Appendix A – Australia's quantum regulation and policy[1, 2]

Currency date 1 September 2024

Table of Contents

---

[1] Prepared by Natarsha Wong with contributions from Jennifer Westmorland, UNSW Allens Hub for Technology, Law & Innovation.

[2] Appended to Lloyd-Jones, Susanne and Kayleen Manwaring, '[Quantum Resilience in the Australian National Security Legislative Framework]' (Policy Brief, Cyber Security Cooperative Research Centre, UNSW Faculty of Law & Justice, September 2024)

1 Australia on Quantum Strategy and Policy

1.1 What has Australia done to date on Quantum strategy and policy?

In the past, Australia, in relation to quantum, was largely focused on research carried out by universities and centres of excellence.[3] There was no clear national strategy for quantum development and Australia was lagging behind on quantum investment, outpaced by China, US, France, Germany, the EU, India and Russia.[4]

In the past decade, notable investments into research include $10M investments each from the Commonwealth Bank and Telstra in the ARC Centre for Quantum Computation and Communication Technology, a centre of excellence with 170 researchers from 6 affiliated universities working across both optical and silicon quantum computing and secure communications.[5] Telstra's pledge followed the federal government's promised $26M as part of the of $1.1B National Innovation and Science Agenda.[6]

In 2018, a $6M investment was announced for industry, academia and government research agencies for quantum development for Defence. [7] This is a very small portion of the total $730M Next Generations Technologies Fund dedicated to ADF development which indicates that the potential for quantum was not nearly appreciated to the extent that foreign states had with their billion-dollar investments.[8]

It was announced in 2021, that Australia would invest $111M in quantum technology and form a new security alliance with the UK and US ('AUKUS') which involves greater security cooperation including the use of quantum technology with the aim of protecting Australia

[3] Gavin Brennen et al, 'An Australian Strategy for the Quantum Revolution' (May 2021) <http://www.aspi.org.au/report/australian-strategy-quantum-revolution>.
[4] Ibid.
[5] 'Commonwealth Bank Invests $5m in Quantum Computing | Australian Research Council' <https://www.arc.gov.au/news-publications/media/research-highlights/commonwealth-bank-invests-5m-quantum-computing>; 'Telstra Matches $10m CBA Pledge for Quantum Computer Race | Australian Research Council' <https://www.arc.gov.au/news-publications/media/research-highlights/telstra-matches-10m-cba-pledge-quantum-computer-race> ('*Telstra*').
[6] *Telstra* (n 3).
[7] '$6 Million Injection into Quantum Technologies Research | Defence Ministers' (2018) <https://www.minister.defence.gov.au/media-releases/2018-01-25/6-million-injection-quantum-technologies-research>.
[8] Ibid.

from China's cyber capabilities.[9] Since then, Australia has committed $15B to establish the National Reconstruction Fund under which $1B has been allocated to critical technologies including quantum technology.[10] The commitment to increasing funding for critical technologies suggests Australia is wanting to be a player amongst other powers in the global quantum field.

1.2 How is Australia approaching quantum technology in strategy and policy?

Recently, there has been increasing recognition of the need to harness the potential of critical emerging technologies ('CETs'), such as quantum, for Australia's competitiveness and economic growth.[11] The Australian Government 'predicts that growing Australia's quantum industry has the potential to add $4 billion and 16,000 new jobs to the economy by 2040'.[12] This $4B contribution in areas of computing, sensing and communications is a relatively small portion of the predicted $86B revenue for the quantum technology global market by 2040.[13] However, Australia's move into quantum is necessary to not fall further behind other global powers and there must be a 'national conversation … about having a coordinated, collaborative, and cooperative approach to growing our domestic quantum economy', said CSIRO Chief Scientist Cathy Foley.[14]

The Government has started releasing reports on the 'National Quantum Strategy', the Government's long-term plan to grow the quantum industry in Australia and to take advantage of quantum technologies.[15] The strategy aims to champion responsible innovation and ensure the growth of Australia's quantum industry supports economic prosperity whilst safeguarding our national interests.[16] There are 3 overarching themes for the strategy: 1) research and development; 2) investment, commercialisation and industry growth; 3) skills, social licence and diversity.[17]

1) Research and Development

Research and development involves building on research and Australia's global leadership, ensuring universities can attract and retain the best international quantum talent, promoting collaboration between universities, and improving domestic and global collaboration between research and industry.[18]

2) Investment, Commercialisation and Industry Growth

[9] Mike Cherney, 'Australia to Beef Up High-Tech Prowess After Security Pact With U.S. American Ally Says Quantum Science Has Commercial, Defense Uses', *Wall Street Journal* (Online) (New York, N.Y., United States, online, 17 November 2021) <https://www.proquest.com/docview/2597974273/citation/6756D0BD728E451EPQ/1>.

[10] Ibid. This information is taken from CN's note on Zotero from the source in (n 7).

[11] 'Critical and Emerging Technologies | Standards Australia' (Undated) <https://www.standards.org.au/engagement-events/strategic-initiatives/critical-and-emerging-technologies#quantum-position-paper-id> ('*Critical and Emerging Technologies*').

[12] Ibid.

[13] Judy Meiksin, 'Australia Launches Quantum Industry Roadmap' (2020) 45(12) MRS Bulletin 987.

[14] Ibid 987.

[15] *Critical and Emerging Technologies* (n 9); Department of Industry, Science and Resources, 'National Quantum Strategy | Department of Industry, Science and Resources', https://www.industry.gov.au/node/92447 (Strategy or plan, 3 May 2023) <https://www.industry.gov.au/publications/national-quantum-strategy> ('*National Quantum Strategy*').

[16] Ibid.

