UNSW Law & Justice Research Series

Quantum Resilience in the Australian National Security Legislative Framework (Policy Brief)

Susanne Lloyd-Jones, Kayleen Manwaring

[2024] *UNSWLRS* 32

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Quantum Resilience in the Australian National Security Legislative Framework[1]

Revised edition August 2024

1 Executive summary

The advent of quantum technology applications presents a significant challenge to cybersecurity worldwide, with the potential to compromise classical cryptographic systems.[2] This policy brief focuses on Australia's preparedness in the face of evolving quantum technology applications, acknowledging the heavy reliance on cryptographic techniques and the predicted future risk of quantum-enabled capabilities including decryption and signature forgery. While quantum-resilient cryptography shows promise, policy tensions arise between the necessity for continuous research and innovation, the requirements of security stakeholders and the imperative to safeguard privacy and security of data.

The brief explores the potential of quantum computers to undermine the effectiveness of current cryptographic processes and infrastructure, emphasising the need to develop quantum-resilient cryptographic methods, processes and technology, such as quantum key distribution (QKD) and post-quantum cryptography (PQC). However, it also investigates a consequent tension arising between ensuring privacy of communications and enabling law enforcement agencies to intercept communications for investigative purposes.

This brief analyses Australia's National Quantum Strategy and Cyber Security Strategy, highlighting commitments to quantum development and the need for post-quantum cryptography standards. The *Security of Critical Infrastructure Act 2018* (Cth) (SOCI), Part 14 and Part 15 of the *Telecommunications Act 1997* (Cth) (TA) and Part 5-3 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) are discussed, emphasising the tension between innovation, security obligations and the use of strong cryptography. We note that technological progress of software techniques and traditional computing at present are likely to impact cryptographic security more than near-term quantum specific developments. However, this brief explores national and international approaches to cryptographic resilience in the context of emerging quantum technologies. [3]

The brief outlines the approaches of the European Union, India, the United Kingdom, and the United States, providing insights into their legislative frameworks, key legislation relevant to quantum technologies, and standards development efforts. It highlights the complex policy landscape surrounding quantum technologies and cryptographic methods and processes including public-key encryption, digital signatures, and key-exchange protocols.

---

[1] The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme. In 2018, the CSCRC was awarded $50 million in Commonwealth funding over seven years. This funding is supplemented by contributions from industry, university, and government agency Participants.

[2] Michele Mosca, 'A quantum of prevention for our cybersecurity', *Global Risk Institute* (Report, 5 September 2016) < https://globalriskinstitute.org/publication/quantum-computing-cybersecurity/> 1.

[3] We acknowledge some researchers regard some of the predictions about the impact of quantum information science as scientific hype. See eg, Olivier Ezratty, 'Mitigating the quantum hype' ArXiv.org (Web Page, 23 January 2022) https://arxiv.org/abs/2202.01925; Frank Smith, 'Quantum technology hype and national security' 51(5) *Security Dialogue* 488-516; Ernst and Young, *Beyond the Hype: A Critical Look at Quantum Computing's Potential for Business and Society in Asia-Pacific* (Report, 2023).

It also serves as a foundation for further research and policy development, recognising the need for a nuanced and adaptive approach to address the evolving challenges posed by quantum advancements.

Recommendations

1. *Design adaptable quantum resilient regulation for the short, medium and long term*
2. *Incorporate quantum standards into existing frameworks*
3. *Contribute more funding for Australian quantum-resilient development*
4. *Continue to advocate for standards development*
5. *Explore law enforcement capabilities*
6. *Develop the Australian Public Service into a quantum workforce, capable of supporting the government's goals*
7. *Contribute to better understanding of the impact of quantum computing on other emerging technologies and associated risks*
8. *Promote collaboration and partnerships between public, private and research sectors to enable development and utilisation of tools for easier access and testing*
9. *Establish resilient quantum supply chain following a risk-based approach*
10. *Develop guidelines for users and vendors of quantum computing solutions (e.g., hardware requirements and impact on performance)*

Figure 1: Recommendation for coordinated implementation of regulatory and policy approaches

2 Introduction

A developing quantum industry brings significant risk for cyber security of systems, networks, and infrastructure. In Australia and worldwide, cryptographic technologies are currently essential to secure a range of network and data transactions and functions. There exist concerns that potential heightened computational power in high-functioning quantum computing could be applied by malicious actors to break contemporary cryptosystems, such as encryption algorithms, public key digital signatures, key exchange protocols and public key infrastructure, that are resistant to conventional computing power. This ability could enable successful cyber-attacks on governments, businesses, and individuals.[4] While quantum computing developments have not yet achieved this capability,[5] there is apprehension that cyber-attacks *in the present,* for example, on encrypted data will increase *in anticipation* of quantum decryption capabilities ('pre-quantum'). Identified as the 'harvest now, decrypt later' problem, it is a method where encrypted data is stolen and stored for future decryption by a computer with sufficient power, which is predicted to be a quantum computer. The problem will impact asymmetric cryptography due to the transmission of data and public keys.[6]

Technical developments in quantum-resilient encryption[7] and innovation in quantum communications hold some promise in defending against these attacks. However, law enforcement and national security stakeholders have policy drivers towards communication interception and decryption that may conflict with encouraging government support of these technologies.

This document provides a brief introduction to the policy and legal support and barriers to quantum-resilient cryptographic systems in Australia, and an overview of approaches in the US, UK, EU and India. It is intended to assist in gauging Australia's regulatory preparedness for quantum, acknowledging the policy tension and technology gaps that exist. The issues are complex, and cannot be comprehensively covered in this project, but it should provide some guideposts towards further research and policy development in this area.

The policy options set out in section 3 are recommended based on our analysis of existing best practice approaches internationally and the gaps we have observed in Australian and international approaches.

3 Policy options

Given the significant cyber security challenges the emergence of quantum technologies presents, there is a need to reconcile competing policy and regulatory goals around quantum-safe encryption. Key steps to achieving such goals are explored below.

a) *Commence* the groundwork for a flexible, proportionate and adaptive regulatory pathway for quantum technology applications for the short, medium and long term. The United States and the United Kingdom have both started laying the foundations for the regulation and governance of quantum technology applications. The United States has enacted a suite of quantum-specific preparedness legislation.[8] The Regulatory Horizons

---

[4] Beth Waller and Elaine McCafferty, 'Comment: The Necessary Evolution of State Data Breach Notification Laws: Keeping Pace with New Cyber Threats, Quantum Decryption, and the Rapid Expansion of Technology' (2022) 79(1) *Washington and Lee Law Review* 521.

[5] To the extent this can be known from current available open-source information.

[6] See Michal Krelina, 'The Prospect of Quantum Technologies in Space for Defence and Security' (2023) 65 *Space Policy* 101563. See also, Quintessence Labs, 'Quantum Computing is Coming, But Quantum Risk is Here Now', Quintessence Labs FAQs (Web Document, 2022) https://info.quintessencelabs.com/hubfs/QuintessenceLabs-Quantum-FAQs.pdf.

[7] Note however that quantum-resilient encryption algorithms will still be subject to the current need for strong keys that are kept secure.

[8] See Appendix E for details.

Council of the United Kingdom released its approach to the regulation of quantum technology applications in February 2024.[9] Australia should be looking to harmonise its approach to governance and regulation with like-minded countries, yet also taking into account the nation's specific needs, requirements and interests.[10]

b) *Incorporate* quantum standards when they are available from organisations such as NIST/ETSI with existing standards in SOCI. While SOCI can absorb technological developments and applications of quantum technologies through the critical infrastructure risk management program rules (CIRMPR), without positive obligations to mitigate quantum risks and build quantum resilience, many industries may not concern themselves with these technologies;

c) *Contribute* more funding for Australian quantum-resilient development: although Australia currently does some sophisticated quantum research, especially in the university sector, the funding allocation appears low compared to other countries,[11] and much concentrates on areas other than cyber security and encryption;[12]

d) *Continue* to advocate and fund Australian involvement in standards development at both the international (eg ISO, IEEE and key national/regional levels such as NIST, ETSI);

e) *Gather* evidence on how successful Australian law enforcement and national security agencies have been in decrypting intercepted data, ie scope the actual problem they will face in the light of 'impenetrable' communications;

f) *Develop* the Australian Public Service (APS) into a skilled and scalable quantum workforce, able to support the government's goals in properly promoting and regulating quantum industries and applications in Australia. While the *National Quantum Strategy* discusses the support of a skilled and growing quantum workforce in industry and academia, its recommendations do not explicitly include the APS. The APS should be included in Action 3.2, or a similar exercise should be undertaken with due focus on the necessary skills specific to the relevant government departments and agencies, eg regulation, trade promotion, law enforcement and intelligence.[13] Knowledge asymmetries between academia, innovators, industry, regulators and government can be mitigated through education, training and impact and engagement activities, such as creating opportunities for knowledge transfer, teaching and learning, professional development and talent acquisition.[14]

---

[9] See Regulatory Horizons Council, 'Regulating Quantum Technology Applications' (Report, February 2024) <https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf>.

[10] Australian Government, '2023-2030 Australian Cyber Security Strategy', (*Strategy*, 22 November 2023) https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf ('Cyber Security Strategy').

[11] Note that reliable data on funding is difficult to discover. It is likely that much of the funding by government is secret due to a perception of potential national security risks. Also, many funding announcements relate to a very broad set of quantum applications, and do not clearly differentiate between applications centred on communications security developments and those in other areas of quantum.

[12] See eg in Australia, a substantial amount of funding is allocated to attempts to build quantum computing architectures in silicon and optical platforms at UNSW's Center for Quantum Computation & Communication Technology (CQC2T): <https://www.cqc2t.org/research/>. Note however that CQC2T also has active projects in quantum communications security.

[13] Department of Industry, Science and Resources, 'Theme 3: A skilled and growing quantum workforce', *National Quantum Strategy* (3 May 2023, Australian Government) < https://www.industry.gov.au/publications/national-quantum-strategy/themes-national-quantum-strategy/theme-3-skilled-and-growing-quantum-workforce>.

[14] See Johanna Weaver and Sarah O'Connor, *Tending the Tech-Ecosystem: who should be the tech-regulator(s)?* (Report, May 2022, Tech Policy Design Centre) https://techpolicydesign.au/wp-content/uploads/2023/08/Web_TPDC_Tending-Tech-Ecosystem_NO.1_2022_2023-Cover-Update_V2.pdf, 7.

4 Quantum technologies and encryption

It is commonly suggested that quantum computers, when fully operational, will be able to compromise the security goals of several conventional cryptographic systems including key exchange protocols, encryption, digital signatures, and public-key infrastructure. For example, quantum computing power can be used to decrypt communications encrypted with many popular forms[15] of public key (asymmetric) encryption, the process underpinning most communications infrastructure, networks, and applications. Conversely, the implementation of quantum communications technologies could significantly aid in efforts to keep data, systems and hardware secure, as developers claim that it will be much more resistant to cyber-attacks than current communications technologies.

Advocates argue that the implementation of 'quantum-resistant' cryptographic systems and quantum communications is essential in protecting entities against successful attacks that use quantum computing to compromise the security of conventional cryptography. However, this potential for 'unbreakable' communications has its natural detractors from a policy perspective. National security and law enforcement agencies, such as the AFP and ASIO, are insistent that they are heavily reliant on interception of decipherable communications for many of their investigative functions.[16] This creates a tension between two estimable policy goals: the goal of preventing anyone but the sender and intended receiver from accessing private communications and the goal of intercepting communications between those intent on criminal acts, including terrorism and other serious offences.

5 Overview of some important current law and policy approaches

5.1 Overview of Australian law and policy

5.1.1 Policy approaches to cyber security and quantum development

Australia's National Quantum Strategy,[17] launched 3 May 2023, includes commitments that the Australian government will:

- 'ensure the growth of Australia's quantum ecosystem supports economic prosperity while safeguarding national well-being';[18] and
- 'champion responsible innovation and the introduction of new standards and regulatory mechanisms where national wellbeing is at risk'.[19]

In 2023, the Australian government launched the *2023-30 Australian Cyber Security Strategy*.[20] In this strategy, the government recognised the risk that '[a]dvances in quantum computing could leave contemporary cryptography insecure' and the need to 'anticipate future requirements of encrypted systems'.[21] Part of the so-called 'Shield 10' of the

---

[15] Roger Grimes, *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto* (Wiley, 2019) at Chapter 3 provides a useful list of the most vulnerable cipher algorithms ie ones that rely on 'the integer factorization problem, the discrete logarithm problem, the elliptic-curve discrete logarithm problem, or any other closely related mathematical problems'.
[16] Ian Walden, '"The Sky Is Falling!" – Responses to the "Going Dark" Problem' (2018) 34(4) *Computer Law & Security Review* 901; more recently see Mike Burgess and Reece Kershaw, 'Address to the National Press Club of Australia', *ABC News* (YouTube Video, 24 April 2024) <https://www.youtube.com/watch?v=ysi1aIY4NkU>.
[17] Ibid; Australian Government, 'National Quantum Strategy' (*Strategy*, 3 May 2023) https://www.industry.gov.au/publications/national-quantum-strategy.
[18] Australian Government, *National Quantum Strategy,* Theme 5: A trusted, ethical and inclusive quantum ecosystem, https://www.industry.gov.au/publications/national-quantum-strategy/themes-national-quantum-strategy/theme-5-trusted-ethical-and-inclusive-quantum-ecosystem
[19] Ibid.
[20] Australian Government, 'Cyber Security Strategy' (n 10).
[21] Ibid 33.

Australian government's Quantum Action Plan (primarily focussed on the public sector) is to '[p]repare for a post-quantum world' by:

> [s]et[ting] standards for post-quantum cryptography by updating guidance within the Information Security Manual. Organisations will also be encouraged to prepare for the post-quantum future by conducting a review of their data holdings and developing a plan to prioritise and protect sensitive and critical data.[22]

The Information Security Manual (ISM) is a public document produced by the Australian Cyber Security Centre and its purpose is 'to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats'.[23]

Australia would benefit from commencing development of its regulatory pathway for a flexible, proportionate, and adaptive framework for quantum resilience. The United States and the United Kingdom are ahead of Australia in this regard. The United States has enacted a suite of quantum-specific preparedness legislation aimed at early adoption of quantum-safe practices and technologies.[24] In the United Kingdom in February 2024, the Regulatory Horizons Council released a report on its approach to the regulation of quantum technology applications.[25]

Australia should be looking to harmonise its approach to governance and regulation with like-minded countries, yet also considering its country specific needs and requirements.[26]

5.1.2 Key legal regimes

Australia has yet to pass any direct legislation in relation to quantum preparedness. The SOCI Act operates as an 'all hazards' risk management framework for critical infrastructure industries, which contains flexible and adaptive mechanisms to absorb quantum-related risks. The main legal obligations directly relevant to quantum technology relate to export controls under the Defence and Strategic Goods List 2021 and foreign investment restrictions in critical technology industries. The Defence and Strategic Goods List 2021 (DSGL) (a legislative instrument authorised under the *Customs Act 1901* (Cth))[27] specifies goods, software and technology that are 'controlled' items under Australian export control legislation. A permit is required when exporting, supplying, brokering or publishing DSGL items, unless exempted. Part 2 of the DSGL lists 'dual-use' goods which are developed for commercial purposes but could also be used for military purposes. These 'dual use goods" include quantum crytography, quantum key distribution, post-quantum, quantum-safe or quantum-resistant algorithms. However, these controls are severely diluted or removed when the technology is in the 'public domain'.[28]

It is worthwhile noting that export restrictions can be a double-edged sword. A key principle of cryptosystem design argues against a 'security by obscurity' approach. Instead,

---

[22] Australian Government '2023-2030 Australian Cyber Security Strategy Action Plan' *(Plan)* https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf 13.
[23] Australian Government, *Information Security Manual (ISM)* (Web Page) https://architecture.digital.gov.au/information-security-manual-ism accessed 25 April 2024. See also the NIST standardization process: https://csrc.nist.gov/projects/post-quantum-cryptography accessed 21 August 2024.
[24] See Appendix E for details.
[25] See Regulatory Horizons Council, 'Regulating Quantum Technology Applications' (Report, February 2024) https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf.
[26] Australian Government, 'Cyber Security Strategy' (n 10).
[27] S 112(2A)(aa).
[28] DSGL ss 3.94, 3.101(2), 3.111, Category 5 Parts 1 and 2.

proponents of this design principle argue that exposure of the system design to the public may be helpful in the following ways:

(1) assuming attackers will know the system in detail means that your design and key security will be stronger; and

(2) broad 'peer review' of the system can assist in uncovering previously unknown flaws and weaknesses.[29]

Quantum technologies, including quantum cryptography, are listed on Australia's *List of Critical Technologies in the National Interest*.[30] The list interacts with the Foreign Acquisitions and Takeovers Act 1975 (Cth) (FATA). The *Foreign Investment Reform (Protecting Australia's National Security) Act 2020* (Cth) amended the FATA so that definitions associated with critical technology, and critical infrastructure in SOCI are now included in the FATA. Foreign investment in a responsible entity or a direct interest in a critical infrastructure asset is now subject to notification to the FIRB. FIRB can undertake 'own motion' review of transactions if it has national security concerns.[31]

See Appendix A for more detail on Australia's regulation, policy and strategy.

