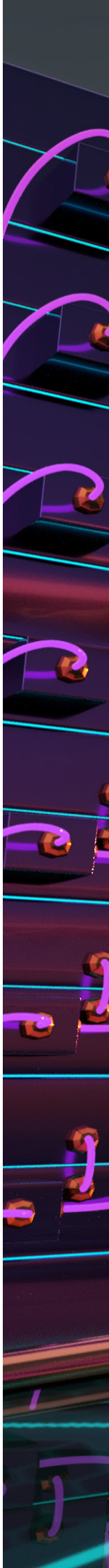
ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

No specific funding was received to fund the production of this report.

An Australian strategy for the quantum revolution

Gavin Brennen, Simon Devitt, Tara Roberson and Peter Rohde



Policy Brief
Report No. 43/2021

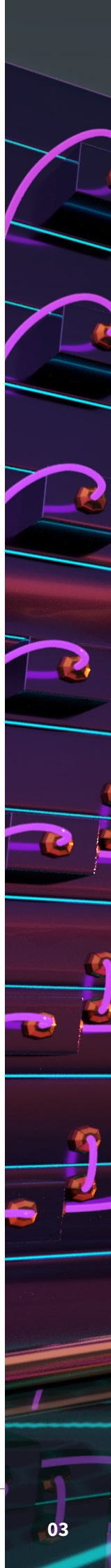
Contents

What's the problem?

The world is now at the precipice of another technological and social revolution—the quantum revolution. The countries that master quantum technology will dominate the information processing space for decades and perhaps centuries to come, giving them control and influence over sectors such as advanced manufacturing, pharmaceuticals, the digital economy, logistics, national security and intelligence.

The power of quantum computing, quantum communications and other quantum-enabled technologies will change the world, reshaping geopolitics, international cooperation and strategic competition. The new United States administration is well aware of this. In his first weeks in office, President Biden signalled a major new policy focus on science and technology,[1] including quantum technologies.[2] This will involve new public investment, working closer with allies, and decisions such as re-establishing the President's Council of Advisors on Science and Technology.[3] The Covid-19 crisis has also seen quantum emerge as an investment vector for post-pandemic recovery: large capital investments have been made over the past year by such nations as China, Japan, Germany, France, South Korea and India.

While Australia benefited from the digital revolution of the 20th century, we missed our opportunity to play a major role in the computing and communications technology sector. A similar fate doesn't have to befall us in the upcoming quantum revolution. We have a long history of leadership in quantum technology and we're highly influential relative to our size. As geopolitical competition over critical technologies escalates, we're also well placed to leverage our quantum capabilities owing to our geostrategic location and alliances with other technologically, economically and militarily dominant powers (most notably the Five Eyes countries) and key partnerships in the Indo-Pacific, including with Japan and India. While Australia is well placed to take full advantage of the quantum revolution, the *status quo* isn't enough. We must build and capitalise on the immense potential of quantum technologies.



What's the solution?

Australia needs a clear quantum strategy, political leadership and an organised effort, including policy focus and public investment. Without those things, we'll be left behind. This report focuses on analysis—and building policy recommendations—to help Australia better leverage the quantum revolution. It also recognises that quantum is just one critical technology and that what's needed is a step change in our current policy settings related to critical and emerging technologies more generally. Hence, this report makes broader policy recommendations that serve the dual purpose of supporting that much-needed step change, while also enabling a more strategic focus on Australia's quantum opportunities.

The Prime Minister should appoint a dedicated and ongoing minister for critical and emerging technologies (that position could also inherit 'cyber'). This minister's focus should be technology, rather than 'technology' being added to a longer list of portfolio topics. This should be a whole-of-government role with the minister working across the relevant economic, national security, industry, research, defence and science agencies in the public service. The Australian Government should also immediately lay the groundwork for a post-Covid-19 $15 billion technology stimulus that should include a $3-4 billion investment in quantum technologies.[4] The stimulus would be a game-changer for Australia and help the country diversify and deepen its technological and R&D base.[5] It would also exploit our disproportionate concentration of world-class quantum expertise, ensuring the long-term growth and maintenance of this vital technological sector.

The government should move quickly in 2021 to develop and articulate a national technology strategy, of which quantum should form a key part. The relatively new but small Critical Technologies Policy Coordination Office in the Department of the Prime Minister & Cabinet (PM&C) should be expanded and elevated to become the 'National Coordinator for Technology'. This division within PM&C—which is already developing a list of key critical technology areas[6]—should lead this whole-of-government technology strategy process. They should work closely with other parts of government, including the Department of Industry, Science, Energy and Resources (DISER), Office of the Chief Scientist, Defence, Home Affairs, DFAT, CSIRO, the Office of National Intelligence, the Australian Signals Directorate, as well as the research and civil society community and the private sector. Within the division, offices should be created to focus on a small number of key critical technology areas deemed most important to Australia and our place in the world. The first such office should be developed for quantum technology, while other offices could focus on, biotechnology[7] and artificial intelligence, for example. A useful model for such appointments is the position of Assistant Director for Quantum Information Science at the White House Office of Science and Technology Policy in the US.

At the same time, the federal government should lead a national quantum initiative, in consultation with the states and territories and the private sector. This national initiative should form the 'Australian Distributed Quantum Zone'—a large collaboration of universities, corporations and Australian-based quantum start-ups tasked with laying the foundations of a dedicated industry in Australia for quantum technology prototyping, development and manufacturing. Significant government investment should be used to help stimulate an economy emerging from the most severe crisis in decades. Australia's favourable handling of Covid-19 presents a unique opportunity to attract new talent as well as to lure back Australians currently running foreign quantum programs, and further expansions to the government's talent visa options should be considered.

Once this groundwork is laid domestically, Australia will be in a strong position to assume a quantum technology leadership role in the Indo-Pacific region.

Introduction

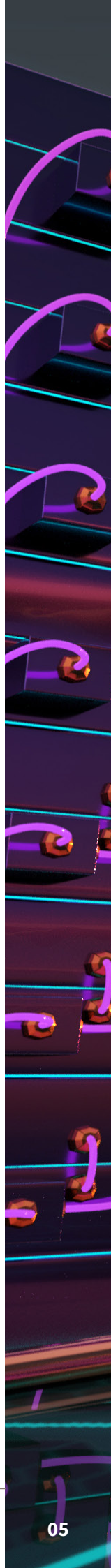
Quantum technology—technology that takes advantage of the rules and behaviour of light and matter at their most fundamental level—has existed for nearly a century. Lasers, MRI machines[8] and transistors all rely on the quantum mechanical properties of nature to function. In fact, quantum technology can be directly attributed to the medical and digital revolutions that occurred in the 20th century. Without lasers there would be no fibre-optic communication, without MRIs the entire field of high-resolution, non-invasive medical imaging wouldn't be possible and without transistors there would be no digital electronics.

However, there's a difference between those types of quantum technology and the devices we're trying to build today. While lasers, MRIs and transistors exploit the quantum mechanical nature of reality to function, they don't manipulate the exact quantum mechanical properties of individual quantum objects such as atoms or particles of light. The second generation of quantum technologies, which includes quantum computers, quantum communication networks and quantum sensors, manipulate single atoms or particles of light with exquisite precision. This leads to computational and communications systems that offer an extraordinary level of new technological power.

Timelines for the delivery of these technologies range widely:

- 0–5 years for sensors for health, geosurveying and security
- 5–10 years for quantum-secured financial transactions, hand-held quantum navigation devices and cloud access to quantum processors of a few thousands of qubits[9]
- 10–15 years+ for the establishment of wide-ranging quantum communications and the integration of quantum sensors into everyday consumer applications, such as mobile phones
- 15 years+ for a quantum computer capable of cracking public-key cryptosystems.

Those time frames could change if and when faster breakthroughs occur, but are at least broadly indicative of the pace and likelihood of quantum development. The quantum technology that birthed the digital revolution of the 20th century was just the beginning. On the one hand, this new class of technology could aid in the creation of new materials and drugs, adapt and secure communication networks, increase economic output and improve quality of life. On the other, quantum technologies also represent a significant long-term threat to our digital security, and the promise of computing technology that can scale exponentially in power in the hands of geostrategic adversaries. These new devices will create a knowledge gap in every piece of technology, from security to manufacturing to medicine and bioscience.



Part 1: Australia and quantum technology

Background: A long history of Australian leadership in quantum technology

Australia has played a pivotal role in the advancement of second-generation quantum technology since the technology's emergence in the 1990s. The country nurtured the intellectual and technological backbone for what's now a global and highly competitive network of academic and corporate research, as well as a rich global start-up ecosystem. However, as world powers are now recognising the urgency of dominating the quantum technology industry, Australia is at risk of losing its competitive edge.

Australia often achieves great things with scarce resources, including in the technology sector, yet we're still small compared to the scientific powerhouses of the US, the UK, Germany, Japan and, in the past 20 years, China. We have a population of just over 25 million and an economy strongly reliant on primary industries, so our scientific research tends to focus on `areas of critical mass' such as mining, agriculture and medical research. Therefore, it may be surprising that a major strength in Australian physics research is still quantum technology.

Australia's expertise in quantum physics and quantum technology emerged thanks to significant research before 1990, as well as government policy and the country's strengths in inexpensive innovation. Since at least the 1980s, Australia and New Zealand have had exceptionally strong representation in the field of quantum optics, for example. It's also an artefact of a time when the fields of particle physics and condensed matter were dominated by the US and USSR. Quantum optics, on the other hand, was a 'cheap and cheerful' science in which real progress could be made with the limited resources available south of the equator.

Here's a brief overview of how Australia currently maintains quantum research:

The Australian Research Council (ARC) Centres of Excellence program is considered the premiere funding vehicle for fundamental and applied research. Many of the (current and past) centres of excellence (CoEs) have a quantum technology aspect. The CoE for Quantum Computation and Communication Technology (CQC2T) has been both the most visible and the best funded of the CoEs since 1999. The vast majority of that investment is focused on the singular goal of designing and building a silicon-based quantum computer. Given the collaborative nature of the CoE, this has resulted in an exceptionally high level of output in the area of quantum computing. In parallel, the CoE for Engineered Quantum Systems (EQUS), funded from 2011 to 2024, has achieved groundbreaking research outcomes in a variety of other quantum technologies falling broadly under the category of quantum machines.

Australia has also hosted other CoEs with significant quantum physics research focused on technology and applications, but they haven't always specifically labelled themselves as quantum technology centres, and many have been discontinued:

- The Centre for Quantum-Atom Optics (ACQAO) combined theoretical and experimental groups to advance the rapidly developing field of quantum atom optics (discontinued in 2010).

- The Centre for Ultrahigh Bandwidth Devices for Optical Systems (CUDOS) focused on photonic engineering and optical devices for communication (discontinued in 2017).
- The Centre for Nanoscale BioPhotonics (CNBP) researched biomedical imaging applications and the control of light at the single photon level (discontinued in 2020).
- The Centre for Future Low-energy Electronics Technologies (FLEET) focuses on low-energy electronics using novel materials, including two-dimensional films and topological insulators (funded until 2024).
- The Centre for Exciton Science (ACEx) is researching the generation, manipulation and control of excitons in molecular and nanoscale materials for solar energy harvesting, lighting and security (funded until 2024).

Beyond ARC-funded schemes, there are other examples of large-scale investment in research in the quantum computing space in Australia. Microsoft has established a strong presence in quantum information and computing via its StationQ (now Microsoft Quantum) research team led by Professor David Reilly at the University of Sydney (also a member of EQUS). Just down the road, the University of Technology Sydney formed the UTS Centre for Quantum Software and Information in 2016 using a combination of university and ARC funding. Although these efforts are still largely university based, they're indicative of the worldwide pivot towards the commercialisation of quantum computing technology by universities, governments and the private sector.

Since around 2016, we've started to see a nascent corporate and start-up sector in quantum technology grow locally. Yet, compared to the rest of the world, Australia is moving very slowly.