[17] Department of Industry, Science, Energy and Resources, *National Quantum Strategy Issues Paper* (Issue Paper, April 2022) <https://storage.googleapis.com/converlens-au-industry/industry/p/prj1e4a0f14eea028ef41a8c/public_assets/DISER%20National%20Quantum%20Strategy%20Issues%20Paper.pdf>.

[18] Ibid.

Australia must develop and coordinate a national vision for quantum technology.[19] Investment must also be fostered by removing barriers and attracting investment for early stage companies.[20] Commercialising research and freeing up university intellectual property, a greater movement between academia and industry, creating infrastructure for commercial development and incentivising creation of shared infrastructure in Australia are also crucial to bolstering industry growth.[21] Furthermore, lowering barriers of entry for start-ups, creating conditions to support a sustainable quantum ecosystem, creating quantum standards, and using a holistic approach to create a full tech stack for quantum including algorithms and software should be considered in Australia's strategy.[22] On a global scale, Australia should leverage existing government partnerships with trusted global partners to foster relationships between researchers and domestic companies, consider advantageous supply chain options internationally and domestically, navigate regulations related to foreign investment and export of critical or dual-use technology, identify Australian quantum applications and boost demand for Australian-made quantum technologies domestically and abroad.[23]

3) Skills, Social Licence and Diversity

It is also important to attract and retain expertise within Australia.[24] A Global Talent visa program is a means to attract international talent.[25] To foster the next generation of quantum leaders domestically, Australia can seek to improve the attraction of students into quantum fields, address skill gaps, build quantum literacy in universities and TAFE, and introduce quantum use in regional and rural communities.[26] On a broader level, increasing awareness of quantum technology and building social licence should be pursued.[27] Diversity in skill and background in the quantum field should also be encouraged.[28]

Additional suggestions for Australia's quantum strategy include appointing a Minister for Critical and Emerging Technologies who would work across relevant economic, national security, industry, research, defence and science agencies in public service and expanding the Critical Technologies Policy Coordination office to 'National Coordinator for Technology'.[29]

1.3 What <u>competition/competing interests</u> are mentioned/raised/identified in Australia's quantum strategy and policy?

1.3.1 Geopolitical Competition

To date, investment in quantum technology initiatives in Australia is lacking compared to other foreign powers including the UK, US, EU, India, Germany and Russia, which have made multibillion [AUD] dollar investments, and China which was reported in 2020 to have allocated approx. $10B [USD] towards quantum research and development.

The Australian Strategic Policy Institute ('ASPI') identified 3 major ways how quantum could reshape geopolitical strategy.

A) National Security, Defence and Intelligence

---

[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Brennen (n 1).

Quantum computing and communications technologies have been classified as having the potential to pose significant national security, defence and intelligence threats. Furthermore, quantum developments in China and the US have been carefully noted by both China and Western allies.[30]

B) Regional Powers

Quantum sensing technologies, including quantum magnetometers and quantum gravimeters, also have the potential to 'tip the balance between regional powers' through improved defensive/offensive capabilities and the ability to outcompete nations by harvesting raw materials more efficiently.[31]

C) Disruption of Digital Economies

The potential of quantum cryptography developments also extends to the ability for quantum computers to attack the digital signatures used to secure cryptocurrency transactions between untrusted parties which could allow a malicious agent to steal crypto tokens like bitcoin undetected.[32]

Given the risks of the potential applications of quantum technology and the potential for quantum to provide a competitive advantage, countries must balance how to 'optimise for international development of [quantum] while subject to geopolitical constraints on collaboration'.[33] In Australia, 'Guidance Note 8 - National Security' was proposed, a rule which requires international collaboration be approved by the Australian Government's Foreign Investment Review Board ('FIRB'), the regulator overseeing foreign investment and joint foreign economic activities in Australia.[34] This rule will be further explored later. Some argue that excessive governance responses would excessively hinder research and development.

Although, as the ASPI posits, 'the chance of any country being able to make a decisive technical breakthrough and then being able to productionise it as an operational system, all the while quarantining it from competitors, seems remote'.[35] Many transformative technologies of the future

> aren't held entirely —or even mainly—within government circles. Quantum technologies are under development in universities and commercial firms around the world … In some cases, such as quantum computing, the scale of investment by the global commercial IT industry swamps government efforts … Because of the globalisation and commercialisation of research efforts, we judge that advantages that any player can generate will tend to be ephemeral, and the rate of diffusion of breakthrough technologies to other players could be quite rapid.[36]

1.3.2 Commercial Competition

The size of the quantum computing market is expected to reach $1.9B by 2023 and grow to $8B by 2027.[37] On a commercial level, most focus is on the race to launch the first large-scale universal industrial quantum computer.[38] Players in the race include computing giants

[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Elija Perrier, 'The Quantum Governance Stack: Models of Governance for Quantum Information Technologies' (2022) 1(3) Digital Society 22, 11.
[34] Perrier (n 31).
[35] Australian Strategic Policy Institute, 'From Little Things: Quantum Technologies and Their Application to Defence', 19 ('From Little Things').
[36] Ibid.
[37] Sukhpal Singh Gill et al, 'Quantum Computing: A Taxonomy, Systematic Review and Future Directions' (2022) 52(1) *Software: Practice and Experience* 66.
[38] Ibid 2.

such as IBM, Microsoft, Alibaba, Intel and Google, dedicated quantum enterprises such as D-Wave, and start-ups such as Rigetti Computing, NVision Imaging Technologies and IonQ.[39] Research and development efforts to commercialise industrial quantum computers are seeing

> continuously increasingly leading contributions from US and other prominent efforts coming from the EU quantum technologies flagship and the UK national quantum technologies program, the Australian Centre for Quantum Computation and Communication Technology (CQC2T) and the Chinese quantum national laboratory for quantum information science.[40]