5.1.3 Implications of quantum technology for Australia's extant national security frameworks - examples

The following obligations may be incompatible with communications industry efforts to secure their communication channels with strong cryptographic systems designed to protect against interception and access.[32] On the one hand, regulated entities required to 'do their best' to secure their assets from authorised access and take an 'all-hazards' approach to risk management. On the other hand, there is an expectation that certain critical infrastructure industry participants – telecommunications and data storage and processing - will also provide access and assistance to their services, systems, and networks.

The SOCI Act[33] imposes Federal cyber security and other obligations on designated critical infrastructure (CI) industries responsible for declared CI assets. In this context, CI assets are assets considered 'essential to the functioning of the economy, society, or national security' of Australia.[34] The SOCI Act established a register of CI assets and has economy-wide coverage of regulated industries including electricity, gas, water, and maritime port sectors. It applies to data storage or processing, communications, financial services, and energy, as

---

[29] Eric Diehl, *Ten Laws for Security* (Springer International Publishing AG, 2016) <http://ebookcentral.proquest.com/lib/unsw/detail.action?docID=4744597>. Ch 3.
[30] Department of Industry, Science and Resources, 'List of Critical Technologies in the National Interest', Australian Government (Web Page, 19 May 2023) < https://www.industry.gov.au/publications/list-critical-technologies-national-interest>.
[31]For more details, see FIRB Foreign Investment Review Board, *Guidance Note* 8 - *National Security Test* (Guide, 17 December 2020) < https://firb.gov.au/sites/firb.gov.au/files/guidance-notes/G08-Nationalsecurity.pdf>.
[32] For a discussion of the issues and possible solutions, Carnegie Endowment for International Peace, *Moving the Encryption Policy Conversation Forward* (Working Group Report, 10 September 2019) https://carnegieendowment.org/2019/09/10/moving-%20encryption-%20policy-%20conversation-forward-pub-79573.
[33] *Security Legislation Amendment (Critical Infrastructure) Act 2021*; *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth).
[34] Gilbert + Tobin, 'A Guide to Critical Infrastructure Assets in Australia' (*Web Page*, 2022) www.gtlaw.com.au/knowledge/guide-critical-infrastructure-assets-australia. The definition of 'CI assets' in s 9 of *Security of Critical Infrastructure Act 2018* (Cth) does not define this term generally, but by reference to industry assets.

well as many other sectors. The *SOCI Act* contains extensive statutory obligations relating to CI assets,[35] including:

- obligations on the operator to:
  - notify the Australian Signals Directorate (ASD) of any cyber incidents impacting CI assets;[36] and
  - establish, maintain, and comply with an all-hazards critical infrastructure risk management program (CIRMP);[37] and
- the ability of the government to:
  - in the case of some cyber-attacks, require the responsible entity to provide information, take or refrain from taking action, and/or authorise the ASD to intervene to defend the asset;[38] and
  - declare certain CI assets as 'Systems of National Significance' ('SoNS'), subjecting the responsible entity to enhanced cyber security obligations, such as incident response plans, cyber security exercises, government access to system information and mandatory cyber security exercises.[39]

A recent consultation paper on proposed legislative reforms in the wake of the new Cyber Security Strategy[40] did not contain any quantum-specific reforms, although it is likely that quantum attacks would be subject to some of the *SOCI Act* provisions, particularly under an 'all-hazards' CIRMP. The consultation paper sought views on a legislative reform proposal to incorporate the telecommunications sector security regulatory framework with the SOCI Act. This reform would harmonise the telecommunications sector's security with that of other critical infrastructure industries, including aligning telecommunications within the 'all-hazards' risk management framework.[41]

Australian law enforcement and intelligence agencies possess powers to obtain access to encrypted communications.[42] Under Part 14 of the TA, carriers and certain carriage service providers must, among other things, give authorities 'such help as is reasonably necessary' for the purposes of enforcing criminal laws and laws imposing pecuniary penalties; protecting public revenue; and safeguarding national security. In addition, carriers, carriage service providers and carriage service intermediaries must 'do their best' to protect telecommunications networks and facilities from unauthorised interference or unauthorised access, including, for the purposes of security, protecting the confidentiality of communications and the availability and integrity of telecommunications networks and services.

Part 15 of the TA authorises a range of technical assistance that security and law enforcement agencies may request from designated communications providers (although noting the type of assistance is constrained by the specified function of the requesting Agency). For example, in the case of the Australian Signals Directorate, giving assistance

---

[35] The asset definitions are set out in *SOCI Act* s 12F and the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth) ('CIRMP Rules').
[36] *SOCI Act* pt 2B.
[37] *SOCI Act* pt 2A.
[38] *SOCI Act* pt 2B.
[39] *SOCI Act* pts 6A and 2C.
[40] Australian Government, *2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper*, (Issued 8 Jan 2024) https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/cyber-security-legislative-reforms.
[41] Ibid.
[42] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), which amended the TA, the TIA, the *Surveillance Devices Act 2004* (Cth) and various other related legislation.

may include providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored, or communicated by electronic or similar means. Authorised assistance may include removing electronic protections and facilitating access to a range of services, devices, and software.

Carriers and carriage service providers also have obligations under Part 5-3 of the TIA to provide interception capability of their telecommunications systems, permitting interception of communications and delivery of the intercepted communications.

Quantum information technologies will impact the national security obligations of critical infrastructure sectors as those technologies evolve and are commercially deployed. For example, a future regulated operator or provider of a quantum communications system or network marketed to customers as a 'premium secure service' may not be technically able to provide interception capability, unless that capability is part of the network or system design. Likewise, "interception-by-design" in a secure quantum communications network or system may be neither economically desirable nor technically feasible due to the quantum mechanics operating the system or network. Equally, a fault tolerant quantum computer may be both friend and foe in an interception scenario, providing both offensive and defensive capability to governments or industry participants.

The quandaries posed by quantum information technologies that we have identified in this brief require careful consideration by government, including further research and co-designed solutions with critical infrastructure industry participants.

5.2 Overview of EU law and policy

The EU has announced significant ambitions in developing quantum technologies. However, it has also publicly recognised the risk posed to current cryptography practices.[43] On 11 April 2024, the European Commission released a recommendation that member states commence developing strategies for a coordinated response and eventual adoption of post-quantum cryptography.[44]

5.2.1 Key legislation

There is no quantum-specific preparedness legislation in place in the EU related to cyber security. However, on 18 April 2023, the European Commission proposed the Cyber Solidarity Act,[45] an EU Regulation to improve the preparedness, detection and response to cyber security incidents across the EU. The proposal includes a European Cybersecurity Shield to protect, detect, defend and deter cyber threats, including post-quantum encryption.[46] Additionally, in April 2024 the European Commission issued a formal Recommendation that 'Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible'[47] and proposed the Member States collaborate to produce a 'Post-

[43] See Appendix B.
[44] European Commission, 'Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography', Policy and Legislation (Web Page, 11 April 2024) https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.
[45] Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents Proposal 2023 (EU) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209.
[46] European Commission, 'A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton', *Speech* (Web Page, 05 April 2023) https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145.
[47] European Commission, 'Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography' https://digital-

Quantum Cryptography Coordinated Implementation Roadmap' and evaluate and select PQC algorithms as EU standards.[48]

Regulation (EU) 2021/821[49] sets out rules throughout the EU to control exports, brokering, technical assistance, transit and transfer of 'dual-use' items. Controlled items include quantum computers and related electronic assemblies and components, qubit devices and qubit circuits containing or supporting arrays of physical qubits, quantum control components and quantum measurement devices; as well as the technology for their development or production.[50]

5.2.2 Quantum standards development

In general, European standards are created by one or more of the following standards organisations: CEN, CENELEC or ETSI. The CEN-CENELEC Focus Group on Quantum Technologies released a standardisation roadmap for the EU in March 2023.[51] In 2021, ETSI released two Technical Reports (TRs) to support the US National Institute of Standards and Technology (NIST) standards for quantum cryptography. To date, ETSI has published several Technical Reports, Technical Specifications and Group Reports on quantum technologies, primarily on quantum-safe cryptography, VPNs and signatures.[52]

See Appendix B for more detail on EU regulation, policy and strategy.

5.3 Overview of Indian law and policy

In January 2024, the Indian Ministry of Electronics and Information Technology released its Quantum Technologies Roadmap for consultation, prioritising research and development in 'thrust areas', such as cyber security.[53] India announced its first 'quantum secure communication link' in March 2023, between the Department of Telecommunications and the National Informatics Centre.[54] In April 2023, it announced funding of in excess of INR6000 crore (USD 730 million) for quantum projects under its National Quantum Mission.[55] By October 2023, India had nearly a hundred quantum projects in development.[56]

---

strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography Recital 5.

[48] Ibid, cl 1.

[49] *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)* [2021] OJ L 206 11.6.2021/1.

[50] Ibid art 9(4).

[51] CEN-CENELEC Focus Group on Quantum Technologies (FGQT) *Standardization Roadmap on Quantum Technologies* (Release 1 – March 2023) https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf.

[52] ETSI, *Search and Browse Standards* (Web page) https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-12-19&harmonized=0&keyword=&TB=856,,836&stdType=&frequency=&mandate=&collection=&sort=1.

[53] Ministry of Electronics and Information Technology, 'Quantum Technologies Roadmap', Government of India (Web page, 23 January 2024) https://www.meity.gov.in/content/project-timeline-qc-roadmap-v5.

[54] 'India's First Quantum Computing-Based Telecom Network Link Now Operational: Ashwini Vaishnaw', *The Economic Times* (online, 27 March 2023) https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99026697.cms ('India's First Quantum Computing-Based Telecom Network Link Now Operational').

[55] 'Cabinet Approves National Quantum Mission to Scale-up Scientific & Industrial R&D for Quantum Technologies', *PMIndia* (19 April 2023) https:/www.pmindia.gov.in/en/news_updates/cabinet-approves-national-quantum-mission-to-scale-up-scientific-industrial-rd-for-quantum-technologies.

[56] Ministry of Science & Technology, 'Industry will be expected to be a major resource contributor in all the future StartUp ventures and other new technology initiatives, says Union Minister Dr Jitendra Singh' (*Press Release*, 5 October 2023) https://pib.gov.in/PressReleseDetailm.aspx?PRID=1964650.

It has also entered into several public, private and university partnerships. However, this funding and these projects are not confined to cyber security and encryption issues: rather, their scope is broad and include computing, communications, sensing and metrology, and materials and devices.[57]

5.3.1 Key legislation

India has several ministerial divisions with some responsibilities for overseeing the development of quantum technology. However, it is yet to put into effect any regulatory or legal frameworks specific to quantum technology. It is currently proposed that a new Digital India Act (DIA) will replace the existing Information Technology Act 2000. The DIA is expected to contain provisions attempting to address the risks of emerging technologies, including strengthened cyber security obligations.[58]

The Foreign Trade (Development & Regulation) Act 1992 (India) regulates India's international trade. The Directorate General of Foreign Trade (DGFT) publishes the Foreign Trade Policy (FTP), which governs exports and imports of goods and services. Under the FTP 2023, 'export of dual-use items, including software and technologies, having potential civilian/industrial applications as well as use in weapons of mass destruction is regulated. It is either prohibited or is permitted under an authorization.'[59] Dual-use items are listed in the Special Chemicals, Organisms, Materials, Equipment and Technologies list (SCOMET), and includes: quantum cryptography, quantum key distribution (QKD), superconducting quantum interference devices, as well as many cryptographic and cryptanalytic technologies.

India's foreign direct investment (FDI) is governed by the Foreign Exchange Management Act 1999 (FEMA). The current FDI Policy has been effective since 2020 and does not include guidelines on quantum technology. Existing rules for the Information Technology sector allow for 100% FDI. However, eleven sectors require government approval for FDI, including some sectors likely to involve quantum technologies (eg mining, defence, satellites, telecommunications, some financial services and pharmaceuticals).[60]

5.3.2 Quantum standards development

The Bureau of Indian Standards (BIS) is the national standards body of India. Its Electronics and IT Division Council (LITDC)[61] is primarily responsible for developing Indian standards in the field of electronics and IT products and has a technical committee for quantum computing.[62] BIS's objectives include aligning Indian standards with international ones.[63]

See Appendix C for more detail on India's quantum regulation, policy and strategy.

5.4 Overview of UK law and policy

The UK has made significant investments as part of its National Quantum Technologies Programme 2014-2024 (NQTP) and National Quantum Strategy 2023-2033 (NQS) (public and private funding of GBP 1 billion in the NQTP, and a planned GBP 3.5 billion in the NQS).

---

[57] See Appendix C.
[58] Ministry of Electronics and Information Technology, 'Proposed Digital India Act 2023', *Digital India Dialogues* (9 March 2023) <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf>.
[59] Directorate General of Foreign Trade, 'Chapter 10: Special Chemicals, Organisms, Materials, Equipment and Technologies'. *Foreign Trade Policy 2023* https://content.dgft.gov.in/Website/dgftprod/a2f58730-df83-49df-a437-b5f6345abb66/FTP2023_Chapter10.pdf.
[60] Foreign Investment Facilitation Portal, 'Present FIFP', (Web Page) https://fifp.gov.in/AboutUs.aspx.
[61] Electronics and IT Division, Bureau of Indian Standards, 'Strategic Roadmap', (Web Page) https://www.services.bis.gov.in/tmp/ELECTRONICS%20AND%20IT%20DIVISION%20COUNCIL.pdf.
[62]Bureau of Indian Standards, 'LITD C : P5 - Quantum Computing Panel', (Web Page) https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/dgdashboard/committee_sso/composition/604/4.
[63] Bureau of Indian Standards, 'Standards National Action Plan (SNAP) 2022-27', https://www.bis.gov.in/wp-content/uploads/2023/05/SNPbookBilingual.pdf 55.