In 2008, Quintessence Labs was the first quantum technology company to emerge from an Australian university—spun out from the Australian National University (ANU) —and focused on commercial technology related to quantum key distribution systems and digital security.

In late 2014, QxBranch was founded as a joint spin-off of Shoal Group and the Tauri Group to focus on data analytics and quantum software.

In 2016, h-bar: Quantum Technology Consultants was formed by researchers at RMIT and UTS to service the rapidly expanding corporate and start-up sector.

In 2017, Q-CTRL was founded out of Sydney University and quickly attracted funding from Main Sequence Ventures (the fund associated with the CSIRO). As of 2020, Q-CTRL has secured more than$30 million in venture capital funding, employs approximately 40 scientists and engineers and has recently formed a partnership with the Seven Sisters collaboration to search for water on the Moon.[10]

While the figures were modest, given international developments, there was a sizeable boost in Australian Government funding for quantum between 2016 and 2019 (Figure 1). This was dominated by the renewal of EQUS and CQC2T and the establishment of Exciton Science and FLEET, funded until 2024, along with the establishment of Silicon Quantum Computing, a spin-off company of the University of New South Wales-led effort to build a silicon quantum computer, headed by Professor Michelle Simmons.

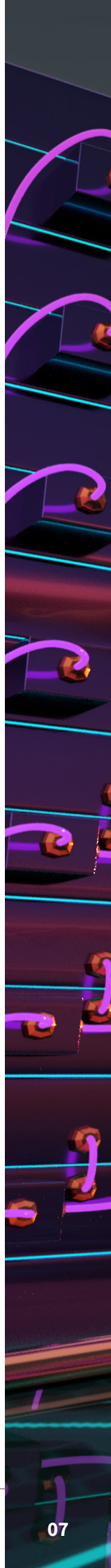
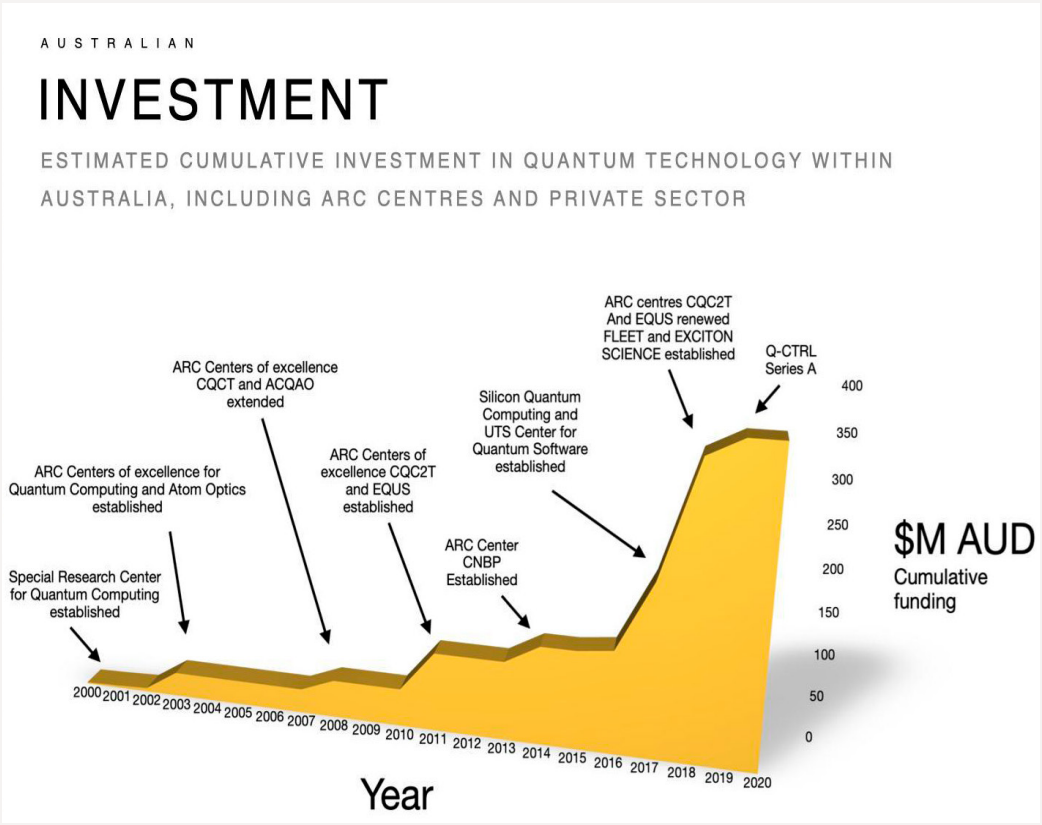


Figure 1: Estimated cumulative investment in quantum technology within Australia, including ARC centres and the private sector, 2000 to 2020



Source: Australian Research Council funding reports (1999-2019), Silicon Quantum Computing and abl.com.au.

Finally, it's important to note that not all industry activity in quantum technology originates from academia. For example the Melbourne-based cybersecurity company Senetas, founded in 1999, has announced that it will distribute post-quantum encryption to customers in Australia and New Zealand.

While Australia has been comparatively slow to seize on the most recent quantum 'boom', there have been recent efforts to begin a coordinated effort in the National Initiative for Quantum Technology Development. In May 2020, the CSIRO released a report titled *Growing Australia's quantum technology industry*. In summarising the current state of quantum technology development in Australia, the report argued that the country could tap potential global revenue of at least $4 billion and create more than 16,000 jobs in the new quantum sector. This is a first step in a national conversation on Australia's future in quantum tech.

Today: Australia is now behind, as the rest of the world started to race in 2014

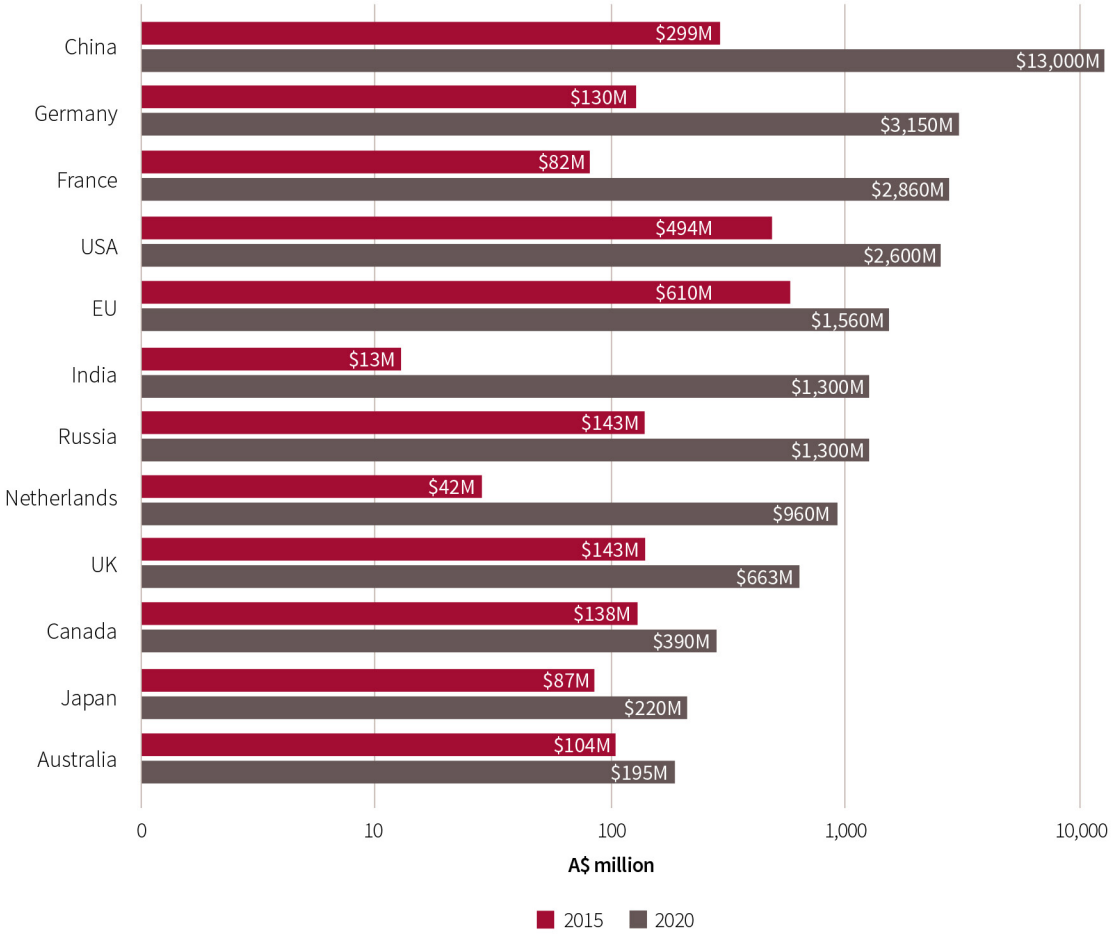
The pace of global quantum technology investment accelerated rapidly between 2015 and 2020, and Australia is falling behind. Before 2015, we ranked sixth in sovereign investment among the nine largest economies actively investing in quantum technology.[11] Today, we're last. Investment in the sector by China, the US, France, Germany, the EU as a whole, India and Russia now exceeds Australian investment by a factor of 10–100, even while Australia maintains a strong position in quantum talent.

Multiple nations have announced billion-dollar programs to develop their quantum technology industries. China has flagged over A$13 billion to set up a four-hectare quantum technology centre in Hefei.[12] In October 2020, China also announced that quantum technologies would be included in

its 14th Five-Year Plan (2021–2025).[13] Japan has stepped up its investment in quantum computing by placing a functional error-corrected computer as one of its six 'moonshot' targets in a newly funded A$1.3 billion program.[14] Japan was one of the major early investors in quantum technology, but it lost significant ground in the late 2000s and early 2010s because of a lack of confidence within government. If Australia doesn't move quickly, we could lose the edge that we've cultivated since the turn of the century and unlike Japan, might not have the resources or talent to recover.

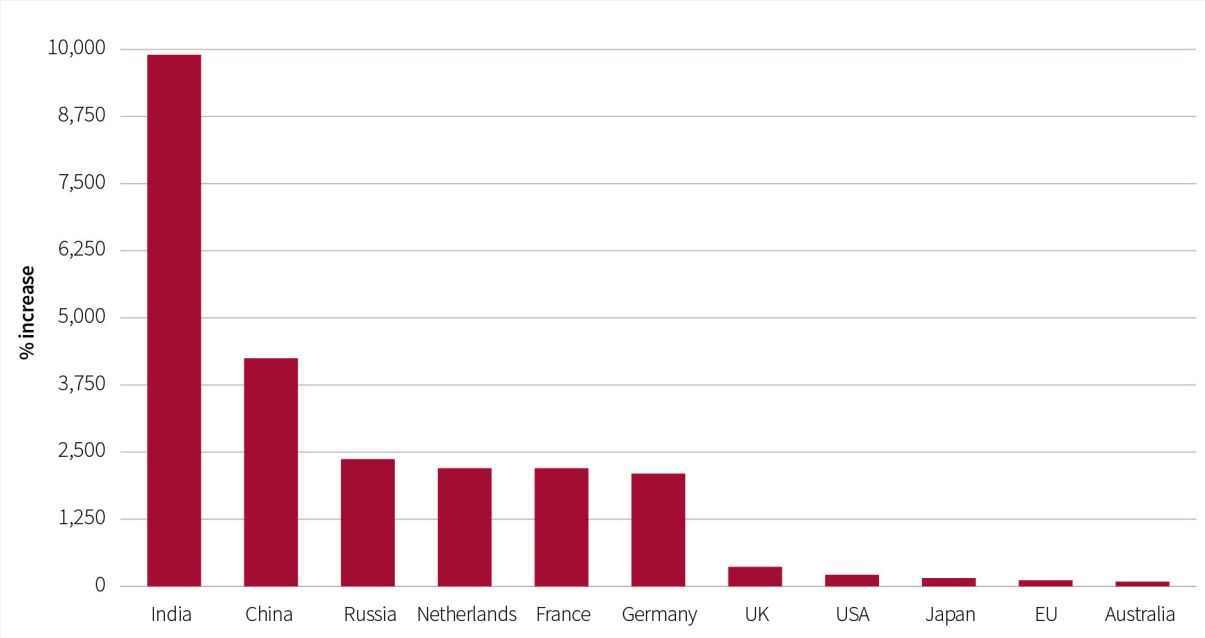
The Covid-19 crisis has also seen quantum technology emerge as an investment vector for post-pandemic recovery (figures 2 and 3). As part of a major stimulus injection, the German Government announced a A$3.15 billion investment into quantum technologies.[15] In January 2021, France announced a five-year A$2.85 billion investment in quantum technologies intended to place it in the top three in the world, together with the US and China.[16] Its investment strategy is broad: it includes funding for a universal quantum computer, quantum simulators and sensors, quantum communications, post-quantum cryptography, and support technologies such as cryogenics. The Israeli Government also announced a A$78 million program to build domestic quantum capacity, including the construction of a 30–40 qubit quantum computer through a contract that will be put out to tender later in 2021.[17] As recently as April 2021, the Netherlands announced a A$960 million investment from the National Growth Fund to train 2,000 researchers and engineers, fund up to 100 new quantum start-ups and host three corporate R&D labs[18].