Professor Michelle Simmons[41] described global competition as 'the case of the tortoise and the hare. We very much see ourselves as a tortoise in this game.'[42] Simmons notes quantum systems that use the superconductor platform, such as Google's and IBM's, will run into problems during scale-ups because of this. She believes she can be a tortoise in the commercial race because her start-up company develops atomically engineered qubits which provide the benefit of being able to engineer 'each aspect of the actual device itself. This allows us to focus on generating the best quality qubits, the lowest noise qubits, and the fastest qubits'.[43]

Not only is there a race to build a scalable quantum computer, but there is also an intense competition to achieve the

> first quantum computing application which solves a useful real-world problem that is intractable on classical computers – also known as "quantum advantage". To achieve this feat, significant progress in both error-corrected quantum hardware and quantum algorithm development will be required in the coming years.[44]

1.3.3 Commercial Interests vs Public/Community Interests

In relation to the flexibility or stringency of standards, competing interests do exist between commercial interests and broader public or community interests. Flexibility may be preferred in areas that provide commercial benefits to avoid 'encroaching on commercial IP and competitiveness', and more stringent standards may be preferred 'in defining rigorous, expert-driven performance standards, such as for comparative benchmarking and quality assurance processes'.[45]

2 Specific Technologies and Applications of Quantum

2.1 What technologies are mentioned in Australia's quantum strategy and policy? Is there consideration of the impact of quantum computing and quantum communications?

In this context, quantum refers to quantum information technologies ('QIT') which are principally quantum computing, communication and sensing because they are 'fundamentally characterised by their informational processing properties'.[46]

---

[39] Ibid.
[40] Ibid 31.
[41] Michelle Simmons is a Scientia Professor and Australian Research Council (ARC) Laureate Fellow at the University of New South Wales, Sydney, director of the Centre of Excellence for Quantum Computation and Communication Technology at ARC, and the founding director of startup company Silicon Quantum Computing Pty. Ltd. (SQC).
[42] Meiksin (n 11).
[43] Ibid.
[44] Gill et al (n 35) 2.
[45] Nathan K Langford and Simon J Devitt, 'At the Intersection Between Scalable Quantum Computing and Standardisation'.
[46] Perrier (n 31).

2.1.1 Quantum Computing

There have been significant developments in quantum computing. However, more research is required in quantum hardware development, software development, algorithm development (eg Grover's, Shor's, Variation Quantum Algorithms, Algebraic, search, variational), quantum machine learning, error correction on Noisy Intermediate Scale Quantum ('NISQ') devices and applications, quantum control, adiabatic quantum computing, fault-tolerant quantum computing, quantum programming languages and systems, simulation software for quantum experiments and quantum simulators.[47]

It is important to note that 'quantum supremacy', which 'implies solving a problem on a quantum computer which is intractable on any classical machine', has been demonstrated.[48] Research is ongoing to find practical problems that can be efficiently solved on quantum computers.[49] 'Quantum supremacy' is to be distinguished from 'quantum advantage', which has a practical element, implying solving a useful real-world problem that cannot be efficiently solved on a classical computer.[50]

Whilst algorithms such as Grover's and Shor's exist which can provide computational advantage for any problem of use (eg faster, more detailed modelling from weather forecasts to radar system simulations) and can demonstrate 'quantum supremacy', a machine capable of running the algorithm requires at least 1 million physical qubits.[51] The current record is IBB's 433 qubit processor.[52] Error correction is also required to create a universal, fault-tolerant quantum computer. Whilst errors in small-scale quantum computers can be manageable, when scaled up it becomes much more difficult.[53] Optimists suggest it is possible given the existence of promising prototypes which have performed simple calculations, however, pessimists recognise the practical difficulties and point to decoherence as the main issue.[54] Although there is no guarantee of success, the potential impact is too significant and there is enough promise in current work to make the pursuit worthwhile.[55]

If fault-tolerant scalable quantum computers are achievable, these computers would only be in large-scale industrial setups within universities, industry or governments, rather than being ubiquitous or available as portable devices, since large-scale investment and considerable infrastructure are necessary.[56] As Perrier states:

> This underlying mode of production for QIT then affects who may access QIT resources and how such access would be governed and monitored for example … In industry, access to superior computational capacity would provide in principle (certeris paribus) firms with a competitive advantage.[57]

Quantum computing would have applications in numerous domains including chemistry, physics, biology, engineering, industrial chemical development, clean energy, energy management, weather and climate modelling, drug design, data science, quantum-assisted machine learning, electronics material discovery, financial modelling, quantum-based

---

47 Gill (n 35).
48 Ibid 28.
49 Ibid.
50 Ibid.
51 Langford (n 43).
52 'IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two', *IBM*, (Web Page, 9 November 2022) <https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two>.
53 'From Little Things' (n 33).
54 Ibid.
55 Ibid.
56 Perrier (n 31).
57 Ibid 7-8.

portfolio-risk optimisation, fraud detection and robotics.[58] On the other hand, as Gill et al identify, 'several other areas such as encryption, communications, financial transactions, critical infrastructure, Blockchain and cryptocurrency are some of the applications which are bound to become vulnerable by the development of an industrial quantum computer'.[59] Applications in decryption will be explored further later. It is also worth noting that compared to supercomputers, quantum computers consume less energy. This means 'processing data intensive problems by quantum machine learning algorithms can reduce down energy cost, and the dependency on fossil-fuels will decrease'.[60]