5.4.1 Key legislation

The NQS is cognisant of the risk that advanced quantum computing poses to much of existing public-key cryptography. The National Cyber Security Centre (NCSC UK) has stated that existing quantum computers cannot do this, but the current threat is rather the interception and stockpiling of encrypted data *now*, with an intention to decrypt in the future once quantum computing has developed that capability. The NCSC UK has issued guidance on the use of quantum key distribution (QKD) and 'quantum-safe cryptography' (QSC).[64] The guidance states that QKD is not suitable for military or government applications due to hardware requirements, and the use of *non-standardised* QSC is not recommended.[65]

The *Regulation of Investigatory Powers Act 2000* (UK) (RIPA) and the *Investigatory Powers Act 2016* (UK) (IPA) together comprise the main regime for interception of communications by UK public authorities. IPA allows for interception and acquisition of communications data, and RIPA governs the obtaining of electronic data protected by encryption. There is no specific mention of quantum technologies.

The *National Security Investment Act 2021* (UK) (NSIA) allows the UK government to scrutinise and intervene in certain acquisitions made by anyone, including businesses and investors, that could harm the UK's national security. Notification is required in 17 sensitive areas of the economy, *including* quantum technologies (as well as several other sectors likely to use quantum technologies, such as communications, computing hardware, and advanced materials.)[66]

The UK's Export Control Order 2008, which regulates the export of dual-use goods also applies to some quantum technologies.[67]

See Appendix D for detailed information on the UK's quantum policy and regulation.

5.4.2 Quantum standards development

The UK has recently (Nov 2023) established the Quantum Standards Network Pilot,[68] which appears to be focused on encouraging UK involvement in international standards systems rather than UK-specific standards. The UK National Cyber Security Centre (NCSC) has indicated that it is waiting on the NIST and ETSI post-quantum standards. The UK is also engaging in conversations on technical standards for quantum with organisations such as the IEEE Standards Association, IOS and IEC.[69]

5.5 Overview of US law and policy

The US has implemented a legislative framework (focusing heavily on government agencies) in anticipation of the widespread availability of quantum computing, cryptography and

---

[64] National Cyber Security Centre (UK), 'Preparing for Quantum-Safe Cryptography' (*Whitepaper*, 11 Nov 2020), https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

[65] It is possible that the UK will encourage QSC based on standards developed by either NIST or ETSI, when these are complete.

[66] Cabinet Office (UK), 'National Security and Investment Act: details of the 17 types of notifiable acquisitions' (*Guidance*, 6 Feb 2024) https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions

[67] From 1 April 2024, the export of '[q]uantum computers and components, as well as software and technology for the development or production of quantum computing' will be subject to the issuing of an export licence under the Export Control (Amendment) Regulations 2024 (UK).

[68] National Physical Laboratory (NPL), *Quantum Standards Network Pilot*, https://www.npl.co.uk/quantum-programme/standards/network-pilot, accessed 25 April 2024.

[69] Department for Science, Innovation and Technology, *National Quantum Strategy* (Mar 2023) https://www.gov.uk/government/publications/national-quantum-strategy#:~:text=A%2010%2Dyear%20vision%20and,the%20UK's%20prosperity%20and%20security ('NQS'). 30

communications. Policy is clearly driven by national security concerns as well as the economic benefits to be derived from quantum commercialisation.

5.5.1 Key legislation

In 2018, the Trump government established the National Quantum Initiative (NQS) under the National Quantum Initiative Act 2018, which concentrated on funding the research activities of NIST, the National Science Foundation and the Department of Energy. Funding for quantum activities has also been made available under the National Defense Authorisation Act (2019, 2020, 2022) (NDAA) for defence activities and the CHIPS and Science Act 2022 for semiconductor chips that can be used in quantum communications.

The US is attentive to the risks of quantum computing acting upon conventional encryption practices. On 21 December 2022 the *Quantum Computing Cybersecurity Preparedness Act 2022*[70] (QCCPA) became law in the US. Section 4 of the QCCPA puts into effect a multi-phase scheme guided by the Office of Management and Budget (OMB) to require federal agencies to (1) inventory and report any IT that is vulnerable to decryption by quantum computers; and (2) when NIST post-quantum cryptography (PQC) standards are issued, develop a plan to migrate their IT to PGC. While national security systems are exempt from the QCCPA (s5), requirements to migrate these systems to PQC standards are covered under an earlier executive order.[71] The NDAA also authorised the Department of Defense to 'increase the technology readiness level of quantum information science technologies under development in the United States, support the development of a quantum information science and technology workforce, and enhance awareness of quantum information science and technology'.[72]

There are various state and federal communications interceptions laws. One important example is the *Communications Assistance for Law Enforcement Act 1994* (CALEA). CALEA required telecommunications carriers to assist law enforcement in intercepting electronic communications where a court order exists. However, providers cannot generally be required to build in access points or decrypt data. The requirements now apply to some broadband and VoIP providers due to administrative action from the Federal Communications Commission. The Foreign Intelligence Surveillance Act 1978 and the PATRIOT Act have also been used to mandate the cooperation of phone companies in collecting connection metadata.[73] However, it is worth noting that US law enforcement has not been very successful in decryption of intercepted encrypted content: eg in 2019, law enforcement could not decrypt 438 out of 464 instances of interception encrypted communications.[74]

The Export Control Reform Act 2018 regulates the export of emerging and 'foundational' dual use technologies including some quantum technologies.

---

[70] H.R. 7535, main operative provisions 6 USC 1526.
[71] Joseph Biden Jr, 'Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems' *National Security Memorandum/NSM-8* (4 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/
[72] National Quantum Coordination Office, 'About the National Quantum Initiative' <*quantum|gov*> (Web Page) https://www.quantum.gov/about/
[73] Scott F Mann, 'Fact Sheet: Section 215 of the USA PATRIOT Act' (*Commentary*, Center for Strategic & International Studies, 27 Feb 2014) https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act
[74] https://crsreports.congress.gov/product/pdf/IF/IF11769

5.5.2 Quantum standards development

The US appears to primarily rely on national standards developed by its own standards body, the National Institute of Standards and Technology (NIST).[75] The National Security Agency released quantum algorithm requirements for national security systems in 2022. On 14 August 2024, NIST published its first three finalised post-quantum encryption standards,[76] incorporating its 'principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer'.[77]

See Appendix E for detailed information on the UK's quantum policy and regulation.

5.6 International standards

On 11 January 2024, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) announced the establishment of a joint technical committee (JTC 3) on quantum technologies, whose professed scope is to 'develop standards in the field of quantum technologies, and more particularly quantum computing, quantum simulation, quantum sources, quantum metrology, quantum detectors and quantum communications'[78] The ISO/IEC has already published a two-part standard relating to quantum key distribution requirements, evaluation and testing.[79] The IEEE Standards Association has also several quantum standards projects currently in development, including projects on post-quantum network security, post-quantum cryptography migration, and quantum computing.[80]

5.7 Summary of regulatory frameworks

Country	Import/Export of Dual Use Goods	Foreign Investment Rules	'Preparedness' Legislation
Australia	✓	✓	✗
United States	✓	✓	✓
European Union	✓	✓	✗
United Kingdom	✓	✓	✗

[75] See National Institute of Standards and Technology, Post-Quantum Cryptography Standardisation (Web Page) https://csrc.nist.gov/pqc-standardization.
[76] Department of Commerce, National Institute of Standards and Technology, *Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard*, 89 FR 66052 2024-17956, 66052-66057.
[77] National Institute of Standards and Technology, 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards' (*Media Release*, 13 August 2024) https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
[78] ISO, 'IEC and ISO launch new joint technical committee on quantum technologies' (*News*, 11 Jan 2024) https://www.iso.org/news/new-joint-committee-quantum-technologies
[79] Eg ISO/IEC 23837-1:2023 (Requirements) and ISO/IEC 23837-2:2023 (Part 2: Evaluation and testing methods).
[80] IEEE SA (Standards Association) 'Quantum Standards and Activities' (*Web Page*) https://standards.ieee.org/practices/foundational/quantum-standards-activities/ accessed 25 April 2024

India			

5.8 Conclusion

Quantum information technology applications present significant challenges to cybersecurity worldwide, with the potential to compromise encrypted systems. This policy brief focuses on Australia's preparedness in the face of evolving quantum technology applications. The brief recommends the following actions for Australian governments:

- Recommendation 1: Design adaptable quantum resilient regulation for the short, medium, and long term.

  The United States has the most advanced regulatory approach to quantum information technology among the countries reviewed. An examination of both procedural and substantive legal and regulatory tools, including mapping extant regulatory frameworks and determining whether they are operationally 'fit for purpose' in the face of quantum threats, would be a good place to begin the design process for adaptable, resilient regulation.

- Recommendation 2: Incorporate quantum standards into existing frameworks.

  Standards will be crucial as the quantum information technology ecosystem evolves over time. Australia is already involved at the highest levels in quantum standardisation. The mapping exercise in Recommendation 1 should be extended to standards to identify which frameworks are operationally 'fit-for-purpose' to adopt quantum standards as they are developed and adopted.

- Recommendation 3: Contribute more funding for Australian quantum-resilient development.

  Resilience is a governance and regulatory concept that can be applied in the context of emerging technologies to design strategies, substantive and procedural measures and overarching governance frameworks. Commencing research and development around the concept of quantum resilience would assist in the development of an adaptive approach. Researchers, developers, innovators, civil society, critical infrastructure industries and governments should be encouraged to contribute to this work through workshops, roundtables and in co-design networks, such as the TISN.

- Recommendation 4: Continue to advocate for standards development.

  Australia is already at the forefront of quantum standards development through the strategic initiatives and involvement of Australia's quantum researchers, the Department of Industry, Science and Resources, Standards Australia and the CSIRO. Researchers, developers, innovators and governments should continue to be encouraged to contribute to this important work through workshops, roundtables and co-design networks.

- Recommendation 5: Explore security and law enforcement capabilities.

The resilience of security and law enforcement capabilities to quantum information technologies will become a pivotal operational concern as quantum computing, communications and cryptography are deployed with uncertain impact and effect. We recommend a comprehensive, independent, expert exploration and inventory of security and law enforcement capabilities vis-à-vis the challenges and opportunities of quantum information technologies. This study should include impact on relevant national security law and policy frameworks, in addition to the forecasted impact of the technology itself. This study should seek to identify both substantive and procedural issues and concerns and make recommendations.

- Recommendation 6: Develop the Australian Public Service into a quantum workforce.

  The Australian Public Service needs to be trained, maintained and retained as a 'quantum-ready workforce'. This upskilling should include targeted recruitment of candidates with subject matter knowledge and expertise, training for current APS members, including targeted training for operational and policy teams. Lessons from the deployment of AI and other emerging technologies should be incorporated into a feasibility or skills study of the APS, including an initial survey of knowledge and expertise in new and emerging technologies, and recommendations. Research should also explore options for driving collaboration and knowledge exchange about quantum resilience in the APS, including secondments, bespoke training courses, scenario testing and tabletop exercises.

- Recommendation 7: Contribute to better understanding of the impact of quantum computing on other emerging technologies and associated risks.

  Australia is well placed to contribute to the understanding of the impact of quantum computing on other emerging technologies and their associated benefits and risks. Increasing domestic and international research collaboration with a multi-factorial, inter-disciplinary approach should be encouraged and funded, so that the interplay between various elements of the emergence of quantum technologies can be studied and policy responses developed and adapted.

- Recommendation 8: Promote collaboration and partnerships between public, private and research sectors to enable development and utilisation of tools for easier access and testing.

  In the quantum field, Australia has a strong track-record of successful collaboration and partnerships between the public, private and research sectors. What is needed now are a range of tools and mechanisms to test and utilise technologies and provide access to potential users and customers of the technology. We have seen joint-ventures, co-investment and sharing of complex resources already in the quantum ecosystem. But we recommend further funding, research and supportive policies to encourage interoperability, common standards and collaborative testing and improvement.

- Recommendation 9: Establish resilient quantum supply chain following a risk-based approach.

  Establishing a resilient quantum supply chain using a risk-based approach will be essential for future deployment of quantum technologies in the Australia economy. Current work being done on supply chain resilience should be expanded to include quantum technologies. For example, the Office of Supply Chain Resilience within the

Department of Industry, Science and Resources could be well placed to undertake this work by partnering with researchers, other government departments and agencies and industry participants to identify critical supply chain vulnerabilities in the quantum supply chain. Further research could also focus on the supply chain resilience framework and its efficacy and effectiveness for quantum technologies.

- Recommendation 10: Develop guidelines for users and vendors of quantum computing solutions (e.g., hardware requirements and impact on performance).

  There are challenges and benefits in developing guidelines for users and vendors of quantum computing solutions. Australia is well placed to develop robust guidelines that support safe and effective development and use of quantum computing solutions. There are successfully operating examples that provide a blueprint for such work. For example, the Australian Signals Directorate has had success with its Essential 8 Maturity Model guidelines for a graduated cyber security posture. In 2022-2023, ASD completed numerous Cyber Maturity Measurement Program assessments for federal, state and territory entities, and performed Cyber Security Uplift services. Private and public organisations can access the Essential 8.

In conclusion, the brief recognises the need for an adaptive approach to address the evolving challenges posed by quantum advancements. It serves as a foundation for further research and policy development.

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

Table of Contents

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

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.[2] 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.[3]

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.[4] Telstra's pledge followed the federal government's promised $26M as part of the of $1.1B National Innovation and Science Agenda.[5]

In 2018, a $6M investment was announced for industry, academia and government research agencies for quantum development for Defence. [6] 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.[7]

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 from China's cyber capabilities.[8] Since then, Australia has committed $15B to establish the National Reconstruction Fund under which $1B has been allocated to critical technologies including quantum technology.[9] The commitment to increasing funding for critical

---

[2] Gavin Brennen et al, 'An Australian Strategy for the Quantum Revolution' (May 2021) <http://www.aspi.org.au/report/australian-strategy-quantum-revolution>.
[3] Ibid.
[4] '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*').
[5] *Telstra* (n 3).
[6] '$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>.
[7] Ibid.
[8] 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>.
[9] Ibid. This information is taken from CN's note on Zotero from the source in (n 7).