Figure 2: Sovereign funding increases, 2015 to 2020 (A$ million)



Source: These figures are the same as quoted in footnotes (11-18), 2015 data is from The Economist, online. Please note that for the Netherlands and Canada, data has been used from early 2021 announcements.

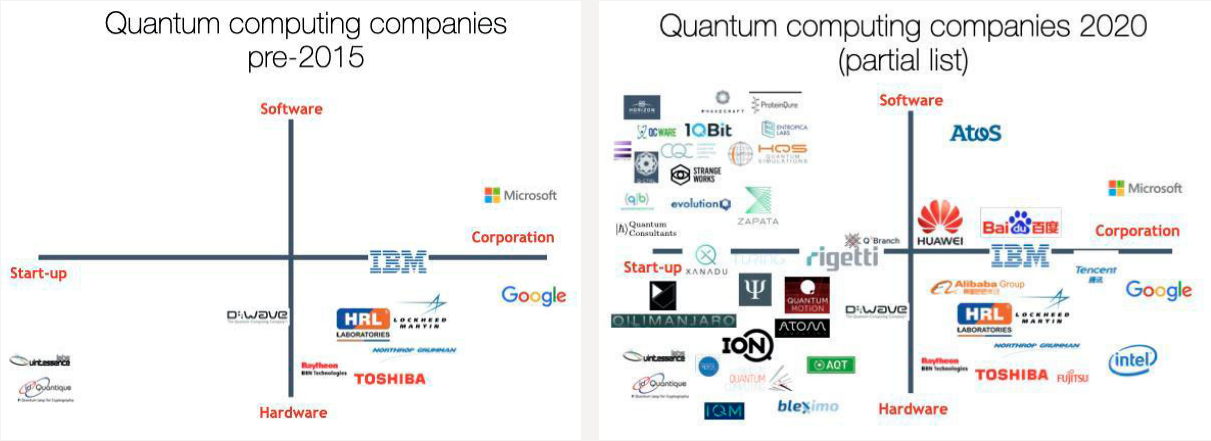
Figure 3: Percentage increase in sovereign funding, 2015 to 2020



Source: derived from Figure 2.

The private sector's involvement in both corporate investment and private equity funding of quantum start-ups has also boomed (Figure 4). Several start-ups in quantum technology are now valued at well over A$1 billion, and shares in at least two quantum tech companies are now publicly traded.[19] Australia has again moved comparatively slowly in the start-up space: only one quantum computing hardware start-up and one software start-up have raised significant levels of funding.[20] National R&D programs have been used extensively overseas to help incentivise private-sector engagement in quantum technology development, but that hasn't been mirrored in Australia.

Figure 4: Quantum computing companies before 2015 and in 2020



In each of the recent examples, governments around the world have recognised that quantum science is no longer an academic field of research, but rather a burgeoning new technological industry. The difficulty faced by the Australian quantum industry is the translation of what, until recently, has been a mostly academically focused endeavour into a nascent new commercial sector.

Building a quantum society

Quantum technologies will affect many aspects of our society and economy, including health care, financial services, defence, weather modelling and cybersecurity.

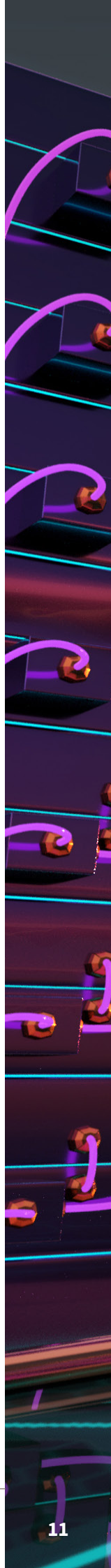
One type of quantum technology—the quantum computer—presents a potentially dazzling range of applications. They include quantum chemistry simulation that will accelerate drug development, improved supply-chain optimisation and supercharged artificial intelligence. These quantum computing applications promise exciting benefits. Yet the history of technology development suggests we can't simply assume that new tools and systems will automatically be in the public interest.[21] We must look ahead to what a quantum society might entail and how the quantum design decisions being made today might affect how we live in the future.

Consider the use of quantum computing to advance machine learning and artificial intelligence (ML/AI). ML/AI technologies are already the subject of ethical frameworks designed to prevent harm and ensure the design of ethical, fair and safe systems.[22] Those frameworks are vital, as potential harms could include the reproduction and amplification of existing socio-economic marginalisation and discrimination, and the reduction of personal privacy.

At this time, no ethical framework for quantum technologies exists in Australia, although the CSIRO Quantum Technology Roadmap calls for quantum stakeholders to explore and address social risks.[23] As quantum technologies progress, such discussions should build literacy in the societal impacts of quantum technologies. This should be a collaborative effort between quantum physics and social science researchers, industry experts, governments and other public stakeholders, and be led by the proposed office of the minister for critical technologies.

An example of this discussion began at the World Economic Forum in 2020 through the launch of a global quantum security coalition,[24] which is working to promote safe and secure quantum technologies. Australia should draw on such initiatives during the creation of a national quantum initiative to ensure the quantum technologies we develop work for the public good. In addition, two new legal organisations launched in 2020—the Australian Society for Computers and Law and the Digital Law Association—have identified quantum as a technology that needs engagement from the legal community in order to draft well-designed standards and regulations.

Quantum researchers and other stakeholders in the emerging quantum tech industry should review the potential impacts of quantum technologies on society.[25] Establishing links between Australian publics and quantum researchers may help them in that review. To begin public engagement with quantum technologies, the quantum sector should invest in accessible information on quantum technologies and establish dialogue with Australian publics on a range of applications related to the new technologies. That will clarify societal expectations for the scientific community and policymakers and prompt work to address any concerns raised. Outcomes from these exercises should also inform the national quantum initiative.



Australia's quantum talent leak

Australia's long history in quantum technology means that our quantum technologists are high on the priority list for recruitment. Australians are some of the most successful start-up founders and leaders in the quantum industry. However, many are now working outside of Australia. Notable examples include the following:

- Jeremy O'Brien and Terry Rudolph (UNSW and the University of Queensland) are founders of the photonics-based quantum computing start-up PsiQuantum located in Silicon Valley. They have raised over A$400 million in venture capital to date.
- Jay Gambetta (Griffith University) is an IBM Fellow and Vice President of Quantum Computing at IBM, where he has spearheaded the massive growth in IBM's investment in quantum computing.
- Christian Weedbrook (University of Queensland) is the CEO and founder of Xanadu, an optics-based quantum computing start-up. Now located in Toronto, Xanadu has raised over A$40 million in venture capital funding.
- Runyao Duan (the founding director of the Centre for Quantum Software and Information at UTS) is now the director of the Quantum Computing Institute at Baidu in Beijing.
- Min-Hsiu Hsieh (a founding member of the Centre for Quantum Software and Information at UTS) is now the director of the Hon Hai Research Institute for Quantum Information Science (a division of Foxconn) in Taiwan.

Australia must prioritise plugging the quantum industry's talent leak over the next two years and attracting back the talent that has moved offshore and acquired new expertise. Without a strong quantum computing sector and without significant mechanisms to train and retain highly qualified personnel, the significant investment that Australia has made in such talent will be lost. The uncertainty about H-1B visas in the US—notwithstanding the recent partial lifting by the Biden administration of the 2020 suspension by the Trump administration[26]—offers an opportunity for Australia to pursue skilled recruitment (in quantum, for example), given our favourable handling of the Covid-19 crisis.

The need to build quantum talent, education and literacy in a post-Covid world

We're all now familiar with the term 'digital literacy': the necessity for the workforce of the 21st century to work with classical computational infrastructure. As quantum technology develops, quantum literacy will become similarly instrumental.

The creation of a talent pipeline of students who can understand and speak the language of quantum technology is a necessity—especially given the explosion of quantum start-ups and corporate teams—and will be strategically critical in the near future as the technology begins to be integrated into global information processing and telecommunications infrastructure.

One promising initiative by the NSW Government, the Sydney Quantum Academy (SQA), brings together the four main research universities in Sydney with strong quantum technology programs. Founded to provide higher degree research training at the masters and PhD levels in a coordinated way between UNSW, Sydney University, UTS and Macquarie University, the SQA is expected to amalgamate

a large amount of the teaching and training efforts in quantum technology in the state. With an initial five-year investment from the NSW Government of A$35 million, it's expected to teach a student cohort of approximately 500 PhD students and is mandated to facilitate outreach and entrepreneurship in the Sydney area—a level of coordination for quantum training that's never before existed in Australia.[27]

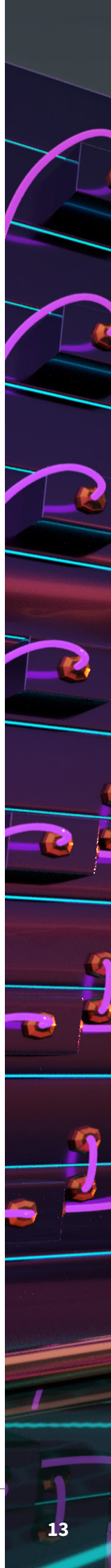
While the SQA is a promising first step, efforts in providing education and training programs to build quantum literacy should be expanded nationwide. The talent pipeline for a quantum technology industry requires integration with graduate, undergraduate and even high-school programs across disciplines such as physics, engineering, computer science, mathematics and business. Just as digital literacy begins in school and becomes more specialised as a student progresses through university, quantum literacy programs should be similarly designed. The US and the EU are already rapidly accelerating their development of quantum education programs at all levels of education, targeting both domestic and international markets.[28]

Education and training should be an immediate focus for Australian investment and leadership to market the country as a leading quantum educator. Establishing educational services internationally, especially in the Asia–Pacific region, should also be a high priority.

Notable targets include the Indian and Taiwanese markets. India has indicated an intention to invest A$1.4 billion into quantum technology, but doesn't have the required domestic expertise to exploit that level of national investment.[29] Australia has the potential to provide those services to burgeoning global quantum industries.[30]

Similarly, Taiwan has indicated that it may more aggressively expand its efforts in quantum technology. Foxconn has established the new Hon Hai Research Institute, which has a dedicated program in quantum computing and there have been rumours that a more concerted government-backed effort may be emerging in Taipei. While the current level of domestic talent in Taiwan is significantly larger than in India, it still represents a market opportunity for Australia to provide training, education and R&D collaboration.

The local quantum talent present in Australia and initial pilot programs[31] should be expanded and developed into a federally coordinated effort in which state-level initiatives—such as the SQA—take a strong leading role. It's expected that states such as Victoria and Queensland will attempt to mirror the SQA model, but a lack of a critical mass of academics outside Sydney will make other state efforts difficult unless more quantum talent is hired or efforts are coordinated across state borders.