2.1.2 Quantum Communication

Quantum communication includes quantum cryptography to secure communications, quantum-based satellite communication and potentially quantum internet. Using quantum key distribution ('QKD'), which is based on quantum mechanics' physics, is cryptographically secure because 'the eavesdropper can interfere with the communication of the key, but can't steal it'.[61] The method is intended to be secure from decryption by classical computers and quantum computers. However, a limitation of quantum communication is that decoherence presents a greater challenge in interfering with the transmission of qubits along fibre-optic cables of greater distances.[62] A cable length of 250km is considered a significant achievement.[63]

In Australia in 2013, the quantum network project was established to connect Parliament House with other government organisations in Canberra.[64] Progress has been made in the US, Germany and China with China appearing ahead of the field in quantum key exchange systems creating the world's first quantum communication satellite in August 2016.[65] China has also been successful in creating a ground-to-space-to-space-to-ground link between two ground stations over 1,400km apart in central and western China.[66] A global quantum communication network rollout could potentially form a 'quantum internet' although this would be more difficult to set up and maintain than classical channels.[67] Due to extra overheads, large-scale quantum communications are unlikely to replace classical communication channels except in specialised applications, such as high-level military or diplomatic communications, where absolute security is required and relatively small volumes of data are involved.[68]

Given there are many cryptographic systems in use today with some being 'quantum' proof, the ASPI does not see quantum communication as a 'game-changer' but as a 'conservative' technology that will 'help preserve existing practices by future-proofing them against developments in cryptography'.[69] The ASPI also interestingly points out that China leading the push for operational quantum communication systems is unsurprising as it could allow China 'to offset the likely advantage the US has in cryptanalytic techniques'.[70]

[58] Gill (n 35).
[59] Ibid 29.
[60] Ibid 2.
[61] 'From Little Things' (n 33) 6.
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid 7.
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Ibid.

2.1.3 Quantum Sensing

There are several applications of quantum sensing technologies in the areas of defence and science as the technologies provide the ability to measure electric and gravitational fields, temperature, pressure, pollutant or chemical levels more accurately.[71] Applications include airport security, hydrographic surveying, battlefield medicine and nonproliferation compliance.[72]

The following technologies are of interest:

A) Quantum Radar

Two approaches to quantum radar have been identified. Firstly, interferometric which targets images more clearly and further away.[73] This method, however, may not be reliable for stealth platforms.[74] On the other hand, the entanglement method, the second approach, is potentially sensitive enough to offer counter-stealth capabilities, but is harder to realise due to numerous practical constraints and there is a base of scepticism in the broader scientific community.[75] However, this scepticism has not stopped interested major players in the US, China and Europe with research being driven by a small community constituted of private, governmental and academic participants.[76] Beyond defence, the greatest use case of quantum radar may be in space.[77]

B) Atomic Clocks

The atomic clock is the most accurate clock and has applications in defence and space.[78]

C) Quantum Magnetometers

Quantum magnetometers ('SQUIDs') precisely measure magnetic fields.[79] However, there lies several practical difficulties when used for defence purposes.[80] SQUIDs may be better utilised for medical imaging with commercialized 'NV diamonds', battlefield medicine or magnetic navigation.[81]

D) Inertial Navigation Systems

Inertial navigation systems are precise navigational systems and can compensate for loss of GPS guidance if GPS signals are jammed.[82]

Whilst quantum sensing technologies can significantly improve defence capabilities, such as with inertial navigation systems which are a potential countermeasure to GPS jamming, the 'measure-countermeasure battle will continue'.[83] The ASPI notes that quantum sensing technologies 'mostly improve existing capabilities without offering novel ones' and suggests quantum computing has more potential to provide breakthroughs.[84] Although, developments in quantum sensing will 'make it easier to build quantum systems that underlie quantum computers and communication relays'.[85]

71 Ibid.
72 Ibid.
73 Ibid.
74 Ibid.
75 Ibid.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid.
80 Ibid.
81 Ibid.
82 Ibid.
83 Ibid.
84 Ibid.
85 Ibid.

2.2 Does Australia's approach to quantum consider/mention quantum-safe encryption and quantum cryptography? What does Australia's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?

In this section classical cryptography, quantum cryptography and post-quantum cryptography will be discussed.

2.2.1 Classical Cryptography

Quantum computing has the potential to decrypt classically encrypted information, depending on the standard used. Shor's algorithm, developed in 1994, can, in principle, break the operational RSA encryption if a large-scale fault-tolerant quantum computer were developed.[86] The current de facto standard for symmetric (or private-key) encryption is the Advanced Encryption Standard (AES), is vulnerable for shorter key lengths (such as AES-128) but where lengths are substantially increased are likely to be quantum-resistant, at least in the medium-term.[87] However, 'regardless of key length, the future of … Rivest-Shamir-Adleman (RSA) is bleak'[88] in the face of successful quantum computing. RSA is an asymmetric (or public key) algorithm that is vulnerable to quantum attack, as is the popular alternative Elliptic Curve Cryptography (ECC).[89] Therefore 'post-quantum encryption methods need to be formulated which can withstand an industrial quantum computer'.[90] The ability to decrypt classically encrypted data would have significant impacts as

> classical encryption is at the bedrock of modern economies and national security apparatuses: financial transactions, credit card transactions, data security etc. all rely upon the inability of classical computers to decrypt (within any meaningful timescale) data that has been encrypted.[91]

This is where quantum and post-quantum cryptography comes in as both methods potentially provide options for quantum-safe encryption.