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.[10] 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'.[11] 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.[12] 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.[13]

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.[14] The strategy aims to champion responsible innovation and ensure the growth of Australia's quantum industry supports economic prosperity whilst safeguarding our national interests.[15] There are 3 overarching themes for the strategy: 1) research and development; 2) investment, commercialisation and industry growth; 3) skills, social licence and diversity.[16]

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.[17]

2) Investment, Commercialisation and Industry Growth

Australia must develop and coordinate a national vision for quantum technology.[18] Investment must also be fostered by removing barriers and attracting investment for early stage companies.[19] 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.[20] Furthermore, lowering barriers of entry for start-ups, creating conditions to support a sustainable quantum ecosystem, creating quantum standards, and

---

[10] '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'*).
[11] Ibid.
[12] Judy Meiksin, 'Australia Launches Quantum Industry Roadmap' (2020) 45(12) MRS Bulletin 987.
[13] Ibid 987.
[14] *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*').
[15] Ibid.
[16] 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>.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.

using a holistic approach to create a full tech stack for quantum including algorithms and software should be considered in Australia's strategy.[21] 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.[22]

3) Skills, Social Licence and Diversity

It is also important to attract and retain expertise within Australia.[23] A Global Talent visa program is a means to attract international talent.[24] 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.[25] On a broader level, increasing awareness of quantum technology and building social licence should be pursued.[26] Diversity in skill and background in the quantum field should also be encouraged.[27]

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'.[28]

1.3 What competition/competing interests 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

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.[29]

B) Regional Powers

Quantum sensing technologies, including quantum magnetometers and quantum gravimeters, also have the potential to 'tip the balance between regional powers' through

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

improved defensive/offensive capabilities and the ability to outcompete nations by harvesting raw materials more efficiently.[30]

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.[31]

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'.[32] 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.[33] 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'.[34] 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.[35]

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.[36] On a commercial level, most focus is on the race to launch the first large-scale universal industrial quantum computer.[37] Players in the race include computing giants 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.[38] 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

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

> program, the Australian Centre for Quantum Computation and Communication Technology (CQC2T) and the Chinese quantum national laboratory for quantum information science.[39]

Professor Michelle Simmons[40] described global competition as 'the case of the tortoise and the hare. We very much see ourselves as a tortoise in this game.'[41] 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'.[42]

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.[43]

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'.[44]

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'.[45]

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.[46]

---

[39] Ibid 31.
[40] 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).
[41] Meiksin (n 11).
[42] Ibid.
[43] Gill et al (n 35) 2.
[44] Nathan K Langford and Simon J Devitt, 'At the Intersection Between Scalable Quantum Computing and Standardisation'.
[45] Perrier (n 31).
[46] Gill (n 35).

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.[47] Research is ongoing to find practical problems that can be efficiently solved on quantum computers.[48] '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.[49]

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.[50] The current record is IBB's 433 qubit processor.[51] 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.[52] 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.[53] 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.[54]

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.[55] 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.[56]

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 portfolio-risk optimisation, fraud detection and robotics.[57] 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'.[58] 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

[47] Ibid 28.
[48] Ibid.
[49] Ibid.
[50] Langford (n 43).
[51] '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>.
[52] 'From Little Things' (n 33).
[53] Ibid.
[54] Ibid.
[55] Perrier (n 31).
[56] Ibid 7-8.
[57] Gill (n 35).
[58] Ibid 29.

intensive problems by quantum machine learning algorithms can reduce down energy cost, and the dependency on fossil-fuels will decrease'.[59]

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'.[60] 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.[61] A cable length of 250km is considered a significant achievement.[62]

In Australia in 2013, the quantum network project was established to connect Parliament House with other government organisations in Canberra.[63] 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.[64] 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.[65] 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.[66] 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.[67]

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'.[68] 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'.[69]

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.[70] Applications include airport security, hydrographic surveying, battlefield medicine and nonproliferation compliance.[71]

The following technologies are of interest:

---

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

A) Quantum Radar

Two approaches to quantum radar have been identified. Firstly, interferometric which targets images more clearly and further away.[72] This method, however, may not be reliable for stealth platforms.[73] 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.[74] 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.[75] Beyond defence, the greatest use case of quantum radar may be in space.[76]

B) Atomic Clocks

The atomic clock is the most accurate clock and has applications in defence and space.[77]

C) Quantum Magnetometers

Quantum magnetometers ('SQUIDs') precisely measure magnetic fields.[78] However, there lies several practical difficulties when used for defence purposes.[79] SQUIDs may be better utilised for medical imaging with commercialized 'NV diamonds', battlefield medicine or magnetic navigation.[80]

D) Inertial Navigation Systems

Inertial navigation systems are precise navigational systems and can compensate for loss of GPS guidance if GPS signals are jammed.[81]

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'.[82] 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.[83] Although, developments in quantum sensing will 'make it easier to build quantum systems that underlie quantum computers and communication relays'.[84]

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

[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.

the operational RSA encryption if a large-scale fault-tolerant quantum computer were developed.[85] 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.[86] However, 'regardless of key length, the future of … Rivest-Shamir-Adleman (RSA) is bleak'[87] 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).[88] Therefore 'post-quantum encryption methods need to be formulated which can withstand an industrial quantum computer'.[89] 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.[90]

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.[91]

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.[92] Applications of post-quantum cryptography range from government-use to secure identify proofs, in information and communication technologies including networks, networking equipment, servers and network services (eg cloud services), and automation in healthcare, vehicles, agriculture and aviation.[93] 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.[94] Cryptographic agility, 'a design feature that enables future updates to cryptographic algorithms and standards without the need to modify or replace

---

[85] Gill (n 35) 29.
[86] 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>.
[87] Ibid 17.
[88] 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/>.
[89] Ibid 29.
[90] Perrier (n 31) 8.
[91] Gill (n 35).
[92] Ibid.
[93] Ibid 17.
[94] Ibid 18.

the surrounding infrastructure',[95] must also be strongly considered.[96] 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.[97] 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'.[98]

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'.[99]

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'.[100] Governance should also recognise the 'need to treat fostering innovation and QIT (quantum information technology) development as an explicit goal of governance themselves'[101] 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'.[102] Quantum governance must be considered within the broader nexus and hierarchy of technology governance in general.[103] 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 policy objectives.[104] We must also consider how quantum technology sits in intellectual property regimes.[105]

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.[106] Although,

---

[95] 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/
[96] Gill (n 35) 35.
[97] Warren Armstrong, 'SOCRATES WP8 – Request for feedback – DRAFT quantum policy brief' Email to authors, sent 15 Jan 2024.
[98] Ibid.
[99] Ibid.
[100] Perrier (n 31) 3.
[101] Ibid 40.
[102] Ibid.
[103] Perrier (n 31).
[104] Ibid.
[105] Ibid.
[106] Ibid.

governance methods must be empirical – dynamic and responsive to the evolution of the technology.[107]

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.[108] He also sees governance as managing and responding to negative risks in the form of a risk-management approach.[109] Overall, there must also be a balance between prescriptive and principles-based approaches with varying degrees of specificity.[110] However, there are strong arguments for the creation of specific laws as they are more actionable.[111]

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.[112]

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.[113] 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.[114]

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.[115]

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 between the two countries.[116]

On 13 February 2024, the Multilateral Dialogue on Quantum was announced between Australia and 12 other countries, to help develop a global quantum ecosystem.[117]

---

[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Ibid.
[111] Ibid.
[112] Ibid 12.
[113] Perrier (n 31).
[114] Ibid.
[115] 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>.
[116]The Hon. Ed Husic, Minister for Industry and Science, 'Australia and UK sign Quantum Joint Statement' (Media Release, 3 November 2023).
[117] 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>.

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.[118] 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.[119]

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.[120] Often they must balance competing interests of various stakeholders including consumers, private sector companies and government.[121]

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.[122] 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.[123] Internal quantum governance in corporations can occur through risk management, auditing/checks/reviews and impacted assessments.[124] Most companies in the quantum sector have objectives aligning with the development of quantum hardware, quantum software, and infrastructure related to quantum technology.[125] 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.[126]

Academia is an instrumental player in quantum with contributions made to formal governance procedures (eg committees, treaty development) and soft measures (eg principles development).[127] Quantum governance within academia includes institutional policies and guidelines (eg research policies), risk-management frameworks, ethical frameworks assessing the impact of technology research, and the ability to dictate the terms and conditions of funding or grants for projects.[128]

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.[129] 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.[130]

---

[118] Ibid.
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Ibid.
[126] Ibid.
[127] Ibid.
[128] Ibid.
[129] Ibid.
[130] Ibid.

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.[131] The media has a role in setting agendas, highlighting risks and drawing attention to issues requiring governance responses.[132] 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.[133] 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.[134] 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.[135]

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.[136] 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.[137] They are also important for translating theoretical research into application and act as conduits for coordination between academia and industry.[138] Technical communities play a key role particularly in the early stage of quantum governance.[139] 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.[140] This is because the technology poses geostrategic risks if disseminated and distributed to potential adversaries.[141] Currently legislative and regulatory instruments which manage national security-related dual-use technologies do exist, such as for nuclear, biotechnology and cybersecurity-related technologies.[142] These can be used as a basis for QIT dual-use regulation.[143]

(1) In addition, many jurisdictions regulate dual-use risks with export controls such as foreign investment export controls.[144] 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.[145] This

[131] Ibid.
[132] Ibid.
[133] Ibid.
[134] Ibid.
[135] Brennen (n 1).
[136] Perrier (n 31).
[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] Brennen (n 1).
[141] Perrier (n 31).
[142] Ibid.
[143] Ibid.
[144] Ibid.
[145] Ibid.

scope is extremely broad and can cover quantum computing, sensing, encryption and communications technologies.[146] 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.[147] This is a valid concern 'given the importance of foreign direct investments and export markets for the growth of Australia's quantum industry'.[148] Additionally, export limitations can limit the availability and capability of a key principle of cryptosystem design which holds *against* a 'security by obscurity' approach.[149] A common modern use of the so-called Kerckhoff's principle[150] 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.[151]

The Defence and Strategic Goods List[152] 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 ethical guidelines or principles 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.[153] In 2020, the 'global quantum security coalition' was launched to work to promote safe and secure quantum technology.[154] 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.[155] 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.[156] Furthermore, the WEF recognises existing standards in other fields may apply to quantum technology, but that there are also distinct governance considerations particular to quantum.[157]

3.3.2 National

In Australia there is no ethical framework for quantum, however, the CSIRO Quantum Technology Roadmap suggests some guidelines.[158]

---

[146] Ibid.
[147] Ibid.
[148] *National Quantum Strategy Issues Paper* (n 15).
[149] Eric Diehl, *Ten Laws for Security* (Springer International Publishing AG, 2016) <http://ebookcentral.proquest.com/lib/unsw/detail.action?docID=4744597>. Ch 3.
[150] 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>.
[151] Warren Armstrong, 'SOCRATES WP8 – Request for feedback – DRAFT quantum policy brief' Email to authors, sent 15 Jan 2024.
[152] https://www.legislation.gov.au/F2021L01198/latest/text
[153] 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>.
[154] Brennen (n 1).
[155] CSIRO (n 142).
[156] Ibid.
[157] Ibid.
[158] Brennen (n 1).

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').[159] Previously, standards were organically adopted in an ad hoc consensus through publications and IBM'S OpenQASM (quantum language).[160] 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.[161] Hardware standardisation is also near non-existent since quantum computers are not designed to be interoperable and not enough is known.[162] For emerging critical technologies such as quantum technology, standardisation is crucial to open new markets, ensure interoperability, facilitate international trade, and manage security risks.[163]

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'.[164]

Notable developments include:

- The ISO/IEC JTC 1 establishing a working group on Quantum Computing (WG14).[165]
- 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.[166]
- The IEC creating the Standardisation Evaluation Group (SEG) 14 on Quantum Technology to summarise use cases and propose a roadmap for standardisation.[167]

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

- Quantum key distribution networks - control & management Y.3804 (09/20);[168] and
- Quantum noise random number generator architecture[169]

Challenges relating to standardisation on an international scale include that, by design, massively multilateral, committee-driven processes 'operate slowly and with considerable inertia' and consequently struggle to match the pace of rapid progress made in quantum computing.[170] An additional challenge is the lack of overlap between experts in standardisation and quantum computing.[171]

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

---

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

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.[172] For example, the IEEE has existing standards for protocols on quantum communication, QIT definitions, performance metrics and benchmarking.[173]

In Australia, Government and Industry have sought to coordinate an Australian standards position in CET including quantum technology.[174] 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.[175] 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.[176] These papers will explore current worldwide quantum standardisation efforts and map the current and emerging standards needs for quantum technologies.[177]

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.[178]

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'.[179] The NISQ era is the current state of quantum computer and implies that quantum computers of this time 'don't have many useful

[172] Ibid.
[173] Perrier (n 31).
[174] *Critical and Emerging Technologies* (n 9).
[175] Ibid.
[176] Ibid.
[177] Ibid.
[178] Langford (n 43).
[179] Gill (n 35) 1.

qubits and possess high error rate'.[180] 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.[181]

Another practical challenge for quantum computing is that many quantum machines are 'bulky' and must be 'kept at superconducting temperatures'.[182] 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.[183] 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'.[184]

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.[185]

4.1.2 Barriers to Development

In Australia, barriers to development include Australian quantum technologists moving to work in overseas quantum industries,[186] and higher barriers of entry for start-ups due to difficulties accessing infrastructure and less developed general business services.[187] 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.[188] This gives 'rise to issues of equity, access and distribution of benefits and risks, especially for under-resourced nations and stakeholder groups'.[189] An 'uneven distribution of skills and knowledge' relating to quantum computing can also exacerbate and create new 'inequalities in terms of technology access'.[190]

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.[191] Potentially, when used alongside classical computing technology, problems already faced today may be amplified.[192] There is also a lack of risk-assessment frameworks to mitigate, control and enable a timely response to risks.[193]

---

[180] 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/>.
[181] Gill (n 35) 2.
[182] Ibid 29.
[183] Ibid 34.
[184] Ibid.
[185] Ibid 28.
[186] Brennen (n 1).
[187] *National Quantum Strategy Issues Paper* (n 15).
[188] CSIRO (n 142) 4.
[189] Ibid 16.
[190] Ibid.
[191] Ibid 13.
[192] Ibid 4.
[193] Ibid 13.

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.

Appendix B - European Union Quantum Regulation and Policy[1]

1. What has the EU done to date on quantum strategy, policy and legislation?

Twenty-seven EU countries have signed a declaration agreeing to explore how to develop and deploy a quantum communication infrastructure (QCI) within the next ten years. The QCI will be the backbone of Europe's Quantum Internet.[2]

- On 06 December 2023 EU published the **European Declaration on Quantum Technologies**, which outlines the ultimate aim of making Europe the 'quantum valley' of the world.

[1] Prepared by Megha Uppal with contributions by Jennifer Westmorland, UNSW Allens Hub for Technology, Law & Innovation.

[2] European Commission, 'The future is quantum: EU countries plan ultra-secure communication network', *News & Views* (Web Page, 13 June 2019) <https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>.

- In October 2023 European Commission adopted the recommendation to **carry out risk assessments** on four critical technology areas including advanced **semiconductors and quantum**.[3]
- On the 18 April 2023, the European Commission proposed the **EU Cyber Solidarity Act**,[4] to improve the preparedness, detection and response to cybersecurity incidents across the EU. The proposal includes a **European Cybersecurity Shield** to protect, detect, defend and deter cyber threats. Under 'protect' and its 'technological front' they are **'working in particular on the issue of post-quantum encryption'**.[5]
- The **European Chips Act** entered into force in September 2023**.** It will **bolster Europe's competitiveness and resilience in semiconductor technologies and applications**, and help achieve both the digital and green transition. It will do this by strengthening Europe's technological leadership in the field.[6]
- The **European Commission's Quantum Strategy** includes:

1) **Quantum Flagship**.[7] Launched in 2018 for 10 years and a budget of €1 billion, its goal is to consolidate and expand European scientific leadership and excellence in this research area, to kick-start a competitive European industry in Quantum Technologies and to make Europe a dynamic and attractive region for innovative research, business and investments in this field (not only research but also go-to-market).

2) The **European Quantum Communication Infrastructure (EuroQCI) Initiative**.[8] Since June 2019, all 27 EU Member States have signed the EuroQCI Declaration, agreeing to work together, with the Commission and with the support of the European Space Agency, towards the development of a quantum communication infrastructure covering the whole EU (EuroQCI).