Part 2: How quantum technology will shape the world

Quantum will reshape not only technology, but also geopolitical strategy

The race to build quantum technologies is not only one of science and commerce. It's a race for geopolitical leadership. Attempts to predict the impact of future technology have been notoriously inaccurate. Famous underestimates include the prediction in 1943 by Thomas Watson, then-president of IBM, that 'there is a world market for maybe five computers.' Clearly, there was a view that computational power was nothing more than a minor scientific tool or curiosity, when it has instead dictated geopolitical power and economic growth over the past 80 years. With that in mind, we outline three scenarios in which quantum technologies could significantly affect geopolitics.

First, there are immediate consequences for relations between Western allies and China, particularly in quantum education and technology transfer. A US senator recently claimed the US had trained some Chinese nationals to 'steal our property and design weapons and other devices', and that 'they don't need to learn quantum computing and artificial intelligence from America.'[32] The mention of quantum computing wasn't incidental. The publicity over Chinese government-sponsored quantum technology, starting with the 2017 demonstration of satellite-based quantum communications, hasn't gone unnoticed by policymakers in Washington.[33]

The US Department of Energy has requested a 2021 budget that includes A$56 million to accelerate the development of the quantum internet[34] on the back of a 2021 budget request, initially by the Trump administration, of A$312 million for quantum technologies.[35] That complements the A$1.6 billion quantum investment signed into law in 2018.[36] Xi Jinping's government is spending A$13 billion on China's National Laboratory for Quantum Information Sciences.[37] In recognition of the national security implications of this technology, Australia has already identified 'quantum cryptography' and 'high performance quantum computers' as controlled technologies in the Defence and Strategic Goods List.[38]

Second, there's potential for quantum technology to tip the balance between regional powers. Some possible scenarios include the following:

- In early 2020, India committed A$1.4 billion for quantum computing research over five years.[39] Access to enhanced imaging provided through satellite-based quantum sensing and enhanced image processing could enable the identification of underground nuclear installations in neighbouring Pakistan.
- Conflict-ridden areas of the Middle East have experienced periods in which even vastly outnumbered insurgents have been able to maintain strategic footholds using improvised explosive devices (IEDs). While IEDs are relatively cheap to produce, technology to respond to counter-IED tools evolves quickly. Quantum technology could benefit either side. For example, extremely precise quantum magnetometers can detect large mobile metal equipment as targets or detect IEDs themselves, and photonic chips could operate even in the presence of an electromagnetic pulse that would knock out conventional electronics.

- China's Belt and Road Initiative, launched in 2014, had signed up about 65 countries, including 20 from Africa, by 2019.[40] Many of its key projects are being financed by mined minerals from sub-Saharan Africa. Quantum gravimeters could significantly improve the accuracy of drilling by sensing density fluctuations that indicate oil and mineral deposits with a precision not possible with classical devices. Increasing access and raw material yields in nations within China's sphere of influence could reduce demand for Australian exports.

Finally, quantum tech will disrupt digital economies. Cryptocurrencies are being used increasingly by institutional and private investors and have a current market value of over A$2 trillion. One significant threat to cryptocurrencies is from quantum computer attacks on the digital signatures used to secure transactions between untrusted parties. That would allow a malicious agent to steal crypto tokens like bitcoin undetected. In fact, up to one-third of all bitcoin, worth hundreds of billions of dollars, is estimated to be vulnerable to such theft.[41] This type of threat, whether realised or not, has the potential to undermine confidence in all contemporary blockchain-based systems. The solution is to use so-called post-quantum cryptography that's thought to be immune to attack using quantum technology. That technology is already used by some cryptocurrencies, such as HyperCash and Quantum Resistant Ledger.[42] It will be a matter of economic security to frequently test and verify that coming post quantum cryptographic standards are met.

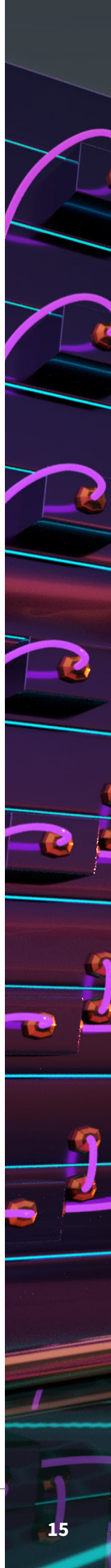
Quantum's role in national security, defence and intelligence

The defence and intelligence implications of quantum technology can be broken down into several categories, depending on the underlying technology: quantum computing, quantum communications and quantum sensing.

1. Quantum computation

The increased power of quantum computing affects a wide range of national security applications, from materials science to logistics, but the most direct application of interest to the defence and intelligence community is in cryptography. Quantum computers applying artificial intelligence to enormous datasets at speeds that create strategic and operational advantage have direct impact in the field for two key reasons:

- The entire security backbone of the internet is built using encryption that's vulnerable to quantum computing. That includes everything from internet banking to the domain name system security certificates that are used to verify whether 'google.com' is really Google.com, instead of a hacker. The development of a quantum computer without changing the current encryption standards that underpin the entire classical internet would be catastrophic to network security.
- While a quantum computer able to break this type of encryption won't be around for at least a decade or two, a large amount of encrypted information crossing networks, some of which is being intercepted by malicious actors, needs long-term security. Medical records, client data held by insurance companies and nuclear weapons stockpile information are just some examples. While hackers might not have the ability to break encryption today, saved copies of encrypted data could quickly be decrypted when quantum computers become available. To prepare for that scenario, policymakers, businesses and researchers need to consider three key questions:



1. For how many years does the encryption need to be secure, if it's assumed data is intercepted and stored?
2. How many years will it take to make our IT infrastructure safe against quantum attacks?
3. How many years will it be before a quantum computer of sufficient power to break encryption protocols is built?

As anticipated by many, the first realisation of quantum computing technology has occurred in the cloud, as users log onto dedicated hardware over the classical internet. These types of 'quantum in the cloud' systems began with the connection of a two-qubit photonic chip to the classical internet by the University of Bristol in 2013[43] and accelerated significantly in 2016 with IBM's introduction of its Quantum Experience platform. We now see both free and paid services offered by IBM, Microsoft, Amazon, Xanadu and Rigetti using a variety of hardware modalities for small-scale quantum computing chipsets with capacities of up to 65 physical qubits. This has spurred the so-called noisy intermediate-scale quantum (NISQ) field of algorithm and hardware research.[44] However, we've only just begun to understand how these machines will be constructed and used, and their technological development is continuing to accelerate.

For a detailed explanation of quantum computing threats to cryptographic systems, see Appendix 1 on page 24.

2. Quantum communications platforms

Quantum technology has progressed rapidly in recent years and will have a significant impact on communication technology. The largest investment in quantum communications technology is currently being made by the Chinese Government.[45]

China has two major quantum networking initiatives geared towards building a quantum key distribution (QKD) infrastructure[46]—a technology that solves some of the security problems, discussed above, that quantum computing creates for public-key cryptography.

The first program in the Quantum Experiments at Space Scale (QUESS) program culminated in the 2016 launch of China's Micius platform, which was a proof-of-concept platform that allowed for the distribution of entangled pairs of photons to elevated telescopic ground stations separated by thousands of kilometres. The QUESS program is designed to use a potential constellation of quantum-enabled satellites. It will provide secure cryptographic keys between multiple ground stations to secure classical communications channels using strong symmetric encryption, with keys provided by a quantum backbone network. The exact amount of funding for the QUESS program is currently unclear; however, based on a 651 kilogram payload and estimates of prices for commercial launches into low Earth orbit at that time, the cost of this technology demonstrator could easily approach A$100 million.[47]

The QUESS program is part of a broader quantum communications effort in China. A second major component is the Beijing-to-Shanghai optical QKD link. This is a 32-node optic-fibre-based link that's built along the high-speed train line between the two cities, in which each node is located in secure facilities at particular stations.

These two technology demonstrators have recently been amalgamated into a national QKD network, combining more than 700 optical fibres on the ground with two ground-to-satellite links to achieve QKD over a total distance of 4,600 kilometres for users across China.[48] That level of investment and technology deployment is significantly more advanced than in any other nation that's building quantum communications systems.

Other countries have instituted similar programs or are planning to do so. For instance, a government-funded quantum repeater network is to be built between four cities in the Netherlands. There's also a A$410 million program authorised in the US for the initial development of technology for a future US quantum internet.[49] There are even discussions within Australia about a space-based quantum communications centre of excellence in collaboration with the Australian Space Agency. However, Australia is significantly behind China in technological development and it isn't clear, from a scientific and technical perspective, whether replicating what China has done is the most appropriate way to proceed.

For a more detailed explanation of the major quantum communications systems being deployed worldwide, see Appendix 2 on page 29.

3. Quantum sensing and its applications for the resources sector and defence

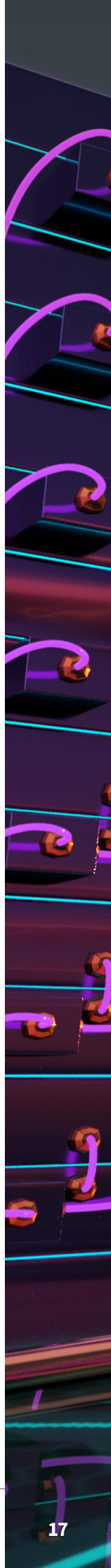
Quantum sensing is seen as one of the three main pillars of quantum technology development, along with quantum computing and quantum communication systems. Applications that provide positioning, navigation and timing could potentially benefit from quantum effects, especially when combined with a quantum communications network. Quantum sensing may be the first technological application to be widely adopted in markets.

Three types of quantum sensors have direct applications in multiple sectors, including mining and defence:

- **Quantum sensors to detect magnetic fields with high precision (magnetometry):** In principle, this can be used for the undersea detection of magnetically discernible materials. The most promising candidates in this area are diamond-based quantum sensors, and significant effort at Melbourne University, Macquarie University and the ANU is focused on developing that technology.
- **Increased timing precision (atomic clocks):** The GPS and inertial guidance positioning, navigation and timing are intricately linked to precise clocks. While atomic clocks have been commercialised for more than 30 years, the ability to miniaturise and package atomic clocks based on technology such as ion traps may be instrumental in even wider adoption.
- **Quantum sensors for ultra high precision measurement of gravitational fields (gravitrometry):** By measuring small deviations in 'little g' (the acceleration due to the Earth's gravitational field), we can possibly detect anomalous underground structures, which could be hidden subterranean bases or large oil and mineral reserves.

None of those platforms requires the hardware resources needed for quantum computing or communications systems, so they're comparatively easier to build and test. However, their superiority over highly precise classical systems isn't as well understood, so they'll need to show a competitive advantage in both price and portability before they're adopted at scale.

The UK, the EU, the US and Canada all have extensive research programs in the quantum sensing space as well as numerous start-ups. In Australia, sensing is most likely to find markets within the minerals sector.



Part 3: What we need to do

Drivers for action: Time for strategic investments

The world is racing to develop quantum technology for business as well as for security and defence. It's now a crucial moment. Australia reacted exceptionally well in the late 1990s and early 2000s as quantum technology became a substantial area of research within academic physics, computer science and engineering departments. The investment in ARC fellowships, special research centres and centres of excellence tied to quantum computing and related technologies ensured that we were at the forefront of development during the 2000s and early 2010s. Yet, in the years since, there's been no acceleration of national funding for quantum technology. Consequently, there's been little movement from the private sector to get involved in the field.

Australia doesn't have the capital needed to build a complete R&D infrastructure and manufacturing base to control a large share of the future quantum technology market. However, that shouldn't stop us making strategic moves to become a major player in some of the more lucrative aspects of this new industry. We already possess the technical know-how to invent, develop and prototype some of the critical components needed for large-scale quantum technologies. We can also set up companies, research centres or even government-backed entities to build up large intellectual property portfolios across a variety of physical hardware platforms.