2.2.2 Quantum Cryptography

As previously discussed, quantum cryptography provides an option for quantum-safe encryption as quantum mechanics' physics is used which cannot be decrypted by quantum computers. Major applications of quantum cryptography include

> dense coding, teleportation, prime factorization, faster and secure database searching, secure secret sharing, secure processing, secure one-to-one communication, secure communications across public networks using a quantum smart card and security for cloud and e-commerce computing environments.[92]

2.2.3 Post-quantum Cryptography

Post-quantum cryptography uses mathematical techniques, similar to classical cryptography, however, these mathematical problems are much more difficult and are able to withstand quantum computing attacks.[93] Applications of post-quantum cryptography range from government-use to secure identify proofs, in information and communication

---

[86] Gill (n 35) 29.
[87] Georgia Wood, 'Encryption Security for a Post Quantum World | Strategic Technologies Blog | CSIS' (6 February 2022) <https://www.csis.org/blogs/strategic-technologies-blog/encryption-security-post-quantum-world>.
[88] Ibid 17.
[89] SCHRÖDINGER, 'Quantum Computing Breakthrough Could Crack ECC Cryptography, Exposing Internet Secrets Claims PsiQuantum Researcher' (20 June 2023) *Quantum Zeitgeist* <https://quantumzeitgeist.com/quantum-computing-breakthrough-could-crack-ecc-cryptography-exposing-internet-secrets-claims-psiquantum-researcher/>.
[90] Ibid 29.
[91] Perrier (n 31) 8.
[92] Gill (n 35).
[93] Ibid.

technologies including networks, networking equipment, servers and network services (eg cloud services), and automation in healthcare, vehicles, agriculture and aviation.[94] Whilst there are significant benefits, challenges must be considered which include security challenges, hardware challenges, performance and cost-related challenges and quantum-related design challenges.[95] Cryptographic agility, 'a design feature that enables future updates to cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure',[96] must also be strongly considered.[97] Legacy devices must either (1) have their software rebuilt; (2) be redesigned and their communications wrapped in a quantum-resistant 'envelope'; (3) replaced; or (4) the risk assessed, analysed and accepted of its data or the device itself being used as an attack vector.[98] It is crucial to study the 'trade-offs between delay, security, and information rate', remembering that 'high computational and communicational rates without scarifying security are the aim'.[99]

Gill et al, also highlight the importance of formalising a wide array of standards in order to adapt to post-quantum cryptography transition in real-time applications such as 'integration with banking, remote learning, mobile communications, healthcare, and other emergency services, and critical infrastructure'.[100]

3 Governance

3.1 Does Australia's approach to quantum mention any specific regulatory or legal frameworks? If so, which frameworks? If so, what is the predicted impact of quantum on those frameworks? If so, does the approach outline any possible solutions?

Perrier, on governance, states that 'governance can cover a variety of formal and informal instruments involving complex interconnections among law, regulation, normativity, institutional practice, risk management and discursive power'.[101] Governance should also recognise the 'need to treat fostering innovation and QIT (quantum information technology) development as an explicit goal of governance themselves'[102] whilst acknowledging that regulation is necessary, despite uncertainty over the future of development, to avoid harmful norms being too deeply ingrained.

Whilst standards development on quantum is nascent and specific quantum regulation has yet to be developed, 'QIT is not emerging into a governance vacuum: a variety of well-established responses exist across the governance landscape'.[103] Quantum governance must be considered within the broader nexus and hierarchy of technology governance in general.[104] This allows us to see how existing governance instruments could relate to quantum technologies or what, if any, novel governance responses are required to meet

---

94 Ibid 17.
95 Ibid 18.
96 Joseph R Biden Jr, 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' *National Security Memorandum/NSM-10* (24 May 2022) https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
97 Gill (n 35) 35.
98 Warren Armstrong, 'SOCRATES WP8 – Request for feedback – DRAFT quantum policy brief' Email to authors, sent 15 Jan 2024.
99 Ibid.
100 Ibid.
101 Perrier (n 31) 3.
102 Ibid 40.
103 Ibid.
104 Perrier (n 31).

policy objectives.[105] We must also consider how quantum technology sits in intellectual property regimes.[106]

Perrier argues that novel governance that is quantum-specific is likely needed because of i) economic rationales, ii) protection of stakeholder rights, and iii) regulation for the maintenance of order. Quantum-specific regulation can be more actionable and help stakeholders realise quantum use and development are governed already.[107] Although, governance methods must be empirical – dynamic and responsive to the evolution of the technology.[108]

Furthermore, Perrier considers governance in a dual manner. Perrier sees governance as including positive objectives in the form of a duties and right-based approach and advocates for moral and ethical principles, such as 'principles of social benefit, accountability and transparency, equity and access, harm-minimisation', to be embedded within formal and informal instruments of governance.[109] He also sees governance as managing and responding to negative risks in the form of a risk-management approach.[110] Overall, there must also be a balance between prescriptive and principles-based approaches with varying degrees of specificity.[111] However, there are strong arguments for the creation of specific laws as they are more actionable.[112]

Perrier also discusses an instrumentalist approach to governance:

> concentrating upon the types of instruments, such as treaties, legislation, protocols, policies and procedures, which can be used to regulate (formally and informally) relations among stakeholders, including by providing means by which rights and obligations are negotiated and disputes or differences resolved.[113]

3.1.1 International

Internationally formal public international law instruments include treaties and conventions, customary law, general principles recognised by states and judicial decisions. In the development of quantum governance internationally, comparable instruments include the Treaty on the Non-Proliferation of Nuclear Weapons Treaty and the EU's approach to AI Governance.[114] Multilateral institutions also have a role in governance eg UN developing governance principles. Furthermore, Perrier suggests the creation of international institutions dedicated towards quantum technology coordination and governance as none currently exist.[115]

In 2021, Australia formed a new security alliance with the UK and US, called AUKUS. The AUKUS Quantum Arrangement focusses on the development of quantum military capabilities.[116]

On 3 Nov 2023, a Joint Statement of the United Kingdom and Australia on Cooperation in Quantum Technologies was released, which promotes knowledge and market sharing