3) The **European High Performance Computing Joint Undertaking (EuroHPC JU) regulation** was adopted in 2021 and is a joint initiative between the EU, European countries and private partners to **develop a World Class Supercomputing Ecosystem** in Europe. To date, **five supercomputers are now fully operational.** EU plans to invest of €7 billion in this till 2033.[9]

- In 2021, **the European Commission published 'European ambitions on Quantum research and innovation'**, which listed these as a part of the **EU quantum technology (QT) ecosystem**: Quantum Flagship, QUANTERA, QTSPACE COST Actions, EURAMET,

---

[3] European Commission, 'Commission recommends carrying out risk assessments on four critical technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies', *Press Release* (Web Page, 03 October 2023) < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735>.

[4] Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents Proposal 2023 (EU) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209>.

[5] European Commission, 'A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton', *Speech* (Web Page, 05 April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145>.

[6] European Commission, 'European Chips Act', <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en#:~:text=The%20Chips%20Act%20proposes%3A,experimentation%20of%20cutting%2Dedge%20chips>.

[7] *Quantum Flagship* (Web Page) <https://qt.eu/about-quantum-flagship/>.

[8] European Commission (n 2).

[9] European Commission, 'The European High Performance Computing Joint Undertaking', *Policies* (Web Page) <https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing-joint-undertaking>.

Digital EU Programme, QKD Testbed, QT in Space, EESA Scylight, and National/Regional initiatives.[10]

- However, in March 2023 it was noted that European Quantum Technologies ecosystem = Quantum Flagship + Quantera +EuroQSM + EuroQCI + EuroQCS + ERC/Marie Skłodowska Curie actions[11]
- **Current funding instruments for EuroQCI** include the **Digital Europe** programme and the **Connecting Europe Facility**, as well as **Horizon Europe**, **ESA**, and **national funds**, including the **Recovery and Resilience Facility**. EuroQCI will be integrated in the proposed Secure Connectivity Programme.

2. How is the EU approaching quantum technology in strategy and policy?

- Its aim to be a global leader in quantum technologies is guiding EU's strategy and policy. This means that they are looking at covering all aspects, such as education, research, skill development, industry and economics, and geopolitics. As noted in Q1, several initiatives have been undertaken for this objective.
- EU's **Digital Decade policy:** 2030 targets include 'first computer with quantum acceleration' and Multi-country Projects (MCP) for 'secure quantum communication'.[12]
- The **European Declaration on Quantum Technologies**, outlines the ultimate aim of making Europe the 'quantum valley' of the world.

3. Does the EU have quantum specific legislation? If so, what does it cover? What does it do?

Does not seem to be the case, however, it has adopted legislations that are not created specifically for quantum but include quantum due to overlapping concerns.

4. What technologies are mentioned in the EU's quantum strategy and policy?

- Quantum computing, quantum communication, quantum sensing and metrology, quantum simulations. The ultimate goal is quantum internet.[13]
- The EU **Competence Framework** (April 2023) 'can be used to facilitate the planning and design of education and training projects in Quantum Technologies and provides an instrument to compare different educational approaches'.[14] **The direct inference is that technologies enlisted here will be a part of EU's policy and strategy beyond the education and training stage.** The long list has several categories, such as quantum hardware, quantum computing and simulation, quantum sensors and imaging sensors, quantum communication and networks; and these have their own sub-categories.

---

[10] Pasacal Maillot, 'European ambitions on Quantum research and innovation', *Quantera* (2021) <https://quantera.eu/wp-content/uploads/2021/11/Pascal_MAILLOT.pdf>.

[11] CEN-CENELEC Focus Group on Quantum Technologies, 'Standardization Roadmap on Quantum Technologies', (March 2023) <https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf>.

[12] European Commission, 'Europe's Digital Decade: digital targets for 2030', *Strategy and Policy* <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en>.

[13] European Commission, 'Quantum technologies and the advent of the Quantum Internet in the European Union — Brochure', *Library* (Web Page, 23 September 2019) <https://digital-strategy.ec.europa.eu/en/library/quantum-technologies-and-advent-quantum-internet-european-union-brochure#What>.

[14] Quantum technology Education, 'European Competence Framework for Quantum Technologies', (Web Page) <https://qtedu.eu/european-competence-framework-quantum-technologies>.

5. What competition/competing interests are mentioned/raised/identified in the EU's quantum strategy and policy?

- A common ambition across documents, reiterated by Andrus Ansip, Commission Vice-President for the Digital Single Market, 'Europe is determined to lead the development of quantum technologies worldwide'.[15] It is acknowledged across the EU communication that Europe is currently behind the US and China in developing quantum technologies, and it wants not just match, but surpass their development.
- Sensitive and immediate risks related to technology security and technology leakage have often been cited as the possible negative outcomes of quantum technologies.[16] For example, it has been noted that cryptography will be one of the most vulnerable fields, posing risk to how sensitive information is stored today.[17]

6**. Is there consideration of the impact of quantum computing and quantum communications?**

Yes.

- advances in quantum computing put at risk Europe's cybersecurity by rendering obsolete current encryption systems and creating new cybersecurity challenges[18]

Positive impact:

- Quantum Communication can help to establish highly secure communication channels for information exchange
- QKD would provide highly secure key exchange protocols to protect sensitive communications, data and critical infrastructures
- Quantum sensors and quantum metrology hold substantial promise, offering the potential for transformative applications in the use of measurement devices in forensics, detection and decision making.
- , there are data analysis, machine learning and artificial intelligence, which may benefit from quantum algorithms for more efficient processing, e.g. to process large amounts of data at scale
- Quantum devices may offer new opportunities for digital forensics
- Password guessing can help authorities maintain safety and security

Negative impact:

- 'save now decrypt later' could lead to new types of ransom demands or a flood of sensitive information being available for crimes such as social engineering and phishing
- Side-channel attacks and fault injection attacks are types of cryptanalysis techniques aiming to weaken or break the security of a cryptosystem
- Parties with malicious intent could make use of quantum communication channels to evade law enforcement detection and prevent criminal prosecution

---

[15] European Commission, 'Quantum Technologies Flagship kicks off with first 20 projects', *Press Release* (Web Page, 29 October 2018) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6205>.

[16] European Commission (n 3).

[17] Europol Innovation Lab, *The Second Quantum Revolution: The impact of quantum computing and quantum technologies on law enforcement* (Report, 2023

[18] Andrea G. Rodríguez, 'A quantum cybersecurity agenda for Europe', (Discussion Paper, European Policy Center, 17 July 2023) <https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf>.

- Password guessing can pose serious threats if used by parties with malicious intent[19]

6. Does the EU's approach to quantum consider/mention quantum-safe encryption, quantum cryptography?

Yes.

- Q1, Cyber Solidarity Act
- Commission of the European Communities supported 'Post-Quantum Cryptography for Long-Term Security', a project focused on developing post-quantum cryptographic techniques.[20]
- As noted in Q5, quantum cryptography has received substantial focus across EU reports due to the vulnerability it will cause for sensitive data, and there is a unanimous call for strengthening cybersecurity to mitigate these risks
- In April 2024, the European Commission published a Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography[21]. This paper builds on the policy objectives set out in the EU Cybersecurity Strategy. The key recommendations are that:
    - Europe should switch to Post-Quantum Cryptography as swiftly as possible, to remove the known vulnerabilities of current asymmetric cryptography and enhance robustness against the threats posed by the malicious use of quantum computers.
    - Member States should develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, which should specify clear goals, actions, milestones, and timelines. This should result, within two years, in the definition of a joint Post-Quantum Cryptography Implementation Roadmap.
    - Member States should develop common European standards and develop a framework for identifying and selecting Post-Quantum Cryptography algorithms to be deployed in the digital networks and services across the Union.
    - Member States should continue to cooperate actively with their international strategic partners to develop international standards that will ensure interoperability of communications going forward.

7. What does the EU's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?

- The EU believes that new quantum computers will threaten the current encryption practices. Implementing new crypto algorithms will increase the security of their systems.[22]
- European Policy Center has emphasised the urgent need for a new EU Coordinated Action Plan to facilitate quantum-secured technologies before 'Q-Day' – the point at which quantum computers are able to break existing cryptographic algorithms.[23]

---

[19] Europol Innovation Lab (n 17).
[20] European Commission, 'PQCRYPTO: an EU-funded project success story', *Projects Story* (Web Page, 24 August 2018) <https://digital-strategy.ec.europa.eu/en/news/pqcrypto-eu-funded-project-success-story>.
[21] European Commission, 'Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography', Policy and Legislation (Web Page, 11 April 2024) < https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography>.
[22] European Commission – ENISA Telecom Security Forum Slide Deck
[23] Rodríguez (n 18).

- Also refer to Q5 and Q7.

8. Does the EU'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?

Standardisation framework is mentioned in Q10 and Dual-use regulation in Q12. EU's approach does not directly mention any other regulatory or legal frameworks, yet.

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

- Ongoing: no clear results. Likely to follow NIST (US) standards.[24]
- **Rolling Plan for ICT standardisation: Quantum Technologies (RP2023)**[25] suggests nine 'Actions' to be undertaken for creating standards for quantum technologies, from European Committee for Standardization (CEN) & European Committee
- for Electrotechnical Standardization (CENELEC) identifying the most important needs for standardisation to SDOs increasing coordination efforts in Europe and internationally to avoid duplication of efforts.
- CEN-CENELEC released a **Standardization Roadmap on Quantum Technologies** in March 2023.[26]
- ETSI has an industry specification group on quantum key distribution (QKD).[27] Standards ETSI GS QKD 014 (Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API) and GS QKD 004 (Quantum Key Distribution (QKD); Application Interface) are emerging as de facto standards for how to interface quantum key distribution systems with new and legacy hardware and software[28]

10. Does the EU's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected?

Yes.

- **Quantum computers will break the most used cryptographic systems:** Research suggests that by 2026, there is a 1 in 7 chance that, which will go as high as 50% by 2031. However, research published in early 2023 by Chinese scholars suggests that it could happen even before.[29] For example, current-use cryptographic standards for webpages of all European Institutions, financial transactions, e-passports, VPNs have been broken at the post-quantum security level.
- Cyberattacks, known as **'harvest attacks'** or **'download now-decrypt later':** cybercriminals and geopolitical adversaries are rushing to obtain sensitive encrypted

---

[24] Ibid.
[25] European Commission, 'Quantum Technologies (RP2023)', *Rolling Plan for ICT standardisation* (Web Page) <https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/quantum-technologies-rp2023#:~:text=Quantum%20Technologies%20(QT)%20include%20a,quantum%20communication%20and%20quantum%20computing>.
[26] CEN-CENELEC Focus Group on Quantum Technologies (n 11).
[27] ETSI, 'Industry Specification Group (ISG) on Quantum Key Distribution (QKD)' *QKD* https://www.etsi.org/committee/1430-qkd.
[28] Email from Dr Warren Armstrong, Director of Engineering, Quintessence Labs, email to authors, 'SOCRATES WP8 - Request for feedback – DRAFT quantum policy brief' 16 January 2024, 3:28 PM.
[29] Rodríguez (n 18).

information that cannot be read today to be de-coded once quantum computers are available.

- Quantum computers will increase the probability of intellectual property theft or data breaches
- Cryptography attacks can also negatively impact the European economy and the competitiveness of European companies. + Cyberattacks on critical infrastructure can have far reaching consequences, with spillover effects on other economic sectors and international security
- Financing is one of the most critical chokepoints for the EU's quantum ambitions[30]

11. Does the EU's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

- EU introduced a **dual-use regulation in 2021**, Regulation (EU) 2021/821.[31] It sets out rules throughout the EU to control exports, brokering, technical assistance, transit and transfer of dual-use items.
- Compilation of national control lists under Article 9(4) of Regulation (EU) 2021/821[32] **includes quantum computers and related electronic assemblies and components, qubit devices and qubit circuits containing or supporting arrays of physical qubits, quantum control components and quantum measurement devices**; as well as the technology for their development or production.

12. Are there any gaps identified in the EU's approach to quantum technology? Are there any barriers and challenges identified in the EU's approach? Are there any advantages to the EU's approach?

Few gaps/barriers/challenges identified:

- In recognising challenges and/or risks of quantum technologies, EU has focussed significantly on cryptography. Comparatively, focus on any other challenges and risks is negligible
- Lack of quantum-specific legislation despite multiple policies and initiatives already underway

Advantage: EU has recognised the significance of quantum technologies across sectors – research, economic, political – and plans to advance in all at the same pace. This would ensure that their development of quantum technology progresses in a balanced manner, without any sector lagging and slowing down the others.

Notes

- The European Quantum Communication Infrastructure Initiative has a space component.

13. Summary

- **To recap, EU has strong policies in place for its quantum strategy. However, in terms of regulation it has only instated dual-use regulation and standardisation framework is**

---

[30] Georg E. Riekeles, 'Quantum technologies and value chains: Why and how Europe must act now', (Discussion Paper, European Policy Center, 23 March 2023) < <https://www.epc.eu/content/PDF/2023/Quantum_Technologies_DP.pdf>.

[31] *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)* [2021] OJ L 206 11.6.2021/1.

[32] Ibid art 9(4).

underway, there is no quantum-specific regulation yet. There is a strong focus on quantum technologies making current cryptography practices vulnerable. EU aims to be a global leader in quantum technologies, and channel its research manpower for the same, and to eventually achieve economic gains from the application of these technologies.

- The latest **European Declaration on Quantum Technologies** provides a good overview of EU's approach. The 11 signatory member states 'recognise the strategic importance of quantum technologies for the scientific and industrial competitiveness of the EU and commit to collaborating on the development of a world-class quantum technology ecosystem across Europe, with the ultimate aim of making Europe the 'quantum valley' of the world, the leading region globally for quantum excellence and innovation'. [33]
- EU seeks to 'maintain a leading global position, safeguard its strategic assets, interests, autonomy, and security, and avoid a situation of strategic dependency on non-EU sources…and build its own capacity to research and develop quantum technologies and produce devices and systems based on them, while at the same time investing in the whole quantum stack, from hardware to software and to applications and standards'.
- **Briefly, it has recognised the following in relation to quantum technologies:** economic significance, develop a world-class ecosystem in supercomputing and quantum computing, industrial exploitation, a secure quantum communication infrastructure, being at the cutting edge of quantum capabilities by 2030.
- At the same time, it is looking at international cooperation, such as the Trade and Technology Councils (TTCs) with the US and India.

[33] European Commission, 'European Declaration on Quantum Technologies', *Policy and Legislation* (Web Page, 06 December 2023) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies>.