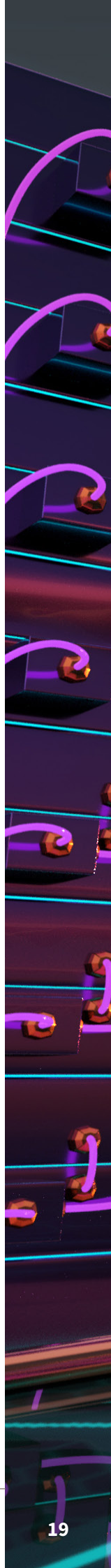
Australia has a significant level of expertise in software and hardware and could develop and manufacture critical components domestically. Of the major hardware systems for large-scale quantum computing, Australia has a near-monopoly on the most advanced technology for silicon (CQC2T and its spin-off company, Silicon Quantum Computing). We were also the pioneers and maintain a very high level of hardware expertise in optical quantum computing platforms, and we have significant capacity in diamond-based systems.

While Australia has the talent and ideas, there's no mechanism to focus that capacity for the benefit of the Australian quantum technology sector. We can no longer rely solely on academia to lead our approach to quantum technology. Private-sector investment must be boosted. As we've seen in the US and the EU, investment comes when the private sector sees the establishment of strong, technology-focused initiatives. Arguably, large quantum efforts at companies such as Microsoft and IBM exist, in part, because those companies were corporate partners in US defence and intelligence funding set up by the Defense Advanced Research Projects Agency and the Intelligence Advanced Research Projects Activity in the 2000s and early 2010s.

In August 2020, for example, the US launched its national quantum research centres as part of its National Quantum Initiative. This should be a particular motivator for Australia, and particularly the Australia–US alliance, as it provides an opportunity for enhanced engagement and cooperation. Five new research centres focused on computing, communications, sensing and simulation have been established and funded to the tune of A$150 million. The centres build in major collaborations between US national labs, universities and, most importantly, quantum technology companies. The level of private–public engagement involved in the research centres is something that Australia needs to replicate.

While world-leading R&D is occurring in Australia, when it benefits private-sector interests, it benefits offshore quantum computing programs. That doesn't happen in other nations. In the US, for example, Amazon has made a multimillion-dollar investment to set up Amazon Web Services' quantum division in collaboration with Caltech in California. Likewise, partnerships with IBM link university research centres and other corporations interested in quantum technology, such as Goldman Sachs, and multi-institutional collaborations are taking advantage of funding incentives made available through the National Quantum Initiative. Such incentives don't currently exist in Australia, and we're being crowded out of the private–public collaborative space that's taking shape.

Australia requires a strategic investment in dedicated research programs that are focused on technology development (unlike the centres of excellence, which mainly have a remit for basic research) to remain relevant on the global stage. This could take the form of a dedicated centre or program for the development of a small-to intermediate-scale quantum computer using optical systems or diamond technology that Australia has significant experience with, or it could be a major initiative to develop key quantum software components.[50] If done correctly, that could reassert a level of Australian leadership in the quantum technology sector that has degraded over the past decade. An initial $3–4 billion national quantum strategy will be needed over the next five years to ensure that Australia can benefit from this new technological revolution.



Policy recommendations

1. A new minister

At the earliest opportunity, the Prime Minister should appoint a dedicated and ongoing minister for critical and emerging technologies (this position could also inherit 'cyber'). This minister's focus should be technology, rather than 'technology' being added to a longer list of portfolio topics. This should be a whole-of-government role with the Minister working across the economic, national security, industry, education, defence, research and science agencies in the public service. The minister would play a key role in the implementation of many of the policy recommendations made here.

2. A national technology strategy

The government should move quickly this year to initiate a whole-of-government technology strategy process led by PM&C, of which quantum should form a key part. By authorising PM&C to lead this initiative, this strategy necessarily recognises that there is no one lens through which to view technology and that its emergence and deployment will impact everything, including our society, the economy and industry, national security and human rights. This strategy should include consideration of appropriate ethical frameworks for critical and emerging technologies such as quantum. PM&C should work closely with other parts of government including the DISER, Office of the Chief Scientist, Defence, Home Affairs, DFAT, CSIRO, the Office of National Intelligence, the Australian Signals Directorate as well as the research and civil society community and the private sector. The new minister for critical and emerging technologies would be responsible for delivering the strategy to the Australian public by 2022.

3. Expand and elevate PM&C's whole-of-government leadership role on technology policy

There is positive momentum in government and growing knowledge on critical and emerging technologies (like quantum) in departments such as Defence, DISER, CSIRO and PM&C. However, there's currently no clear government lead on 'technology', and that lack of leadership and coordination is preventing policy progress. Critical and emerging technologies present a myriad of opportunities, challenges and threats, and PM&C is the only department with the whole-of-government perspective to balance them in our economy, society and national security. The relatively new but small Critical Technologies Policy Coordination Office in PM&C—the creation of which was a welcome move by the government—should be immediately expanded and elevated to become the National Coordinator for Technology.

The expanded division should work with Australia's new minister for critical and emerging technologies to support the delivery of the recommended national technology strategy.

Within the new PM&C division in 2021, small offices focusing on key critical technology areas should be created. Quantum technology should be the first such office developed, and other small offices could be built to focus on biotechnology[51] and artificial intelligence, for example. A useful model for such appointments is the Assistant Director for Quantum Information Science at the White House Office of Science and Technology Policy in the US.

The government should search for individuals to lead these offices who can serve as catalysts, working across government (including with the military and intelligence agencies), business, the research sector and internationally, to deliver a post-Covid-19 technology stimulus and build a pipeline of focus, policy and investment that should last decades. These leaders will need to engage globally and strengthen relationships with our key partners in the Indo-Pacific and work across key groupings such as the Quad (US, India, Japan, Australia). Investments in quantum technology, for example, require careful consideration of our interdependence with our strategic allies, which we're currently well placed to cooperate with and piggyback on, and of our likely adversaries.

4. A$15 billion post-Covid-19 technology stimulus

The Australian Government should immediately lay the groundwork for a multi-year $15 billion post-Covid-19 technology stimulus that would also be informed by the delivery of a new national technology strategy. This stimulus should include a $3-4 billion investment in quantum technologies. The stimulus would be a game-changer for Australia and help the country diversify and deepen its technological and R&D base. It would also exploit our disproportionate concentration of world-class quantum technology expertise, ensuring the long-term growth and maintenance of this vital technological sector. The following recommendations describe what this stimulus could look like from a purely quantum perspective.

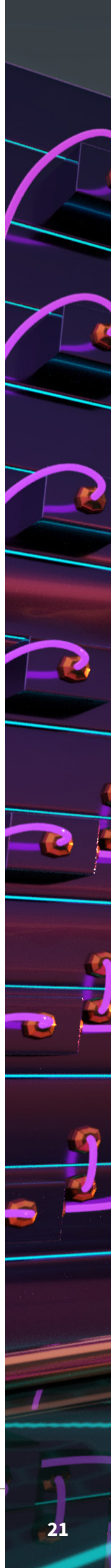
5. Establish an 'Australian distributed quantum zone'

A national quantum R&D initiative should be a key part of the government's post-Covid-19 technology stimulus. This could be established with a multibillion-dollar national funding initiative that would leverage the seed investments Australia has already made over the past 30 years. This initiative could be akin to a special economic zone—a place for quantum-related economic activity that wouldn't sit with one city or state but instead be distributed nationally across universities and research institutes. The Melbourne Biomedical Precinct provides an attractive blueprint for the development of such a national initiative.[52] Given the diversity of expertise and capabilities across the country, a distributed quantum zone not tied to a capital city or state is preferable.

The commercialisation of university-developed intellectual property is currently a major roadblock in building a quantum ecosystem in Australia beyond university research. Researchers are often actively disincentivised from spinning out academic research into new start-ups because of the administrative overhead in extracting relevant intellectual property. Universities should be encouraged to ensure that they foster collaboration, entrepreneurship and commercialisation in the quantum space. The newly announced A$5.8 million University Research Commercialisation Scheme scoping study should be encouraged to address the commercialisation of quantum technology.

6. Lure Australian talent back home and attract foreign talent

Australia's favourable handling of Covid-19 presents a unique opportunity to attract new technology talent as well as to lure back Australians currently running quantum programs in other countries. This could involve increasing the accessibility, scope and clarity of R&D tax incentives, especially for small and medium-sized enterprises and further expansions and tweaks to the government's 'Global Talent Independent Program', including for example, lowering the expected salary requirements below A$153,600/year.[53]



7. Build global cooperation and increase direct involvement in quantum development by the defence and intelligence communities

The Australian defence and intelligence communities, when compared to their counterparts in the Five Eyes alliance, are disengaged from the quantum technology community.

The Chief Scientist (Cathy Foley) and the Chief Defence Scientist (Tanya Monro) have strong backgrounds in quantum. Their expertise should be immediately tapped to create a quantum defence and intelligence working group, connecting stakeholders within government to the quantum technology community in order to identify key national security priorities that can benefit from quantum technology.

Australia should focus quantum technology work related to national security and defence through a formal partnership with the US, using the precedent of cooperation in other areas of science and technology. The national security and defence implications of quantum technology are clear enough to make this area of development a new core element of the Australia–US alliance. Formalising this partnership, in a similar manner to the US–Japan Tokyo statement on quantum cooperation,[54] will also enable academic and industry contributions to contribute to and draw from the partnership. We support the similar policy recommendation in ASPI's defence-focused report, *The impact of quantum technologies on secure communications*, which argues for the formalisation and prioritisation of Australia–US cooperation on quantum technology.[55]

Quantum experts should be encouraged and aided to gain the security clearances needed to be read into programs that may benefit from quantum technology. This should occur initially in an advisory context, but expand as projects are identified.

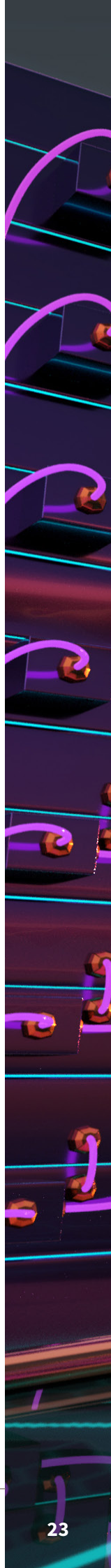
8. Eliminate uncertainty by developing a national framework outlining national security and defence policy covering quantum technology

The explosion of investment around the world and the unique expertise that Australia has open up tremendous opportunities for incoming investment from overseas. However, both the private sector and Australian research centres are in many cases timid or hostile to such partnerships due to the expected nature of a future national policy covering technology transfer in the quantum space. There are already examples of multimillion-dollar deals that have been rejected at the university level because of perceived future problems with export controls and their ability to work with certain nations, which isn't yet enshrined in any articulated policy. This uncertainty needs to be rectified as soon as possible. This new national framework should involve the Department of Defence and other parts of government who work on export controls.

9. Expand the role of education and training within Australia

The coordinated national quantum initiative should include establishing major training hubs for quantum technology in Australia, which will assist the university sector in its post-Covid-19 recovery. This would also help build quantum literacy in Australia and throughout the Indo-Pacific region.

- **Establish a national quantum academy:** The Sydney Quantum Academy is the first step in this direction, and it ought to be expanded to a tightly integrated national quantum academy, providing education and training at all levels to service future demand for quantum technology intellectual capital, both domestically and globally.
- **Build initial education and training partnerships abroad:** With a particular focus on the Indian and Taiwanese markets, establish bilateral partnerships with their emerging quantum sectors and build domestic talent, research expertise and collaboration with the Australian quantum sector.
- **Enter the school sector, building quantum literacy:** Initiate a pilot program that brings together stakeholders from state and federal departments of education, school teachers, students and members of the Australian quantum community to create entry-level educational material that introduces core concepts taught in high-school physics, chemistry, mathematics and computer science through the lens of quantum technology.