---

[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid 12.
[114] Perrier (n 31).
[115] Ibid.
[116] Department of Industry, Science and Resources, National Quantum Strategy (Strategy, 3 May 2023, Australian Government) <https://www.industry.gov.au/publications/national-quantum-strategy/national-and-international-approach>.

between the two countries.[117]

On 13 February 2024, the Multilateral Dialogue on Quantum was announced between Australia and 12 other countries, to help develop a global quantum ecosystem.[118]

3.1.2 National

3.1.2.1 Government

On a national level, the government can introduce quantum governance through legislative and executive powers. A majority of initiatives have been largely confined to policy-related instruments such as national strategies, agendas or plans, or policy papers published by governments or administrative departments.[119] The government also plays a significant role in quantum technology developments through direct investments and indirect investments via academia, procurement policies and public/private partnerships.[120]

Public institutions (eg CSIRO), which are institutions established by public legislation or are publicly funded, also contribute to governance via policy development, administrative oversight or procurement and internally via internal policies or risk management.[121] Often they must balance competing interests of various stakeholders including consumers, private sector companies and government.[122]

3.1.2.2 Non-Governmental

Non-Governmental stakeholders include the commercial private sector, academia, individuals, civil society and technical communities.

The private sector would aim to maximise profit, grow their business and build scalable/useful products.[123] Governance for corporations is mandated by municipal business laws including corporations' law statutes and regulations, delegated authority of agents bound by fiduciary duties, and company policies.[124] Internal quantum governance in corporations can occur through risk management, auditing/checks/reviews and impacted assessments.[125] Most companies in the quantum sector have objectives aligning with the development of quantum hardware, quantum software, and infrastructure related to quantum technology.[126] For start-ups, business objectives and the practical availability or utility of complex internal policy architecture are limited due to limited resources and higher-pressure timelines.[127]

Academia is an instrumental player in quantum with contributions made to formal governance procedures (eg committees, treaty development) and soft measures (eg principles development).[128] Quantum governance within academia includes institutional policies and guidelines (eg research policies), risk-management frameworks, ethical

---

[117]The Hon. Ed Husic, Minister for Industry and Science, 'Australia and UK sign Quantum Joint Statement' (Media Release, 3 November 2023).
[118] Department of Industry, Science and Resources, 'Guiding principles for a global quantum ecosystem informed by science', Policy Statement (Web Page, 13 February 2024, Australian Government) <https://www.industry.gov.au/publications/guiding-principles-global-quantum-ecosystem-informed-science>.
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Ibid.
[126] Ibid.
[127] Ibid.
[128] Ibid.

frameworks assessing the impact of technology research, and the ability to dictate the terms and conditions of funding or grants for projects.[129]

Consideration of the impact of quantum on individuals is also necessary as individual rights must be protected. Existing rights exist through charters, legislation and the constitutions.[130] Rights such as the right to be informed, right to have consent and right to be free from harm, and accountability are relevant to the development of quantum technology.[131]

Civil society which includes trade unions, political parties, charities, privately constituted associations that receive public or other funding, media participants and journalists, also play a role in i) the development and deliberation of governance and ii) the socialising and acceptance of governance including through outreach.[132] The media has a role in setting agendas, highlighting risks and drawing attention to issues requiring governance responses.[133] This is relevant to quantum governance. Similar to culture war debates over vaccines or conspiracy theories and misinformation relating to climate science, misinformation, hype or ignorance on public responses to quantum technology can hinder development and appropriate governance.[134] Civil institutions have the power to counter these negative influences. Furthermore, these institutions can also raise public awareness of the risks of quantum development and drive governmental responses like they did with AI ethical issues which has led to restrictions in some jurisdictions on facial recognition or emotional profiling.[135] Existing organisations such as the Australian Society for Computers and Law (launched 2020) and Digital Law Association (launched 2020) may have a future role in quantum governance.[136]

Lastly, governance is upheld via technical communities which include industry groups, institutes and other collective associations whose activities involve research, development of standards and coordination eg ISO, IEEE.[137] These associations are critical for technological governance with respect to standardisation, development of codes of conduct and setting proposals for risk management specific to technology.[138] They are also important for translating theoretical research into application and act as conduits for coordination between academia and industry.[139] Technical communities play a key role particularly in the early stage of quantum governance.[140] Standards development will be explored further later.

3.2 Does Australia's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

Given the dual-use risks of quantum technology, as previously discussed, a national framework should be established to outline national security and defence policies for quantum technology.[141] This is because the technology poses geostrategic risks if disseminated and distributed to potential adversaries.[142] Currently legislative and regulatory instruments which manage national security-related dual-use technologies do exist, such as

---

129 Ibid.
130 Ibid.
131 Ibid.
132 Ibid.
133 Ibid.
134 Ibid.
135 Ibid.
136 Brennen (n 1).
137 Perrier (n 31).
138 Ibid.
139 Ibid.
140 Ibid.
141 Brennen (n 1).
142 Perrier (n 31).

for nuclear, biotechnology and cybersecurity-related technologies.[143] These can be used as a basis for QIT dual-use regulation.[144]

(1) In addition, many jurisdictions regulate dual-use risks with export controls such as foreign investment export controls.[145] For example, as referred to earlier, the FIRB must approve foreign persons or governments who may obtain a broad scope of interest in critical technologies when used for defence or intelligence purposes of a foreign country.[146] This scope is extremely broad and can cover quantum computing, sensing, encryption and communications technologies.[147] However, some in academia and the private sector have criticised these policies for potentially stifling innovation due to the increased regulatory burden and potential interference with international collaboration.[148] This is a valid concern 'given the importance of foreign direct investments and export markets for the growth of Australia's quantum industry'.[149] Additionally, export limitations can limit the availability and capability of a key principle of cryptosystem design which holds *against* a 'security by obscurity' approach.[150] A common modern use of the so-called Kerckhoff's principle[151] is to use algorithms and designs that are public and subject to public scrutiny, which allows security researchers and professionals to draw on world-wide expertise to look for flaws and find them before adversaries are able to exploit them.[152]

The Defence and Strategic Goods List[153] was updated on 28 August 2021. Of the 209 amendments, 23 have resulted in an expanded scope. Notably, 5A002 Technical Note 2 has expanded control to capture quantum cryptography algorithms and associated software and technology. Approval must be obtained not only for the export of these items, but also for the technology and software required for the development, production or use of these items.