APPENDIX C: INDIA'S QUANTUM POLICY AND REGULATION[1]

Table of Contents

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

1. What has India done to date on Quantum strategy and policy?

India is the seventh country to launch a quantum program.[2] The country's first quantum computing-based telecom network link was launched in March 2023.[3] Presently, India has nearly a hundred quantum projects, of which about 92 percent are sponsored by the Centre.[4]

The execution of India's quantum strategy is meted out by different **governing bodies**:

- The Ministry of Science and Technology (MoS&T),[5] Department of Science and Technology (DST)[6] and Centre for Development of Telematics (C-DOT).[7] DST is at the forefront of R&D initiatives under India's quantum strategy.
- The Ministry of Electronics and Information Technology (MEITY)[8] is also a major stakeholder in R&D initiatives, through its divisions like the Centre for Development of Advanced Computing (C-DAC).[9]
- In 2020, the Ministry of External Affairs (MEA)[10] established a new department -- New, Emerging and Strategic Technologies (NEST), to engage in technology diplomacy and deal with the foreign policy and international legal aspects of new and emerging technologies.
- The Prime Minister's Science, Technology and Innovation Advisory Council (PM-STIAC)[11] assesses the status in specific science and technology domains, comprehends challenges, formulates interventions, develops a futuristic roadmap, and advises the PM accordingly.
- Department of Space/Indian Space Research Organisation (DoS/ISRO)[12]
- Department of Atomic Energy (DAE)[13]
- Defence Research and Development Organisation (DRDO)[14]

---

[2] Kalyan Ray, 'India to Become Seventh Nation to Have National Quantum Mission', *Deccan Herald* (online, 20 April 2023) <https://www.deccanherald.com/india/india-to-become-seventh-nation-to-have-national-quantum-mission-1211108.html>.
[3] Press Trust of India, 'India's First Quantum Computing-Based Telecom Network Link Now Operational: Ashwini Vaishnaw', *The Economic Times* (online, 27 March 2023) <https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99026697.cms?from=mdr>.
[4] Press Information Bureau, *Industry Will Be Expected to Be a Major Resource Contributor in All the Future StartUp Ventures and Other New Technology Initiatives, Says Union Minister Dr Jitendra Singh* (Press Release, 5 October 2023) <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1964650>.
[5] 'About Ministry of Science & Technology, Government of India', *Ministry of Science & Technology, Government of India* (Web Page) <https://most.gov.in/about-us.html>.
[6] 'Department Of Science & Technology | विज्ञान एवं प्रौद्योगिकी विभाग', *Government of India, Ministry of Science and Technology* (Web Page) <https://dst.gov.in/>.
[7] *Centre for Development of Telematics* (Web Page) <https://www.cdot.in/cdotweb/web/home.php>.
[8] *Ministry of Electronics and Information Technology* (Web Page) < https://www.meity.gov.in/>.
[9] *Centre for Development of Advanced Computing* (Web Page) <https://www.cdac.in/index.aspx>.
[10] *Ministry of External Affairs* (Web Page) <https://www.mea.gov.in/>.
[11] *The Prime Minister's Science, Technology and Innovation Advisory Council* (Web Page) <https://www.psa.gov.in/pm-stiac>.
[12] *Department of Space/Indian Space Research Organisation* (Web Page) <https://www.isro.gov.in/index.html>.
[13] *Department of Atomic Energy* (Web Page) <https://dae.gov.in/>.
[14] *Defence Research and Development Organisation* (Web Page) <https://www.drdo.gov.in/>.

1.1 National Quantum Mission (NQM)

- In April 2023 India approved its National Quantum Mission (NQM), committing INR 6,000 crore (USD 730 million) to the development of quantum technology for the next eight years. The NQM has four major domains -- Quantum Computing, Quantum Communication, Quantum Sensing & Metrology, and Quantum Materials & Devices. The government is setting up four R&D thematic hubs (T-hubs), one for each domain.
- The NQM also has a Quantum Entanglement Exchange (Quantum EE) program,[15] which aims to facilitate the exchange of students, researchers, and professionals in the field of quantum technologies, and has ongoing partnerships with the US and Japan.
- 'NQM has the potential to elevate the country's technology development ecosystem to a level of global competitiveness. The mission would greatly benefit various sectors including communication, health, financial, energy with applications in drug design, space, banking, security etc. The mission will also provide a huge boost to national priorities like Digital India, Make in India, Skill India and Stand-up India, Start-up India, Self-reliant India and Sustainable Development Goals (SDG).'[16]
- As of July 2023, MoS&T said that 'the framework on the funding outlay and operations to develop the quantum computing ecosystem is likely to be published by August [2023]'.[17] There hasn't been an update on this since.

1.2 Quantum Technology Roadmap

- In January 2024, MEITY announced a draft of its first Quantum Technology Roadmap.[18] Eight areas of focus have been allocated project milestones between 2023 and 2047:
  - Quantum Research and Development
  - Quantum Computing
  - Quantum Simulation
  - Cryptography and Cybersecurity
  - Quantum Communication
  - Quantum Sensing and Metrology
  - Quantum Strategic Applications
  - Quantum Standardization

Cryptography and Cybersecurity have been given the highest priority, with a completion date of 2028, while research and development efforts are expected to continue until 2047. Feedback submissions are currently being reviewed by MEITY.

---

[15] Department of Science and Technology, 'International Collaborations', *National Quantum* (Web Page) <https://dst.gov.in/quantum-entanglement-exchange-programme>.
[16] Department of Science and Technology, 'National Quantum' (Web Page) <https://dst.gov.in/national-quantum-mission-nqm>.
[17] Shouvik Das, 'India to Issue Framework on $730 Mn Quantum Mission in Aug' (18 July 2023) *mint* <https://www.livemint.com/technology/tech-news/india-to-issue-framework-on-730-mn-quantum-mission-in-aug-11689675255958.html>
[18] https://www.meity.gov.in/writereaddata/files/Quantum%20Technologies%20Roadmap.pdf

1.3 Laboratories and Research Centres

- MEITY has collaborated with Amazon Web Services (AWS) to establish the Quantum Computing Applications Lab (QCAL). This lab will assist the scientific, academic, and developer communities in their R&D on quantum technologies.[19]
- **C-DOT** launched a **Quantum Communications Lab** in 2021, which developed a Quantum Key Distribution (QKD) solution capable of supporting a distance of more than 100 kilometres on standard optical fibre.[20] C-DOT had previously developed Post Quantum Cryptography Encryptors (PQCE) amongst other quantum technologies, and offers a complete portfolio of indigenous quantum secure telecom products and solutions.
- In February 2023, a joint team from **DRDO and IIT Delhi** demonstrated a Quantum Key Distribution (QKD) link.
- The Quantum Measurement and Control Laboratory (QuMaC) at **Tata Institute of Fundamental Research (TIFR)** primarily investigates quantum phenomena in superconducting circuits,[21] and has already made a 5-qubit quantum computer. TIFR is under the DAE.
- The Quantum Information and Computing (QuIC) lab at the **Raman Research Institute** (RRI), Bangalore is one of the first labs in India to manufacture and establish the usage of heralded and entangled photon sources towards various applications in quantum technologies.[22] The **lab has also collaborated with ISRO**.
- Samsung Semiconductor India Research and the **Indian Institute of Science (IISc)** signed an MoU to set up a quantum technology lab. The lab will focus on integrating cryogenic control chips with qubits, single photon sources and detectors while addressing reliability challenges in quantum technologies.[23]
- The **IIT Madras** has established the Center for Quantum Information, Communication and Computing (CQuICC) with an objective of developing secure quantum communications, including quantum key delivery, quantum random number generation, quantum sensing and metrology, as well as quantum computing-related innovations.[24]
- **IIT Bombay** has the Centre of Excellence in Quantum Information Computing Science & Technology (QuICST) for R&D in quantum simulation, computing, sensing and metrology, amongst others.[25]
- The **Indian Institute of Science, Education and Research (IISER)** Pune hosts the I-HUB Quantum Technology Foundation, which aims to harness quantum phenomena for developing advanced computing systems, as well as for more immediate applications in

---

[19] *MEITY Quantum Computing Applications Lab* (Web Page) <https://quantumcomputing.negd.in/>.
[20] Press Information Bureau, 'Secretary Telecom Shri K. Rajaraman visits C-DOT; Inaugurates futuristic Quantum Communication Lab', (News, 10 October 2021) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1762590>.
[21] *Quantum Measurement and Control* (Web Page) <https://www.tifr.res.in/~quantro/>.
[22] *Raman Research Institute* (Web Page) <https://wwws.rri.res.in/quic/>.
[23] Bengaluru Bureau, 'Samsung, IISc sign MoU to set up quantum technology lab', (News, 19 October 2023) <https://www.thehindubusinessline.com/companies/samsung-iisc-sign-mou-to-set-up-quantum-technology-lab/article67438414.ece>.
[24] *Center for Quantum Information, Communication and Computing* (Web Page) <https://quantum.iitm.ac.in/>.
[25] *Centre of Excellence in Quantum Information Computing Science & Technology* (Web Page) <https://www.quicst.org/>.

precision sensors, navigation devices for global positioning systems, geological mapping, atomic clocks, encrypted communication, and novel materials.[26]

- **Harish-Chandra Research Institute (HRI)** is an autonomous institute funded by DAE and conducts research on quantum communication, quantum cryptography, realizable quantum computing devices, especially ultra-cold gases and quantum optical systems, and foundations of quantum mechanics.[27]
- **IISc** Bangalore has a Centre for Excellence in Quantum Technology. This centre aims to deliver quantum enhanced technologies. Its experimental program will focus on superconducting qubit devices, single photon sources and detectors for quantum communications, integrated photonic quantum networks, and quantum sensors.[28]
- The **Indian Army**, with support from the National Security Council Secretariat (NSCS) established the Quantum Lab at Military College of Telecommunication Engineering, Mhow (Madhya Pradesh) in 2021.[29]
- In 2021 **Quantum Computer Simulator Toolkit (QSim)** was launched, to enable researchers and students to carryout research in quantum computing in a cost-effective manner. QSim is an outcome of the project 'Design and Development of Quantum Computer Toolkit (Simulator, Workbench) and Capacity Building', which is being executed collaboratively by IISc Bangalore, IIT Roorkee and C-DAC with the support of MEITY.[30]
- In August 2023, the Uttar Pradesh (UP) state government signed an MoU with Innogress, a project promoter, for the Indraprastha Quantum Data Center (IQDC). The data centre is planned to have a million-qubit-powered quantum computer.[31]

1.4 Private Sector

- The Centre for Quantum Engineering, Research and Education (CQuERE) at **The Chatterjee Group Centre for Research and Education in Science & Technology (TCG CREST)** is dedicated to carry out research in quantum computation and information, and train researchers and academia in India and internationally.[32]
- **Infosys** Quantum Living Labs leverages quantum technology for its business consulting services.[33]
- **QNu Labs** is a cybersecurity company credited to be the first firm in India to successfully develop commercial cybersecurity products using quantum physics. Its subsidiary, QNu Labs Inc, was set up in Massachusetts, US in 2019.[34]

---

[26] *I-HUB Quantum Technology Foundation* (Web Page) <https://www.quantech.org.in/>.
[27] *Harish-Chandra Research Institute* (Web Page) <https://www.hri.res.in/>.
[28] *Centre for Excellence in Quantum Technology* (Web Page) <https://ceqt.iisc.ac.in/>.
[29] Press Information Bureau, 'Indian Army Establishes Quantum Laboratory at Mhow (MP)', (News, 29 December 2021) <https://pib.gov.in/PressReleasePage.aspx?PRID=1786012>.
[30] Press Information Bureau, 'QSim – Quantum Computer Simulator Toolkit launched today', (News, 27 August 2021) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1749667>.
[31] Georgia Butler, 'India to get "million qubit" quantum computing-focused data center', *HPC & Quantum* (News, 14 August 2023) <https://www.datacenterdynamics.com/en/news/india-to-get-million-qubit-quantum-computing-focused-data-center/#:~:text=Greater%20Noida%20in%20India%20is,Quantum%20Data%20Center%20(IQDC)>.
[32] *Centre for Quantum Engineering, Research and Education* (Web Page) <https://www.tcgcrest.org/institutes/cquere/>.
[33] *Infosys Quantum Living Labs* (Web Page) <https://www.infosys.com/services/incubating-emerging-technologies/insights/quantum-living-labs.html>.
[34] *QNu Labs* (Web Page) <https://www.qnulabs.com/>.

- **BosonQ Psi** is a software venture that leverages the power of Quantum computing to perform simulations. It is the first start-up in India to join the IBM Quantum Network.[35]
- Qkrishi works to reshape the finance industry and redefine business models through the power of quantum computing. It has signed an MoU with IIT Kottayam to conduct research in quantum finance. It has also partnered with the SRM Institute of Science and Technology (SRMIST) to set up the SRMIST Qkrishi Centre of Excellence in Quantum Information and Computing (SQ-QuIC).[36]
- Mphasis provides quantum solutions and has a patent pending, EON (Energy Optimized Network), a classical-quantum hybrid network consisting of energy optimization, quantum circuit and deep neural network layers.[37]
- QuLabs,[38] Qpiai,[39] and QRDLab[40] are also at the forefront of India's quantum technology-related research and business solutions.

India has also entered several **international collaborations** for mutually beneficial development of quantum technology. These are detailed in Q14.

Although what India has done does not extend to law or regulation, the above steps could influence the formulation of future regulations.

It should be noted that a defined roadmap for the NQM is yet to be released by the government. In October 2023 the Principal Scientific Advisor (PSA) to the Centre, Ajay Sood stated that DST will put 'an appropriate structure for it [NQM] in place'.[41]

2. How is India approaching quantum technology in strategy and policy?

- India's approach is heavily focused on research and development, as seen in Q1.
- The NQM also promotes industry growth within the country, such as incubating start-ups, training programmes for new talent in the quantum workforce and growth of this workforce.[42]
- While India aims to become one of the leading nations in quantum technology, it acknowledges the necessity of working with other countries, 'the mission will generate several indigenously developed technologies but in an increasingly globalized world, a careful balance must be struck between a push for self-reliance and quick access to much needed (and easily available) global resources'.[43] Its active participation in international collaborations include dialogue about international standardisation of quantum technologies (discussed in Q9) to bilateral partnerships across R&D, academia, and trade (discussed in Q14).

---

[35] *BosonQ Psi* (Web Page) <https://www.bosonqpsi.com/>.
[36] Qkrishi (Web Page) <https://qkrishi.com/about>.
[37] *Mphasis* (Web Page) <https://www.mphasis.com/home.html>.
[38] *QuLabs* (Web Page) <https://www.qulabs.ai/about.html>.
[39] *Qpiai* (Web Page) <https://qpiai.tech/>.
[40] *QRDLab* (Web Page) <https://www.qrdlab.in/overview>.
[41] Shouvik Das, 'India's quantum mission geopolitically key, to be actualized soon', (News, 5 October 2023) <https://www.livemint.com/news/india/indias-quantum-mission-geopolitically-key-to-be-actualized-soon-11696526031816.html>.
[42] Department of Science and Technology, 'The National Quantum Mission: An unprecedented opportunity for India to leapfrog in quantum computing technologies', (Web Page) <https://dst.gov.in/national-quantum-mission-unprecedented-opportunity-india-leapfrog-quantum-computing-technologies>.
[43] Ibid.

- Quantum technology is mentioned in regulations regarding foreign trade and standardisation. Although R&D plans are in motion, the execution and regulation of it and its outcomes is not yet known.