Appendix 1: Quantum computing threats to cryptographic systems

In broad terms, there are two types of classical cryptosystem that are commonly used throughout the world for a variety of applications: symmetric-key cryptosystems and public-key (or asymmetric) cryptosystems.

The most commonly known example is one-time pad symmetric encryption. One-time pads are provably secure against any attack (quantum or classical) *if implemented perfectly*: a caveat that's arguably impossible to meet practically and economically. Symmetric-key cryptosystems use the same key to both encrypt and decrypt data. This offers the advantage of more secure message transmission but suffers from the downside of how to distribute keys to both the sender and receiver in a secure manner. For symmetric-key cryptosystems, there are secure protocols against quantum attacks.

Public-key cryptosystems use two separate keys that are mathematically related. One is used for encryption and one for decryption. One of the keys is publicly advertised (for example, a PGP or 'pretty good privacy' key, that some people attach to their email signature), while the other needs to remain completely secret and secure. Public-key cryptosystems are used for the vast majority of encrypted traffic traversing publicly accessible channels, such as the global internet, Wi-Fi, Bluetooth and microwave transmissions. While all public-key cryptosystems work on the same mathematical principles, the most well-known example is the RSA cryptosystem, in which security is based on the difficulty in factoring large composite numbers.

For factoring, the state of the art in classical algorithms remains the general number field sieve. Figure A1 (below) shows the year in which various bit-sizes (L) for the RSA cryptosystem were factored as part of the RSA challenge and an estimate of the computational time needed to factor a specific L-bit number using the scaling of the number field sieve for 100 PCs in 2003 and 2018. Once L becomes bigger than about 1,000, the time needed to complete the computation becomes prohibitively long. Currently, for online encryption, an L of 2,048 is commonplace.

Peter Shor, a professor in applied mathematics at Massachusetts Institute of Technology, completely changed the discussion by showing that a hypothetical (as it was in 1994) quantum computer allowed for a computationally efficient solution to factoring. Finding an efficient quantum algorithm to solve the foundational problems underpinning public-key cryptography opens up an irreconcilable security flaw in these protocols. Regardless of whether you think it will ever be practical to build a quantum computer, the fact that this *fundamental mathematical* result exists is a significant problem: any cryptosystem can't have such a flaw *even in theory*, as this result underpins everything else.

The existence of an efficient algorithm for factoring adds a new curve to the scaling figures. Figure A1 illustrates the importance of the concept of computational complexity or algorithmic scaling. The new curve takes the scaling of Shor's factoring algorithm and overlays the time to break the RSA. As Shor's algorithm is a polynomial algorithm, computational times increase more slowly as the key length increases, compared to the classical number field sieve. Consequently, even key lengths of 10,000 bits or more are factorable in acceptable time frames using quantum computers of moderate to fast physical speed.

The existence of a quantum computer makes public-key protocols such as RSA insecure, as simply increasing key sizes can be easily overcome by a commensurate increase in quantum computing capability.

A potentially more immediate threat is posed by quantum attacks on digital signatures. A digital signature is like an electronic fingerprint appended to data, which proves to the receiver that a document was sent by the signer. It can be done in a completely public manner over the internet. Such signatures are routinely used for financial transactions and have a broad use case for blockchain-enabled technologies such as smart contracts for insurance and cryptocurrency trading. The signature is secured using trusted algorithms such as elliptic-curve cryptography, which make forging by stealing the sender's private key exponentially hard for classical computers. However, due to another quantum algorithm discovered by Peter Shor for calculating discrete logs, quantum computers can quickly hack the message to learn the private key. Such an attack is in fact easier for quantum computers than breaking RSA cryptography, and could be possible within 15 years using around 1 million qubits.[56]

While the theoretical nature of Shor's algorithm poses a security problem for public-key cryptography in a world where quantum computers exist, there's still the practical question of when such machines of sufficient size to threaten current public-key cryptosystems can be built. Errors in quantum computing systems (due to both fabrication and control imperfections) require the use of extensive error correction, which requires more and more physical qubits within the chipset.

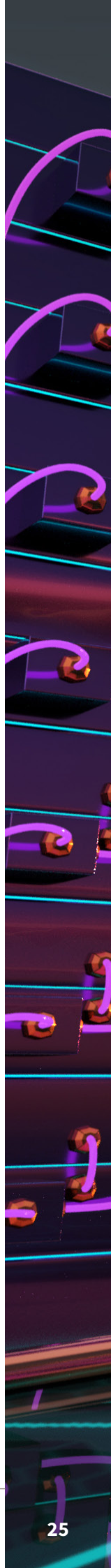
While there's been remarkable progress both from the theoretical perspective (resource costs for Shor's algorithm have dropped by a factor of nearly 1,000 since 2012) and from an experimental perspective (qubit chipsets of approximately 50 qubits with error rates of less than 1% are now possible), there's still a long way to go before a machine of sufficient size to break public-key cryptosystems will be available on any hardware platform.

The current state of quantum computing systems

Blueprints for large-scale quantum computing systems were developed only in the late 2010s, and the current estimate of the resources needed for a fully error-corrected implementation of Shor's factoring algorithm to break RSA-2048 is approximately 20 million superconducting qubits over a computational time of approximately eight hours. This assumes:

- reliable gate error rates for each qubit of 0.1% (this should be achievable in experimental systems in the next 3–5 years)
- significant ability to mass manufacture cheap qubits
- the solution of several major engineering and infrastructure challenges to allow for chip sizes of the order of tens of millions of qubits.

The data that has been presented shows the current state-of-the-art knowledge in the theoretical and experimental space for implementing cryptographic-related protocols on quantum computing systems, but the future is open to speculation. We've focused specifically on Shor's algorithm as it has been the most well-studied and optimised large-scale algorithm of interest to the non-scientific community. It should be noted that shorter timelines are certainly possible, particularly in the case



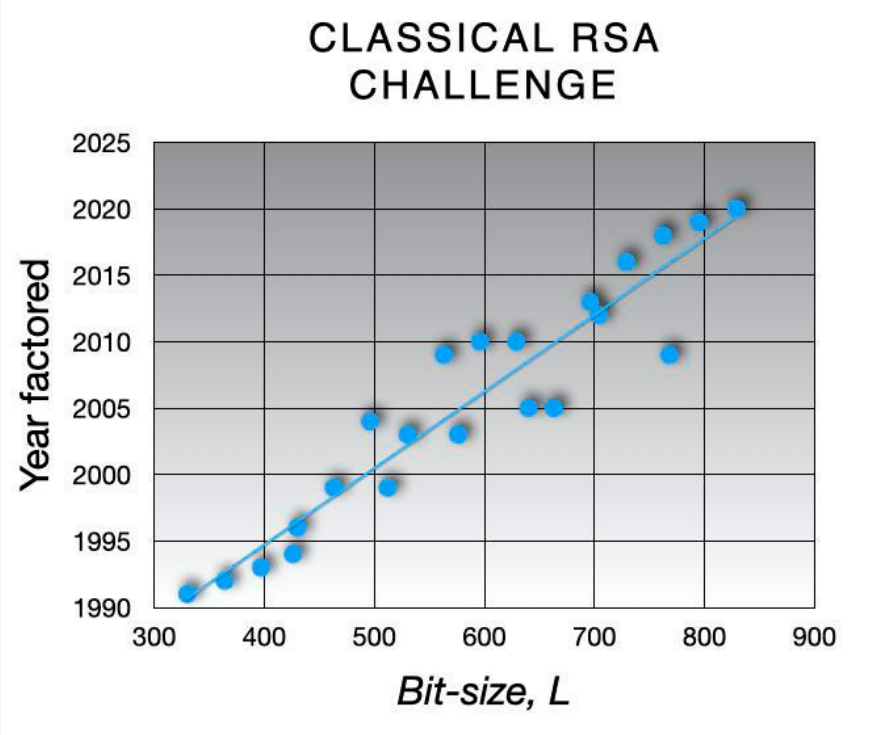
of a quantum-assisted side channel attack. That is, one taking advantage of leaked information in cryptographic transactions, which would require fewer quantum resources than a full-blown Shor attack.

Certainly, quantum system developers are attempting to replicate a type of Moore's law for quantum computing, doubling power every 18–24 months, but it's unclear whether that will eventuate. Consequently, when classical cryptosystems will come under threat from quantum computers is subject to debate; that is, we don't yet know when we'll be able to close the gap between the requirements of breaking RSA-2048 and the size and quality of the chipsets than can be built in the laboratory.

The direct simulation of quantum mechanical systems for use in bioscience, material science and other fields has also been studied in depth. However, the size of a physical machine to provide unambiguous quantum advantage in these spaces is often larger than that of a useful factoring machine.[57]

At the smaller scale, corporations marketing new NISQ-based quantum cloud systems have been aggressive in soliciting the Australian quantum community and other markets in adopting access packages for those systems. This has included the establishment of the University of Melbourne's IBMQ Hub in 2017 to coordinate access to IBM hardware in Australia.[58] The accessibility of these services in Australia and access by Australian researchers will be a critical tool for quantum computing R&D into the future, but we should remain cautious to ensure that diversification in online providers is maintained and that we use these tools to augment Australian R&D efforts, rather than substituting the use of subscription services offered by international corporates for building sovereign capacity in the quantum space.

Figure A1: Estimated times required for RSA factoring on quantum and classical hardware



Source: R. Van Meter, PhD thesis, online, online.

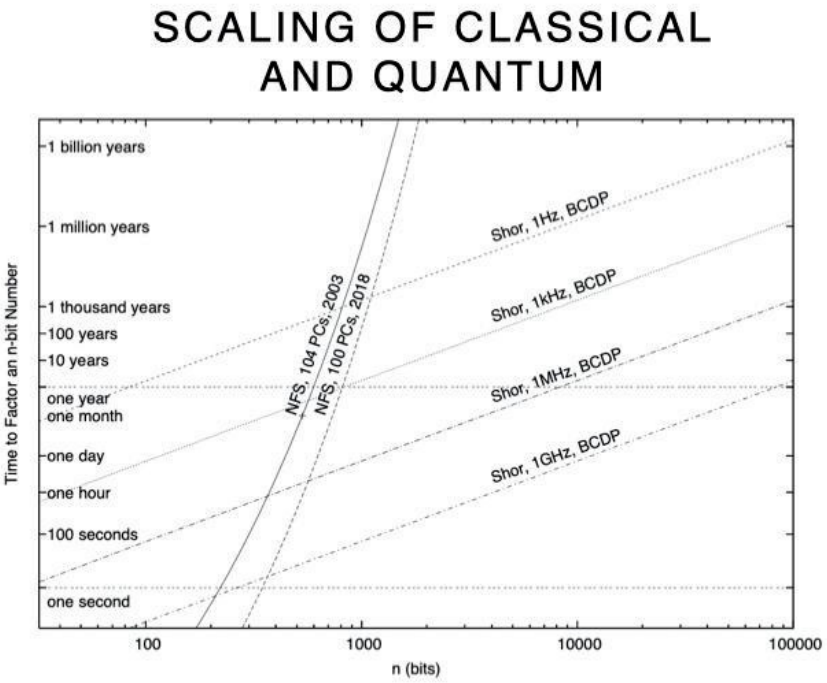
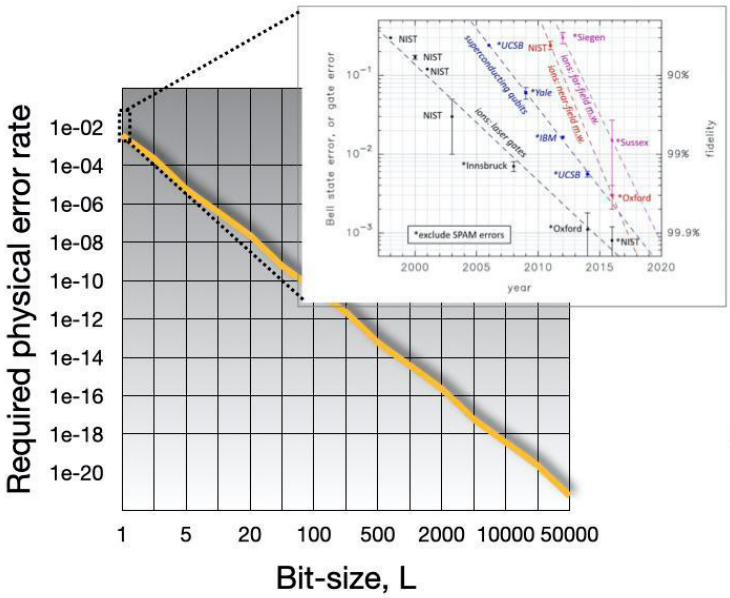


Figure A2: Physical error rates required in quantum hardware to implement Shor's algorithm without active quantum error correction. Insert: historical decreases in qubit error rates from 1996 to 2020.