3.3 Are there any <u>ethical guidelines or principles</u> identified in Australia's approach to quantum technology? If so, what are they and where do they come from?

3.3.1 International

The World Economic Forum ('WEF') believes that early intervention in governance is crucial as it can shape how CETs are developed.[154] In 2020, the 'global quantum security coalition' was launched to work to promote safe and secure quantum technology.[155] The WEF, in January 2022, proposed a set of ethical principles or guidelines on quantum computing technology which can be used to inform governance and regulation.[156] Although, the principles are only a proposal as broader stakeholders were not involved in the formulation and consideration of how the principles would be adopted more widely.[157] Furthermore, the

143 Ibid.
144 Ibid.
145 Ibid.
146 Ibid.
147 Ibid.
148 Ibid.
149 *National Quantum Strategy Issues Paper* (n 15).
150 Eric Diehl, *Ten Laws for Security* (Springer International Publishing AG, 2016) <http://ebookcentral.proquest.com/lib/unsw/detail.action?docID=4744597>. Ch 3.
151 Fabien AP Petitcolas, 'Kerckhoffs' Principle' in Henk CA van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US, 2011) 675 <https://doi.org/10.1007/978-1-4419-5906-5_487>.
152 Warren Armstrong, 'SOCRATES WP8 – Request for feedback – DRAFT quantum policy brief' Email to authors, sent 15 Jan 2024.
153 https://www.legislation.gov.au/F2021L01198/latest/text
154 CSIRO, 'First Quantum Computing Guidelines Launched as Investment Booms' (January 2022) <https://www.csiro.au/en/news/news-releases/2022/first-quantum-computing-guidelines-launched>.
155 Brennen (n 1).
156 CSIRO (n 142).
157 Ibid.

WEF recognises existing standards in other fields may apply to quantum technology, but that there are also distinct governance considerations particular to quantum.[158]

3.3.2 National

In Australia there is no ethical framework for quantum, however, the CSIRO Quantum Technology Roadmap suggests some guidelines.[159]

3.4 Are there any international or national standards identified in Australia's approach to quantum technology? If so, what are they and where do they come from?

The development of formal standards on quantum technology has only recently emerged with focused initiatives being driven by governments, broad industry consortia, key players and various recognised Standards Development Organisations ('SDOs').[160] Previously, standards were organically adopted in an ad hoc consensus through publications and IBM'S OpenQASM (quantum language).[161] However, without formal standards, highly influential players can distort standards for their own benefit, such as commercial parties reporting selective benchmarks in order to paint their technology in the best light.[162] Hardware standardisation is also near non-existent since quantum computers are not designed to be interoperable and not enough is known.[163] For emerging critical technologies such as quantum technology, standardisation is crucial to open new markets, ensure interoperability, facilitate international trade, and manage security risks.[164]

3.4.1 International

The purpose of formal standards development on an international level is to 'produce robust and equitable consensus among the broadest possible cross-section of stakeholders'.[165]

Notable developments include:

- The ISO/IEC JTC 1 establishing a working group on Quantum Computing (WG14).[166]
- The IEC publishing a white paper on Quantum Information Technology which advocates for relevant SDOs to keep track of parallel quantum computing standardisation efforts and form a mechanism to assess standardisation readiness levels for emerging technologies to inform quantum standardisation development.[167]
- The IEC creating the Standardisation Evaluation Group (SEG) 14 on Quantum Technology to summarise use cases and propose a roadmap for standardisation.[168]

Other important standards include the following from the International Telecommunications Union (ITU):

- Quantum key distribution networks - control & management Y.3804 (09/20);[169] and
- Quantum noise random number generator architecture[170]

Challenges relating to standardisation on an international scale include that, by design, massively multilateral, committee-driven processes 'operate slowly and with considerable

[158] Ibid.
[159] Brennen (n 1).
[160] Langford (n 43).
[161] Ibid.
[162] Ibid 31.
[163] Langford (n 43).
[164] *Critical and Emerging Technologies* (n 9).
[165] Ibid 23.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] https://www.itu.int/rec/T-REC-Y.3804/en.
[170] https://www.itu.int/rec/T-REC-X.1702

inertia' and consequently struggle to match the pace of rapid progress made in quantum computing.[171] An additional challenge is the lack of overlap between experts in standardisation and quantum computing.[172]

Thus, the most agile formal standards development occurs more locally on a national or regional level.