3. What technologies are mentioned in India's quantum strategy and policy?

- The NQM is expected to have a significant impact on various sectors including communication, health, finance, energy, drug design, and space applications.[44] It has four major domains -- Quantum Computing, Quantum Communication, Quantum Sensing & Metrology, and Quantum Materials & Devices.
- It targets to develop intermediate-scale **quantum computers with 50-1000 physical qubits** within eight years, using various platforms such as **superconducting and photonic technology**. It also aims to establish **satellite-based secure quantum communications** between ground stations within India and with other countries over a range of 2,000 kilometers, as well as **inter-city quantum key distribution** over 2,000 kilometers and **multi-node Quantum network with quantum memories.**
- The mission will also focus on developing **high-sensitivity magnetometers in atomic systems and Atomic Clocks** for precision timing, communications, and navigation. Additionally, it will support the **design and synthesis of quantum materials such as superconductors, novel semiconductor structures, and topological materials** for fabrication of quantum devices. **Single photon sources/detectors and entangled photon sources** will be developed for quantum communications, sensing, and metrological applications.[45]

4. What competition/competing interests are mentioned/raised/identified in India's quantum strategy and policy?

India aims to be a leader in quantum technology, represented by such commentary:

- India's PSA has said that NQM will be 'crucial in geopolitical strategies'.[4]
- The Indian government has stated that currently India 'trails considerably behind China and the United States' but is making steady moves towards achieving quantum supremacy ('moves' as enlisted in Q1).[5]
- Referring to the initiatives listed in Q1, the government has stated that these have taken India a 'step closer towards achieving quantum readiness' and that India is 'ready to take the lead in quantum tech'.[6]
- The Additional Secretary, MEITY, Rajendra Kumar said, 'A**n early and successful foundation in quantum computing is important to achieve leadership in this emerging field.** The MEITY QCAL, established with the support of AWS, is the **first of its kind initiative in the world**, and aims to enable India's talented researchers to explore the unchartered applications of quantum computing, and pave the way for new discoveries and disruptions'.[7]
- Minister of Science & Technology, Dr Jitendra Singh recently said the NQM will make India one of the top global leaders in areas like quantum computing, quantum communication, quantum sensing, quantum materials, metrology and devices.[46]

---

[44] Matt Swayne, 'India Announces $730 Million-Plus National Quantum Mission', (News, 20 April 2023) <https://thequantuminsider.com/2023/04/20/india-announces-730-million-plus-national-quantum-mission/>.
[45] Press Information Bureau, 'Cabinet approves National Quantum Mission to scale-up scientific & industrial R&D for quantum technologies', (News, 19 April 2023) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888>.
[46] Press Information Bureau (n 3).

- A 2022 NASSCOM-Avasant report on India's quantum supremacy stated that, 'in noisy intermediate-scale quantum (NISQ) era the number of quantum bits is too small (50-100 qubits) and lack error correction to perform complex computations but large enough to demonstrate quantum advantage.'[47]

At the same time, as seen in Q14, India is actively collaborating with several countries, so it can be inferred that while India aims to be a leader in quantum technology, it seeks to do so collaboratively rather than competitively at the global stage.

While it has not been communicated how India intends to become a leader in quantum technology / achieve quantum supremacy or advantage, it may be implied that the many domestic and international initiatives for quantum R&D will pave the way for this goal.

Additionally, indirectly quantum technologies are included in India's dual-use list, and may be protected under the import-export and foreign investment policies in cases where quantum technology is used for defence goods and services. However, competing interests are not mentioned within the NQM.

5. Is there consideration of the impact of quantum computing and quantum communications?

Other than the technological and economic benefits mentioned in Q1, the impact of quantum computing and communications has not been addressed.

6. Does India's approach to quantum consider/mention quantum-safe encryption, quantum cryptography?

Yes, as mentioned in Q3 Quantum Communications is one of the four main domains under NQM, and quantum cryptography is included in this.

Further details are mentioned in Q7.

7. What does India's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?

India has developed the following in furtherance of its quantum communications:

- ISRO demonstrated free-space quantum communication over a distance of 300 metres, with the claim that, 'quantum cryptography is considered as 'future-proof', since no future advancements in the computational power can break quantum-cryptosystem.'[48]
- In February 2023, a joint team from DRDO and IIT Delhi demonstrated Quantum Key Distribution (QKD) link between the cities Prayagraj and Vindhyachal in Uttar Pradesh, across a distance of more than 100 kilometres.[49]
- In March 2023 the GOI announced that the first quantum secure communication link is active between the Department of Telecommunications (DoT) and the National

[47] NASSCOM-AVASANT, 'The quantum revolution in India: Betting big on quantum supremacy', (Report, February 2022) < https://nasscom.in/knowledge-center/publications/quantum-revolution-india-betting-big-quantum-supremacy>.
[48] Indian Space Research Organisation, 'ISRO makes breakthrough demonstration of free-space Quantum Key Distribution (QKD) over 300 m', *Media* (Web Page) <https://www.isro.gov.in/Quantum%20Key%20Distribution%20(QKD).html>.
[49] Press Information Bureau, 'DRDO and IIT Delhi scientists demonstrate Quantum Key Distribution between two cities 100 kilometres apart', (News, 23 February 2022) <https://pib.gov.in/PressReleasePage.aspx?PRID=1800648>.

Informatics Centre (NIC).[50] C-DoT has said that '**the traditional key-based cryptography has become vulnerable for attacks...to protect the channels from such attacks post-quantum cryptography is picking up**'.[51]

- CQuICC is developing quantum key delivery.
- The I-HUB Quantum Technology Foundation aims to harness encrypted communication

It is evident that cryptography is an integral part of India's NQM. The focus is on developing quantum communication systems, and apart from general discussion about the possibility of quantum computers breaking current encryption,[52] the NQM does not address the latter.

8. Does India'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?

As mentioned in the strategy and policy discussion, India has several ministerial divisions overseeing the development of quantum technology. However, it is yet to put into effect any regulatory or legal frameworks. The proposed **Digital India Act (DIA) 2023**[53] seeks to enforce 'global standard cyber laws' which will have seven objectives, one of which is to 'address emerging technologies and risks'. Further, one of the goals of the DIA is that 'the new law should evolve through rules that can be updated, and address the tenets of Digital India', and one of these tenets is 'new technologies'. It mentions 'Open Internet' as a key component, which enlists an aim to, 'Safeguard innovation to enable emerging technologies like AI/ML... **Quantum Computing**...Natural-language processing, etc.'. Currently, the proposed legislation has not provided further details on how India will approach quantum and related technologies.

It may be noted that the DIA is set to replace the Information Technology Act 2000[54] (revised in 2008 and 2011), because the latter is 'old and dated' and 'provisioned for nascent IT ecosystem in 2000 pre-Digital India in the absence of modern internet-based service such as e-Commerce, social media platforms'.[55] Thus, the new Act will address the modern-day digital technology issues.

Moreover, India is in the process of introducing new regulatory and legal frameworks across the spectrum of data and digital technology. In furtherance of the same, it recently passed the Digital Personal Data Protection (DPDP) Act 2023[56] in August, the Intermediary Rules 2022,[57] and the Consumer Protection (E-commerce) Rules 2020. It is also considering enacting several other laws, such as the Digital Competition law (speculated to follow the EU Digital Markets Act), the Non-personal Data Framework, and Online Gaming (Regulation) Bill 2022. While there is no explicit mention of quantum technology in relation to these, India's parallel development of emerging technologies and digital regulations may cause the two to intersect at some point in the future.

---

[50] Yuthika Bhargava, 'Govt launches 'quantum communication' network with a dare: Rs 10L for ethical hackers who can break encryption', *Governance* (News, 27 March 2023) <https://theprint.in/india/govt-launches-quantum-communication-network-with-a-dare-rs-10l-for-ethical-hackers-who-can-break-encryption/1476283/>.
[51] C-DoT, 'First International Quantum Communication Conclave' (Web Page) <https://cdot.in/cdotweb/web/quantumConclave23.php>.
[52] Department of Science and Technology (n 42).
[53] Ministry of Electronics and Information Technology, 'Proposed Digital India Act 2023', *Digital India Dialogues* (9 March 2023) <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf>.
[54] *Information Technology Act 2000* (India).
[55] Ministry of Electronics and Information Technology (n 53) 2.
[56] *Digital Personal Data Protection Act 2023* (India).
[57] *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* (India).

Lastly, India enforced the Anusandhan National Research Foundation Act, 2023[58] this year. The bill establishes the National Research Foundation (NRF), which will be the apex body in the country to provide strategic direction for research, innovation, and entrepreneurship in the fields of natural sciences including mathematics, engineering and technology, environmental and earth sciences, health and agriculture, and scientific and technological interfaces of humanities and social sciences. NRF will be funded by government as well as non-government resources.[59] Given its scope, it is likely that NRF will create provisions for quantum technology in the future.

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

- The Bureau of Indian Standards (BIS) is the national standards body of India, it develops standardization, marking, and quality certification of goods and services. Presently, in relation to critical technologies the BIS has published standards for 'Semiconductor and Other Electronic Components and Devices'.[60] The Electronics and IT Division Council (LITDC),[61] under BIS, is primarily responsible for developing Indian Standards in the field of Electronics and IT products, and has a technical committee for quantum computing.[62]
- The BIS has undertaken the Standards National Action Plan (SNAP) 2022-27[63], launched in January 2023, it will steer the national efforts for standards, certifications, and the specifications for future emerging technologies, amongst other sectors.[64] SNAP identifies 'Digital Engineering and other Enabling Technologies' as one of the primary drivers of future standardisation, and these enlist quantum computing as one of the emerging technologies which will be addressed.
- The International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Joint Technical Committee (JTC 1) is a consensus based, voluntary international standards group focussing on information technology (IT). India is a member of its Working Group (WG) 14, it serves as a systems integration entity to focus on JTC 1's standardization program on Quantum Computing and maintain relationships with other related ISO and IEC/TCs and other organizations. The responsibility of WG 14 is to identify gaps and opportunities and develop deliverables in the area of Quantum Computing.[65]

---

[58] *Anusandhan National Research Foundation Act 2023* (India).
[59] Press Information Bureau (n 3).
[60]Bureau of Indian Standards, 'Published Standards: (LITD)', (Web Page) <https://www.services.bis.gov.in/php/BIS_2.0/dgdashboard/published/subcommtt?depid=NjY%3D&aspect=&doe=&dt_from=&dt_to=>.
[61] Electronics and IT Division, Bureau of Indian Standards, 'Strategic Roadmap', (Web Page) <https://www.services.bis.gov.in/tmp/ELECTRONICS%20AND%20IT%20DIVISION%20COUNCIL.pdf>.
[62]Bureau of Indian Standards, 'LITD C : P5 - Quantum Computing Panel', (Web Page) <https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/dgdashboard/committee_sso/composition/604/4>.
[63] Bureau of Indian Standards, 'Standards National Action Plan (SNAP) 2022-27', 55 <https://www.bis.gov.in/wp-content/uploads/2023/05/SNPbookBilingual.pdf>.
[64] Press Information Bureau, 'India must recognize and accept the importance of quality to become a developed nation: Shri Piyush Goyal', (News, 6 January 2023) <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1889301#:~:text=Launch%20of%20Standards%20National%20Action,of%20sustainability%20and%20climate%20change>.
[65] ISO-IEC Joint Technical Committee, 'ISO/IEC JTC 1/WG 14 Quantum Information Technology', *WG 14* (Web Page, November 2022) <https://jtc1info.org/sd-2-history/jtc1-working-groups/wg-14/#:~:text=Quantum%20Information%20Technology&text=In%20June%202020%2C%20WG%2014,IEC%2FTCs%20and%20other%20organizations>.

- India is a member of the Quantum Economic Development Consortium (QED-C), which supports the formation of the proposed ISO/IEC Joint Technical Committee on Quantum Technologies (JTC-Q).[66]
- India is also a member of International Telecommunication Union (ITU). In March 2021 ITU, in collaboration with the IEC, the Institute of Electrical and Electronics Engineers (IEEE) UK and Ireland Photonics Chapter, organised a Joint Symposium on Standards for Quantum Technologies.[67] 'The discussion aims to establish panelists' opinion on the appropriate shape of 'standardization roadmap' for quantum information technologies'.

India has effectuated national standards for semiconductors, but for any other critical technology the formulation of national standards is underway. India is also actively involved in the international dialogue on standardisation of quantum computing, and is likely to incorporate those standards into its national plan, because one of the SNAP objectives is to align Indian standards with international standards.[68]

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

The government's approach has not outlined the challenges that may be faced during the development of quantum technologies. However, a 2019 draft concept note by the Technology Information, Forecasting and Assessment Council (TIFAC) discussed three national gap areas in India's quantum strategy:

- Lack of resources for higher education
- Increase university-level adoption: If India wants to build a quantum-ready workforce and compete at a global stage, it will have to develop quantum science and engineering as its own discipline at the graduate level. This will have to be coupled with new faculty and deepening engagement with industry players. This would also require an increased investment in setting up QT research centres in public-private partnerships. Also, the Government will have to play a proactive role in generating awareness about quantum science at secondary school level.
- To capitalise on quantum computing, India needs to build the required technical infrastructure[69]

11. Does India's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

India's quantum approach itself does not discuss critical technology and dual-use regulatory and legal frameworks. At the same time, it's export control regulation of dual-use goods and services, which exists separately from India's quantum strategy, does include critical technologies like quantum, cryptography, and encryption. This has been detailed in Q13.

---

[66] QED-C, 'Support for the Formation of the ISO/IEC Joint Technical Committee for Quantum Technologies (JTC-Q)', *News & Events* (Web Page, 30 August 2023) <https://quantumconsortium.org/support-for-the-formation-of-the-iso-iec-joint-technical-committee-for-quantum-technologies-jtc-q/>.
[67] ITU, 'Joint Symposium on Standards for Quantum Technologies', (Web Page) <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0323/Pages/default.aspx>.
[68] Bureau of Indian Standards (n 63) 59.
[69] Technology Information, Forecasting and Assessment Council, 'Draft Concept Note National Mission on Quantum Technology & Applications (NM-QTA)', 6-7 <https://tifac.org.in/images/nmqta/concept_note12.06.19.pdf>.

It can be observed that the country's quantum mission has not established any legal or regulatory frameworks for dual-use goods and services in the quantum sector, however, protection is extended to these indirectly via India's foreign trade regulation.

12. Are there any gaps identified in India's approach to quantum technology? Are there any barriers and challenges identified in India's approach? Are there any advantages to India's approach?

In its endeavour to power through to becoming a world leader in quantum technology, India has **prioritised its R&D initiatives and international collaborations**. This will be **advantageous** for becoming an innovation hub for quantum technologies and harnessing international relations for mutually beneficial development and use of these technologies. At the same time, **policy, regulatory and legal frameworks are lacking**, and without this support the growth and use of quantum technology can be uncertain. The **gaps identified** in India's approach are listed as under:

- The government's communication of NQM comprises of press updates including generic goals and methods to achieve those. Detailed and quantifiable information regarding the objectives and pathways to attain those is required
- The discussion for NQM did not invite inputs from experts across academia and industry. Opening the discussion can help tackle on-ground problems and advance the commercialisation of quantum technology
- As noted in Q2, Q4, and Q10, India has not yet defined the competing interests, considered the impact of quantum computing, and the challenges faced by its quantum technology sector. The NQM should outline these to facilitate a sharper vision of status quo, intended result, and a roadmap for it
- Investment, standardisation, dual-use, and import-export regulation in relation to quantum technologies is being addressed in India, however, this is via the separate bodies which oversee these frameworks, creating a piecemeal approach. A consolidated approach under the NQM, which addresses (or attempts to address) all regulatory and legal factors related to quantum technology is lacking
- Following from the previous point, unlike countries like the US and Australia, India has not established a separate governing body for its quantum mission. The NQM is being carried out by various government ministries and departments, as discussed in Q1. This scattered implementation can cause delayed processing, non-uniform guidelines, gratuitous competition amongst departments, which can be avoided if there is a single governing body for India's quantum approach

Further, the Observer Research Foundation (ORF) has put forth possible **challenges** to India's quantum mission.[70] This report was published before the NQM was announced, but the challenges are likely to remain unchanged:

- **Funding:** the budget for India's quantum strategy is not being allocated separately for the mission, but will be extracted from the annual allocation made to different central ministries and departments. For example, the DST will have to draw out funds from its annual financial statement for its experiments for the mission.[71]

[70] Prachi Mishra, Observer Research Foundation, 'India's Challenges and Opportunities in the Quantum Era', (Report, 14 April 2023) < https://www.orfonline.org/wp-content/uploads/2023/04/orf_report_quantum.pdf>.
[71] Ibid 46.