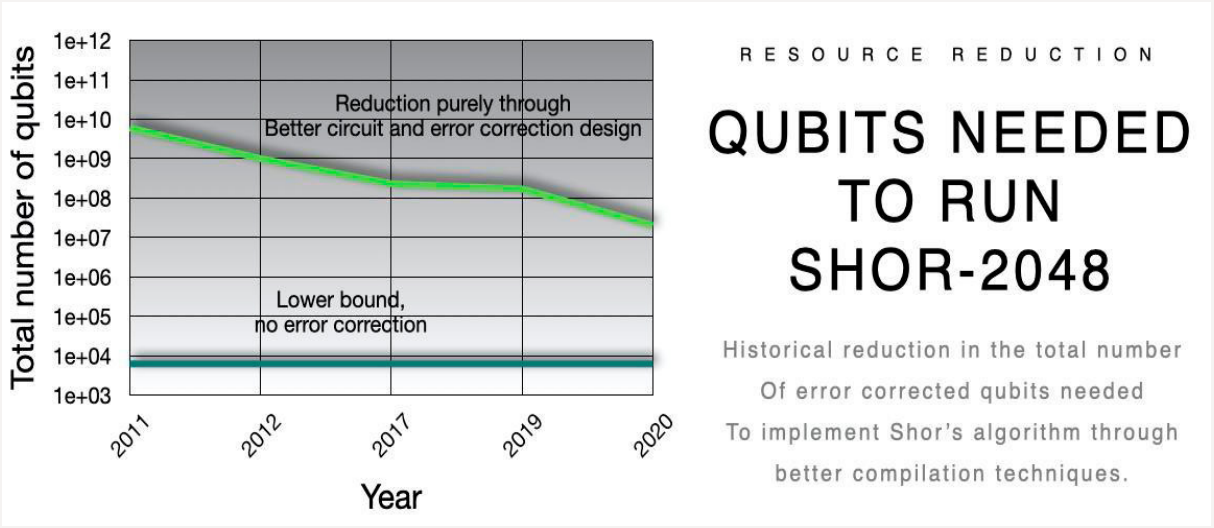


PHYSICAL ERRORS

RATES REQUIRED TO FACTOR

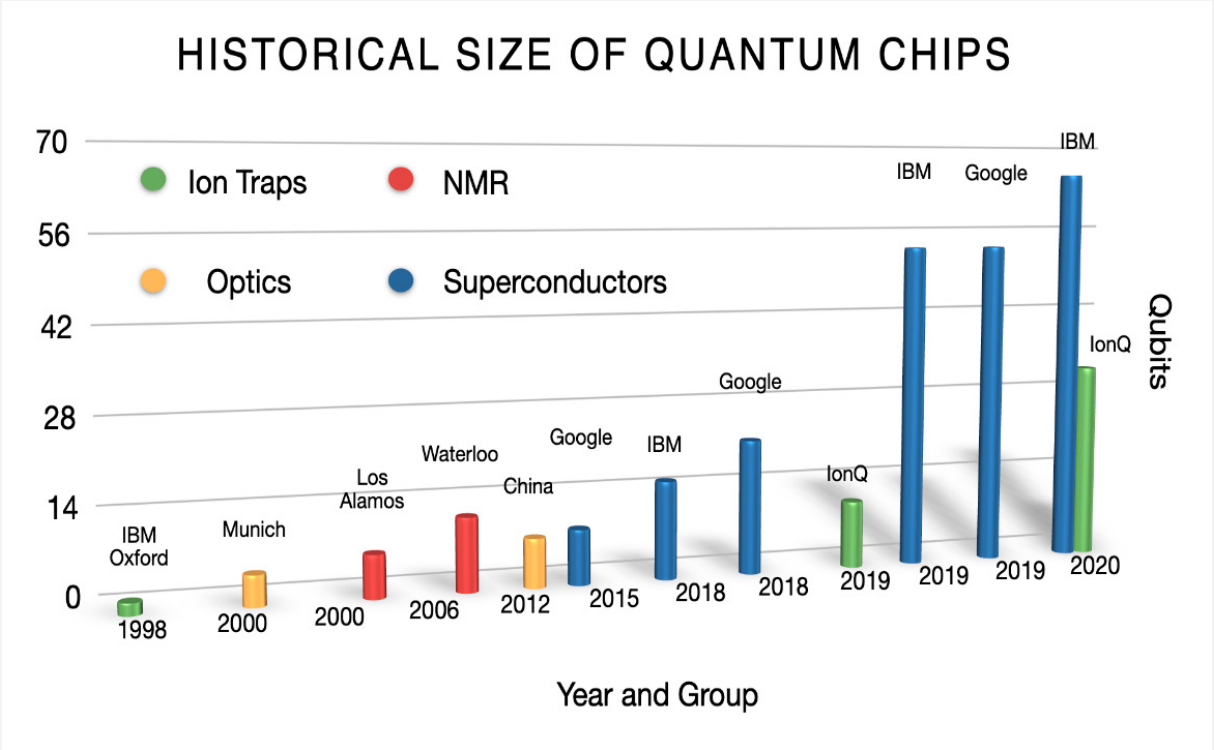
Physical error rates needed to break RSA-L if error correction is not used. Insert: Historical progress in physical Errors

Figure A3: Decrease in qubit resources for Shor's algorithm between 2011 and 2020.



Source: online, online.

Figure A4: Historical demonstration of small qubit chip-sets in four major quantum hardware platforms.



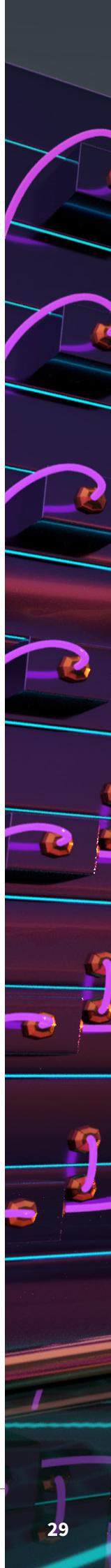
Source: online.

Appendix 2: The status of quantum communications

Quantum communication systems, like their classical counterparts, use several types of hardware. The major ones being developed and deployed worldwide are as follows:

- **Quantum repeater systems:** Unlike classical fibre optics, quantum states can't be copied. Consequently, overcoming losses in fibre optics requires the use of what are effectively mini-quantum computers to relay quantum information at regular intervals across the link.
- **Quantum free space systems:** Developed primarily by researchers in Austria, with prototype systems deployed in the Canary Islands, free space quantum systems work by beaming a particle stream of photons (light particles) from source to receiver using a direct line of sight. Developed as a precursor to quantum satellite systems, free space quantum transmission isn't as aggressively pursued as it once was and might be useful only for 'last mile' type applications in quantum communications.
- **Quantum satellites:** These systems are now the favourite for multiple nations and research groups. Spearheaded by the Chinese Micius platform, launched in 2014, quantum satellites beam either a single particle stream of photons (or a pair of entangled particle streams) to ground stations that can be separated by thousands of kilometres. This platform holds the record for longest distance quantum communications protocols.
- **Quantum memory units (sneakernet):** A new model that's still only theoretical, quantum memory units use the classical principle of sneakernet communications (physically transporting hard drives from point A to point B to achieve a communications link) but overcome the biggest downside of classical sneakernets: long latency times in information transport. Built using the same underlying technology as quantum computers.

The requirements of a quantum communication system are highly dependent on the desired application. The constraints that hardware must satisfy for quantum secured authentication tokens or the distribution of quantum secured keys for symmetric cryptosystems are different from those of a global quantum internet that connects quantum computing systems for distributed computation or blind server/client-based quantum computing. The tendency for people to conflate applications and speak of a quantum key distribution system in the same breath as a quantum internet doesn't reflect the reality of what applications require and what current quantum communications hardware can do.



Notes

1 US$180 billion of Biden's US$2 trillion infrastructure plan is earmarked for technologies of the future like quantum computing. See Martin Giles, *Forbes*, 1 April 2021, online.

2 'AI, quantum R&D funding to remain a priority under Biden', *Wall Street Journal*, 9 November 2020, online.

3 'Fact sheet: President Biden takes executive actions to tackle the climate crisis at home and abroad, create jobs, and restore scientific integrity across federal government', The White House, 27 January 2021, online.

4 This technology stimulus would of course be spread over multiple years.

5 See Germany's June 2020 €50 billion 'future-focused' technology stimulus for an example of how other countries have managed and deployed such technology-focused investments: Eanna Kelly, 'Germany unveils €50B stimulus for "future-focused" technologies', *Science Business*, 4 June 2020, online.

6 Ben Packham, 'PM's department developing list of research, technology to shield from foreign interests', *The Australian*, 12 March 2021, online.

7 See John S Mattick, *Biodata and biotechnology: opportunity and challenges for Australia*, ASPI, Canberra, 27 August 2020, online.

8 MRI = Magnetic resonance imaging.

9 Qubit = A Quantum Bit (Qubit) is the fundamental element of quantum information. Analogous to classical bits, a qubit is formed from two-level quantum mechanical systems such as the spin state of an electron or the polarisation state of a single particle of light—a photon.

10 Rebecca Atkinson, 'Seven Sisters to leverage quantum-based technologies', media release, Seven Sisters, 3 March 2020, online.

11 Jason Palmer, 'Quantum technology is beginning to come into its own', *The Economist*, 2021, online.

12 Jeffrey Lim, PW Singer, 'China is opening a new quantum research supercenter', *Popular Science*, 10 October 2017, online.

13 'China to include quantum technology in its 14th Five-Year Plan', news release, State Council of the PRC, 22 October 2020, online.

14 Moonshot Research and Development Program, 'About', Japan Science and Technology Agency, 2020, online.

15 Matt Swayne, 'Qubit alles: Germany invest 2 billion euros in quantum technology, build two quantum computers', *Quantum Daily*, 15 June 2020, online.

16 Matt Swayne, 'La Monde: France pledges 1.8 billion euros for quantum technologies', *Quantum Daily*, 22 January 2021, online.

17 Yaacov Benmeleh, 'Israel allocates $60 million to build first quantum computer', *Bloomberg*, 3 March 2021, online.

18 Leiden University, '615 million euros awarded to Quantum Delta NL for Quantum research in the Netherlands', HPC wire, 9 April 2021, online.

19 Naomi Xu Elegant, 'A tech firm just recorded the largest first-day jump of any Chinese IPO—924%', *Fortune*, 9 July 2020, online; 'IonQ to become the first publicly traded pure-play quantum computing company', news release, IonQ, 8 March 2021, online.

20 In the case of Silicon Quantum Computing, for example, its funding is obtained through combined investment through UNSW and CQC2T and is still nearly a factor of 5 below the funding level of the most capitalised quantum hardware start-up in the world, PsiQuantum.

21 S Parthasarathy, 'More testing alone will not get us out of this pandemic', *Nature*, 2020. 585(8); T Roberson, J Leach, S Raman, 'Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies', *Quantum Science and Technology*, 2021, 6(2), doi: 10.1088/2058-9565/abc5ab.