3.4.2 National/Regional

National (or European) standards bodies (NSBs), professional bodies and industry-engaged consortia – eg the IEEE, Quantum Economic Development Consortium (QED-C) and European CEN-CENELEC – arising especially out of flagship quantum strategies such as those of the US National Quantum Initiative and the EU Quantum Flagship, all have active standardisation activities.[173] For example, the IEEE has existing standards for protocols on quantum communication, QIT definitions, performance metrics and benchmarking.[174]

In Australia, Government and Industry have sought to coordinate an Australian standards position in CET including quantum technology.[175] Quantum standardisation is nascent, however, Standards Australia is actively working towards supporting a strong Australian position on quantum and has formed a national Quantum Working Group to contribute to international standards development on terminology for quantum computing, a crucial first step to ensure future interoperability.[176] Standards Australia has also released the first research report of their series of Quantum Position Papers following a March 2022 forum and subsequent roundtable meetings.[177] These papers will explore current worldwide quantum standardisation efforts and map the current and emerging standards needs for quantum technologies.[178]

In the first paper, Langford and Devitt recommend standards be made in the following areas:

1) Terminology standards (relevant to educating the quantum workforce and helping build consumer/investor confidence)

2) Technical reports to disseminate a broader understanding of development trajectories and key challenges

3) Measurement and Test Method

4) Specifications and System Architecture standards

5) Practice Guidelines (development stage)

6) Requirement standards (later stage, evolved from Practice Guidelines)

7) Software Specifications, Frameworks for System Architectures

8) Formal Models.[179]

---

[171] *Critical and Emerging Technologies* (n 9).
[172] Ibid.
[173] Ibid.
[174] Perrier (n 31).
[175] *Critical and Emerging Technologies* (n 9).
[176] Ibid.
[177] Ibid.
[178] Ibid.
[179] Langford (n 43).

4 Barriers or Challenges

4.1 Does Australia's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected?

4.1.1 Practical/Technological Challenges of quantum computing

The key challenge of quantum technology development lies in quantum physics itself. Gill et al identify quantum decoherence and qubit interconnectivity as 'two of the major challenges to achieve quantum advantage in the NISQ era'.[180] The NISQ era is the current state of quantum computer and implies that quantum computers of this time 'don't have many useful qubits and possess high error rate'.[181] As quantum devices start scaling up in the next few years, these challenges will be magnified. Currently, much of the ongoing research efforts are dedicated to developing efficient error correction protocols to overcome errors caused by decoherence in NISQ devices.[182]

Another practical challenge for quantum computing is that many quantum machines are 'bulky' and must be 'kept at superconducting temperatures'.[183] This limits the availability of these machines to parties that have the appropriate infrastructure to house these machines. Furthermore, whilst more energy efficient than supercomputers, when scaling quantum computers up (50 qubits to 10,000), more energy is required for computing and cooling to maintain the temperature.[184] This suggests a 'need to develop energy-efficient quantum data centres for better utilisation of energy' for which 'renewable energy with brown power can be considered in future'.[185]

Lastly, an important consideration, rather than a challenge, is researching what practical problems can be efficiently solved on quantum computers if quantum computing is error-corrected and able to deliver a quantum advantage.[186]

4.1.2 Barriers to Development

In Australia, barriers to development include Australian quantum technologists moving to work in overseas quantum industries,[187] and higher barriers of entry for start-ups due to difficulties accessing infrastructure and less developed general business services.[188] Additionally, current visa backlogs can affect attempts to recruit from overseas.

4.1.3 Broader Risks of Development

High costs and technical expertise also create the risk of monopolisation of quantum computing. Countries and corporations that heavily invest in developments will benefit if commercial applications of the technology are realised which can have implications socio-economically and geo-politically.[189] This gives 'rise to issues of equity, access and distribution of benefits and risks, especially for under-resourced nations and stakeholder groups'.[190] An 'uneven distribution of skills and knowledge' relating to quantum computing can also exacerbate and create new 'inequalities in terms of technology access'.[191]

---

[180] Gill (n 35) 1.
[181] James Dargan, 'What Is NISQ Quantum Computing?', The Quantum Insider, (Web Page, 13 March 2023) <https://thequantuminsider.com/2023/03/13/what-is-nisq-quantum-computing/>.
[182] Gill (n 35) 2.
[183] Ibid 29.
[184] Ibid 34.
[185] Ibid.
[186] Ibid 28.
[187] Brennen (n 1).
[188] *National Quantum Strategy Issues Paper* (n 15).
[189] CSIRO (n 142) 4.
[190] Ibid 16.
[191] Ibid.

Furthermore, on a broader level, the exact implications of quantum technology are unknown as there is a lack of due diligence or impact assessments of the technologies.[192] Potentially, when used alongside classical computing technology, problems already faced today may be amplified.[193] There is also a lack of risk-assessment frameworks to mitigate, control and enable a timely response to risks.[194]

5 Australia's Overall Approach

5.1 Are there any advantages to Australia's approach?

There are advantages to Australia's approach as investment into quantum technology has been boosted in recent years and a National Quantum Strategy is being developed which comprehensively considers investment, collaboration, commercialisation, building a skilled quantum workforce and drawing a balance between economic prosperity and protecting national interests.

5.2 Are there any gaps identified in Australia's approach to quantum technology?

Much of Australia's approach to quantum technology is focused on boosting investment into research and development of quantum technologies to gain commercial benefits and protect national interests. Here, Australia aims to close the gap between Australia's quantum capabilities and knowledge and overseas players such as the UK, US, EU, India, Germany, Russia and China. However, Australia's focus on strategy overshadows the need for governance which includes the development of ethical principles, standards and regulation.

There is some focus on adopting ethical frameworks by the CSIRO and moves to develop standards on quantum technology by Standards Australia. However, ethical principles and standards development do not appear to be at the forefront of discourse on quantum technology despite being significant. Governance overall has been considered with propositions to create novel governance specific to quantum technology in addition to adapting existing technological governance regimes which include hard and soft approaches. It seems that the discussion on governance is in the early stages. This seems to be the case in Australia as well as in other countries and regions. It is not surprising given the technology itself is in its early stages. However, this highlights the need for governance and it should be more strongly prioritised since it can shape future developments and implications of the use of the technology. Governance must also be balanced with promoting innovation and must be flexible to adapt to rapid technological developments.

---

[192] Ibid 13.
[193] Ibid 4.
[194] Ibid 13.