22 For an example of one framework see Department of Industry, Science, Energy and Resources. AI Ethics Framework, 2019, online.

23 Commonwealth Scientific and Industrial Research Organisation, 'Growing Australia's quantum technology industry', 2020, online.

24 V Sharma, W Dixon, 'We need to build a quantum security coalition. Here's why', World Economic Forum, 2020, online.

25 R de Wolf, 'The potential impact of quantum 1 computers on society', *Ethics Information Technology*, 2017, 19:271–276; P Ingelsant, M Hartswood, M Jirotka, *Thinking ahead to a world with quantum computers: the landscape of responsible research and innovation in quantum computing*, University of Oxford, 2016.

26 It's expected that the Biden administration will repeal this suspension soon: Daniel Waldron, 'US work visa ban targeted by Biden', *workpermit.com*, 28 January 2021, online.

27 Sydney Quantum Academy, online.

28 National Q-12 Education Partnership, online.

29 T.V. Padma, 'India bets big on quantum technology', *Nature*, 2020, online.

30 Aakriti Bachhawat, Danielle Cave, Jocelinn Kang, Rajeswari Pillai Rajagopalan, Trisha Ray, *Critical technologies and the Indo-Pacific: a new India–Australia partnership*, ASPI, Canberra, 15 October 2020, online.

31 Such as the UTS undergraduate major in quantum information science; the UNSW major in quantum engineering, the Macquarie, Melbourne University and UQ master's program in quantum science; and other similar programs being developed nationwide.

32 Greg Re, 'Tom Cotton suggests Chinese students shouldn't be allowed to study sciences in the US', *Fox News*, 26 April 2020, online.

33 Jeanne Whalen, 'The quantum revolution is coming, and Chinese scientists are at the forefront', *Washington Post*, 19 August 2019, online.

34 Charlie Wood, 'Trump betting millions to lay the groundwork for quantum internet in the US', *CNBC*, 27 April 2020, online.

35 Wood, 'Trump betting millions to lay the groundwork for quantum internet in the US'.

36 HR 6227—National Quantum Initiative Act, online.

37 Lim & Singer, 'China is opening a new quantum research supercenter'.

38 Department of Defence, 'Defence Export Controls', Australian Government, no date, online.

39 TV Padma, 'India bets big on quantum technology', *Nature*, 3 February 2020, online.

40 Paul Nantulya, *Implications for Africa from China's One Belt One Road strategy*, Africa Center for Strategic Studies, 22 March 2019, online.

41 D Aggarwal, G Brennen, T Lee, M Santha, M Tomamichael, 'Quantum attacks on bitcoin, and how to protect against them', *Ledger*, 2018, 3, online; I Stewart, D Ilie, A Zamyatin, S Werner, MF Torshizi, WJ Knottenbelt,. 'Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack', *Open Science*, Royal Society, 20 June 2018, online.

42 In 2016, the National Institute of Standards and Technology issued a call for post-quantum crypto algorithms. Draft standards are expected by 2024: 'Post-quantum cryptography PQC: call for proposals', 3 January 2017, online.

43 'Quantum in the cloud', School of Physics, University of Bristol, no date, online.

44 NISQ refers to quantum algorithms that are small enough to be faithfully executed on near term, low qubit count, high error rate, quantum hardware without the need for resource costly error-correction protocols. While NISQ algorithms exist in principle—quantum supremacy is a quintessential example (see F Arute, K Arya, R Babbush et al., 'Quantum supremacy using a programmable superconducting processor', *Nature*, 23 October 2019, online). An added caveat is that the algorithm needs to be either scientifically viable, commercially viable, or both—quantum supremacy is not. Consequently, NISQ algorithms must be highly compact but still either reach the quantum supremacy regime (where the problem simply can't be solved on any classical computer) or reach the regime where it's more cost-efficient (in either dollars or computational time) to run the algorithm on a quantum computer. NISQ algorithms satisfying the commercial or scientific viability condition are under active research, but don't currently exist. See also John Preskill, 'Quantum computing in the NISQ era and beyond', *Quantum*, 6 June 2018, 2:79, online.

45 Shiyin Chen, 'Chinese scientists claim breakthrough in quantum computing race', *Bloomberg*, 4 December 2020, online.

46 Hamish Johnston, 'Quantum cryptography network spans 4600 km in China', *Physics World*, 7 January 2021, online.

47 Aerospace Security, 'Space launch to low Earth orbit: how much does it cost?', Center for Strategic and International Studies, no date, online.

48 Johnston, 'Quantum cryptography network spans 4600 km in China'.

49 Wood, 'Trump betting millions to lay the groundwork for quantum internet in the US'.

50 Note: This could be in a similar vein to a 2020 initiative by the UK Government for a A$13.7 million program to develop a British quantum operating system. See Leonie Mueck, 'Riverlane to build radically new operating system for quantum computers', news release, River Lane Research Ltd, 14 May 2020, online.

51 See Mattick, *Biodata and biotechnology: opportunity and challenges for Australia*.

52 The biocentre precinct in Melbourne has received $2.8 billion in Victorian Government investment in the past decade, has generated more than A$12 billion in economic activity and has secured A$14 billion of private R&D investment. The precinct claims that 53% of all ASX-listed life-sciences companies are based in Melbourne and that the precinct attracts 40% of all Australian medical research funding, driven in part by a $0.45 on the dollar tax incentive for corporate R&D expenses conducted within the state.

53 For further discussions on some of these topics see, for example: James Eyers, 'Australia can win war for tech talent: Afterpay boss', *The Australian Financial Review*, 11 February 2021, online. Michael Bailey, Paul Smith, 'Fix R&D, visas if you want to help tech, PM told', *The Australian Financial Review*, 25 June 2019, online.

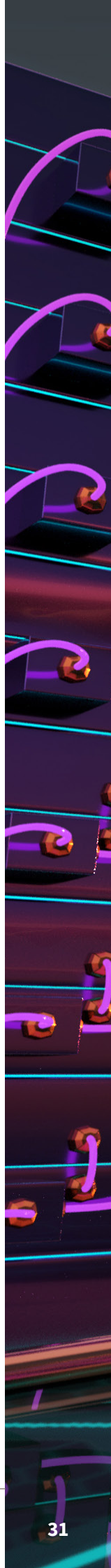
54 State Department, 'Tokyo Statement on Quantum Cooperation', US Government, 19 December 2019, online.

55 Dr Robert Clark AO, Professor Stephen Bartlett, Professor Michael Bremner, Professor Ping Koy Lam, Professor Timothy Ralph, 'The impact of quantum technologies on secure communications', The Australian Strategic Policy Institute, 20 April 2021, online.

56 Aggarwal et al., 'Quantum attacks on bitcoin, and how to protect against them'.

57 Vera von Burg, Guang Hao Low, Thomas Häner et al., 'Quantum computing enhanced computational catalysis', Microsoft, July 2020, online.

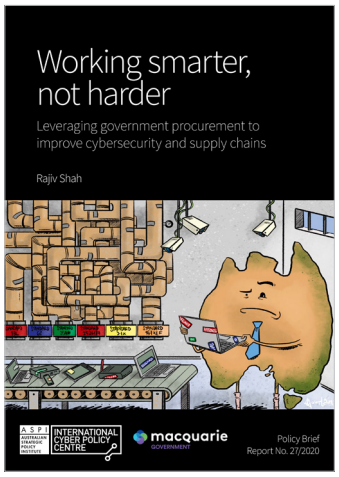
58 'University of Melbourne collaborates with IBM to accelerate quantum computing', news release, University of Melbourne, 20 December 2017, online.

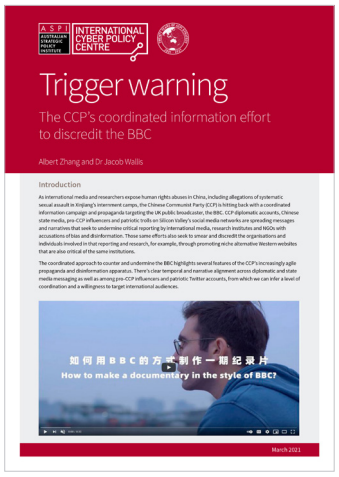


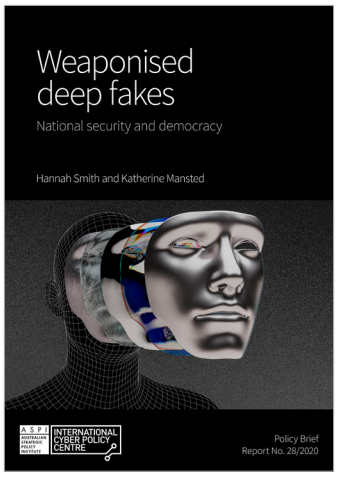
Acronyms and abbreviations

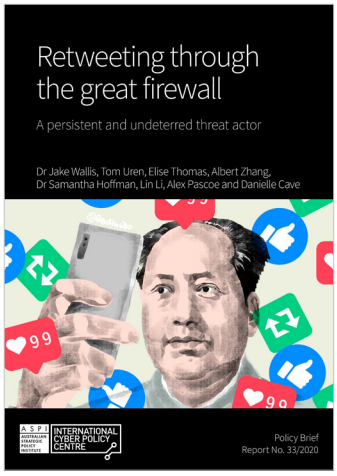
ARC	Australian Research Council
CoE	centre of excellence
CQC2T	Centre of Excellence for Quantum Computation and Communication Technology
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DFAT	Department of Foreign Affairs and Trade
DISER	Department of Industry, Science, Energy and Resources
EQUS	Centre of Excellence for Engineered Quantum Systems
EU	European Union
GPS	Global Positioning System
IED	improvised explosive device
IT	information technology
ML/AI	machine learning and artificial intelligence
NISQ	noisy intermediate scale quantum
PM&C	Department of the Prime Minister and Cabinet
QKD	quantum key distribution
QUESS program	Quantum Experiments at Space Scale program
R&D	research and development
RMIT	Royal Melbourne Institute of Technology
SQA	Sydney Quantum Academy
UK	United Kingdom
UNSW	University of New South Wales
UTS	University of Technology Sydney

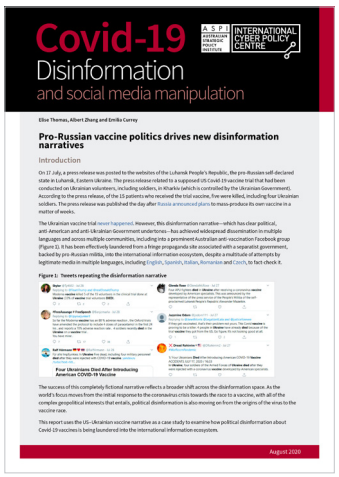
Some previous ICPC publications

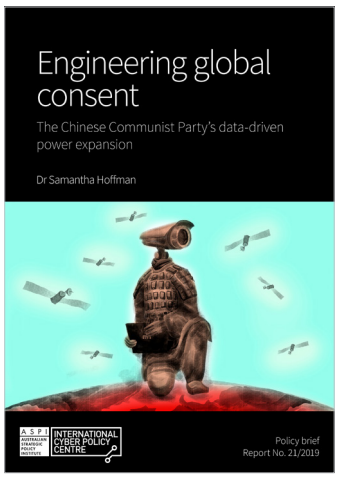


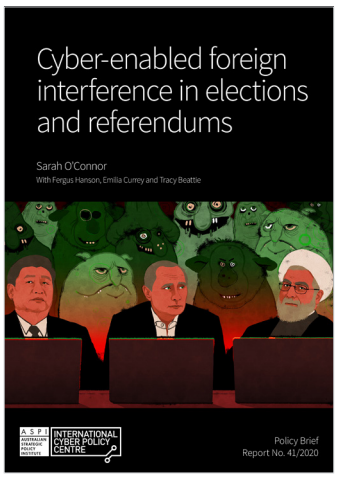












ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021