- Current **import policy** does not allow for quick and easy access to global quantum hardware and software technologies, which are needed to develop India's indigenous quantum sector.[72]
- India has **limited investment** for manufacturing quantum hardware within the country[73]
- To exert tech sovereignty, India not only has to produce hardware but also **scale quantum computing to commercial levels.** However, India's **investment and funding is not at par with countries like US and China**, the **private sector's involvement** is not as requisite as needed, and a **lack of policies** and investment that boost local manufacturing of electronic equipment has been an ongoing problem in India.[74]
- India's quantum computing needs more academics and support staff, increased industry-academia liaising, and reducing the education and skills gap.[75]
- India needs to **support innovation** by creating patent offices in universities, seamless sanctioning of labs to new scientists, open innovation platforms, and well-defined metrics to gauge progress.

Thus, as India takes strides in developing quantum technology indigenously and collaboratively, it needs to administer appropriate policies which help support and streamline the outcomes of its R&D.

13. Summarise dual-use and investment regulation for quantum technologies.

The Foreign Trade (Development & Regulation) Act, 1992[76] provides for the development and regulation of India's international trade. The Directorate General of Foreign Trade (DGFT) publishes the Foreign Trade Policy (FTP), which governs the exports and imports of goods and services.

As per India's FTP 2023, 'export of dual-use items, including software and technologies, having potential civilian / industrial applications as well as use in weapons of mass destruction is regulated. It is either prohibited or is permitted under an authorization unless specifically exempted.'[77] The dual-use items are mentioned in the SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) list, which includes software and technology. In relation to quantum and critical technologies, this list mentions:

- Cryptographic activation
- Cryptography
- Cryptanalysis (under Information Technology)
- Quantum Cryptography
- Quantum Key Distribution (QKD)
- Superconducting Quantum Interference Device (SQUID)
- Symmetric and Asymmetric Algorithms for encryption/decryption

---

[72] Mishra (n 70) 47.
[73] Ibid.
[74] Mishra (n 70) 50
[75] Mishra (n 70) 52-54
[76] *Foreign Trade (Development & Regulation) Act 1992* (India).
[77] Directorate General of Foreign Trade, 'Chapter 10: Special Chemicals, Organisms, Materials, Equipment and Technologies'. *Foreign Trade Policy 2023* <https://content.dgft.gov.in/Website/dgftprod/a2f58730-df83-49df-a437-b5f6345abb66/FTP2023_Chapter10.pdf>.

Examples include:

- 8A502: '"Information security" systems, equipment and components designed or modified to use (a)'**cryptography for data confidentiality**'…or (c) perform "**quantum cryptography**"...'
- 8E303(b): 'Other "technology" for the "development" or "production" of hetero-structure semiconductor electronic devices such as high electron mobility transistors (HEMT), hetero-bipolar transistors (HBT), **quantum well and super lattice devices**'.

The FTP 2023 also states catch-all controls for any dual use items not mentioned in the SCOMET list, which may be regulated by the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.[78] This could be applied to critical technologies which may be used for WMD in the future.

India is a signatory to the major Multilateral Export Control Regimes (MECR), namely, Missile Technology Control Regime (MTCR), Wassenaar Arrangement (WA) and Australia Group (AG), and adherent to Nuclear Supply Group (NSG). India is also a signatory to international conventions on non-proliferation, namely, Chemical Weapons Convention (CWC) and Biological and Toxic Weapons Convention (BWC). Accordingly, the SCOMET control list is aligned to the control lists of all four MECR and both conventions.

When it comes to the import policy, the government's list of 'Restricted Items for Import' could be used to deduce that certain products where quantum technology could be used are not permitted except when those have a government license, like communication jamming equipment, satellite communication equipment, marine radio communication equipment, etc. However, there is no explicit mention of quantum or critical technologies.

A look at India's position at importing quantum technology, apart from existing regulation, presents a mixed opinion. On one hand officials within MEITY have commented on the topic that, 'importing or purchasing the technology is not a sustainable solution in the long term. India needs to develop the capabilities for this technology internally...'[79]. On the other hand, the DST has stated on separate occasions that, ' We believe materials and devices-based innovation will create new businesses from manufacturing supporting equipment, which India now needs to import, to high-end specialized devices, such as semiconductor-based single photon detectors, at the bulk scale.'[80] and 'Delays in funds disbursal and other impediments like restrictions on import of critical enabling technologies must be removed to enable rapid progress and prevent wastage of time and resources.'[81] Furthermore, TCG CREST is building a quantum computer in India and has already imported a dilution refrigerator from Finland as the first building block for its hardware.[82]

Thus, it can be gathered that India's export policy of dual-use and defence goods substantially regulates quantum technology. At the same time, the import policy is lacking in

---

[78] *Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005* (India).
[79] Ojasvi Nath, 'Quantum Tech's Promising Growth Post Govt Initiative', (News, 3 June 2021) <https://www.businessworld.in/article/Quantum-Tech-s-Promising-Growth-Post-Govt-Initiative/03-06-2021-391922/>.
[80] Department of Science and Technology, 'Material Opportunities for India's Quantum Technology Mission', (Web Page) <https://dst.gov.in/material-opportunities-indias-quantum-technology-mission>.
[81] Department of Science and Technology, 'The National Quantum Mission: An unprecedented opportunity for India to leapfrog in quantum computing technologies', (Web Page) <https://dst.gov.in/national-quantum-mission-unprecedented-opportunity-india-leapfrog-quantum-computing-technologies>.
[82] Matt Swayne, 'India's The Chatterjee Group, Partners to Build Quantum Computer', *Quantum Computing Business, Research* (Web Page, 1 May 2023) <https://thequantuminsider.com/2023/05/01/indias-the-chatterjee-group-partners-to-build-quantum-computer/>.

this aspect. It also appears that while India is aiming to be an exporter of quantum software, it needs and plans to import hardware in order to develop said software.

13.1 Foreign Investment

India's Foreign Direct Investment (FDI) is overseen by the Department for Promotion of Industry and Internal Trade (DPIIT) under the Ministry of Commerce and Industry, and it is governed by the Foreign Exchange Management Act, 1999 (FEMA). The current FDI Policy has been effective since 2020 and does not include guidelines on quantum technology. It is likely that until specific regulation for FDI on critical technologies is developed, these will follow the existing rules for the Information Technology sector.

India allows 100 percent FDI in the IT sector[83], and is the country to receive the most foreign investment in data centres since 2019[84]. Foreign venture capital investors (FVCIs) are permitted to invest in many sectors, including software and information technology.[85] India also has Software Technology Parks (STPs), which are special zones for incentives for foreign investors in software export-oriented businesses. Once again, although no detailed discussion around critical technologies exists in relation to foreign investment, there has been a fleeting mention of quantum technologies in the draft Data Centre Policy 2020 by MEITY. As noted above, Indian data centres receive the world's biggest share of FDI, and MEITY refers to growing these data centres by the adoption of "emerging technologies such as quantum computing".[86]

Additionally, the FDI Policy allows foreign investment either via the automatic route (no government approval needed) or via the government approval route. Eleven sectors require government approval: Mining, Defence/cases relating to FDI in small arms, Broadcasting, Print media, Civil Aviation, Satellites, Telecom, Private Security Agencies, Trading (Single, Multi brand and Food Products), Financial services not regulated or regulated by more than one regulator/Banking Public and Private (as per FDI Policy) and Pharmaceuticals.[87] So, if the quantum technology-based foreign investment is any of these sectors, it will require a government permit, unlike the 100 percent allowance for IT sector.

Finally, it can be observed that India's policy on foreign investment does not provide well-defined guidelines for quantum technology. This is juxtaposed with the country's multiple international collaborations on quantum technology, few of which entail foreign investment in India.[88] Thus, it appears that while India's trade is prepared for foreign investment, its policies are yet to catch up with the quantum industry.

14. Has India partnered with other countries for developing quantum technology?

Yes, India has entered into several international partnerships on quantum technology. These are listed as under:

---

[83] Legal Window, 'Guidelines on FDI in Information Technology Sector in India', (Web Page, 1 March 2021) <https://www.legalwindow.in/guidelines-on-fdi-in-information-technology-sector-in-india/>.
[84] Sebastian Shehadi, 'India is top global destination for foreign investment in data centres', (News, 27 September 2023) <https://www.investmentmonitor.ai/news/india-data-centres-fdi-leading-global-germany/>.
[85] Bureau of Economic and Business Affairs (US), '2021 Investment Climate Statements: India', (Report) <https://www.state.gov/reports/2021-investment-climate-statements/india>.
[86] Ministry of Electronics & Information Technology, 'Data Centre Policy 2020', (Draft) 1.3 <https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf>.
[87] Foreign Investment Facilitation Portal, 'Present FIFP', (Web Page) <https://fifp.gov.in/AboutUs.aspx>.
[88] US Department of Defense, 'Joint Statement on the Fifth Annual India-U.S. 2+2 Ministerial Dialogue', *Release* (Press Release, 10 November 2023) < https://www.defense.gov/News/Releases/Release/Article/3586228/joint-statement-on-the-fifth-annual-india-us-22-ministerial-dialogue/#:~:text=The%20Ministers%20welcomed%20the%20rapid,in%20New%20Delhi%20in%20early>.

14.1 India-US collaboration

1) **Initiative on Critical and Emerging Technology (iCET):** Both countries signed the iCET in January 2023, a bilateral initiative which harbours cooperation between their governments, industry, and academia. The initiative spans across sectors like defence, space, telecommunications; and in relation to quantum technology, it entails the following:

- establishing a joint Indo-US Quantum Coordination Mechanism to facilitate research and industry collaboration
- signing a new Implementation Arrangement for a Research Agency Partnership, to expand international collaboration in a range of areas including quantum technologies
- the U.S. Department of Defense (DoD) and the Indian Ministry of Defense (MoD) launched the India-U.S. Defense Acceleration Ecosystem (INDUS-X) to expand the strategic technology partnership and defence industrial cooperation

2) IIT Bombay has joined the **Chicago Quantum Exchange** as an international partner.

3) India and the US have signed an **MoU** between Indian universities, represented by the IIT Council, and the Association of American Universities (AAU) to establish the **India-US Global Challenges Institute**, with a combined initial commitment of at least USD 10 million. The Global Challenges Institute will advance new frontiers in science and technology, spanning collaboration in semiconductor technology and manufacturing and quantum science, amongst other industries.

4) They have a **growing number of multi-institutional collaborative education partnerships**, such as those between New York University-Tandon and IIT Kanpur Advanced Research Center, and the Joint Research Centres of the State University of New York at Buffalo and IIT Delhi, Kanpur, Jodhpur, and BHU, **in the areas of critical and emerging technologies.**

5) Both countries have signed an **MoU on Semiconductor Supply Chain and Innovation Partnership**. The **combined investment is valued at USD 2.75 billion**, with Micron Technology Inc., to invest up to USD 825 million to build a new semiconductor assembly and test facility in India and Applied Materials Inc., to invest USD 400 million to establish a collaborative engineering centre in India.

6) They have launched a **USD 2 million grant** program under the **U.S.-India Science and Technology Endowment fund** for the joint development and commercialization of AI and quantum technologies, and encouraged public-private collaborations to develop high performance computing (HPC) facilities in India.

7) The **US-based IBM has signed an MoU with three MEITY entities** for advancing India's comprehensive strategy for AI, strengthen efforts to be self-reliant in semiconductors and advance its National Quantum Mission. These MoUs have been signed between IBM and MEITY's INDIAai, India Semiconductor Mission (ISM) and C-DAC.[89]

[89] Nidhi Singal, 'IBM, MeitY sign MoUs to advance innovation in AI, semiconductor and quantum innovation in India', (News, 18 October 2023) <https://www.businesstoday.in/latest/in-focus/story/ibm-meity-sign-mous-to-advance-innovation-in-ai-semiconductor-and-quantum-innovation-in-india-402508-2023-10-18>.

8) India's Tata Consulting Services (TCS) has as launched the TCS Quantum Computing Lab on US-based AWS to help enterprises explore, develop, and test business solutions and accelerate the adoption of quantum computing.[90]

14.2 India's partnerships with other countries

1. India is already engaged with **Entanglement Exchange** and the **US QED-C** enabling multi-nation exchanges on quantum computing.
2. **EU-India Trade and Technology Council:** Launched in February 2023, the TTC seeks to increase EU-India bilateral trade. The European Union and India will cooperate on **quantum and High-Performance Computing research and development projects** to help address challenges such as climate change and natural disasters and improve healthcare via personalised medicine. They will also coordinate their policies with regards to the strategic **semiconductors** sector through a dedicated **MoU**.
3. **DESI initiative by Finland:** The Digitalisation, Education, Sustainability and Innovation (DESI) initiative aims to 'combine the strengths of both countries to create new business opportunities, drive innovation, and build a more sustainable future for all.' The DESI Initiative together with the Team Finland network and the Finnish business and science community, Finnish top expertise from all sectors will be gathered under one umbrella. This is **Finland's first export promotion program and seeks to be a part of India's economic growth by providing Finnish expertise on quantum technology** and other sectors. Additionally, India's **HCLTech and Business Finland** have signed a **MoU** to collaborate on quantum technology, AI, and space technology.
4. **HCL Tech has also signed an MoU with Sydney Quantum Academy** (SQA). SQA is a partnership between Macquarie University, the University of New South Wales, the University of Technology Sydney, and the University of Sydney. **SQA is supported by the New South Wales (NSW) government** with a vision to build Australia's quantum economy. Through this industry-academia partnership, **HCL Technologies and SQA aim to bring together their capabilities to create education and development opportunities for students** within the realm of quantum technology. Other opportunities, which will be explored as part of the MoU, will **connect HCL's diverse and large client base with the growing Sydney quantum community**.[91]
5. India's Tech Mahindra has signed a partnership deal with **Spain's** Multiverse Computing to bring quantum software to its enterprise clients.
6. **India's TCG CREST** has built major partnerships with the University of Tokyo and Keio University in **Japan**, the University of Wisconsin **(US)**, **Singapore's** Centre for Quantum Technologies (CQT), and **Spanish** start-up Qilimanjaro for quantum computing.
7. **India Japan Science and Technology Cooperation** is a part of India's NQM to promote bilateral scientific collaboration between Indian and Japanese scientists. Additionally, in July 2023 India and Japan agreed to **collaborate on semiconductors** to create a more resilient supply chain for this critical technology. The partnership will focus on five areas: 'semiconductor design, manufacturing, equipment research, establishing resilience in the

---

[90] Tata Consultancy Services, 'TCS Joins Hands with AWS to Help Enterprises Harness the Power of Quantum Computing', (Web Pag, 28 November 2022) <https://www.tcs.com/who-we-are/newsroom/press-release/tcs-joins-hands-with-aws-help-enterprises-harness-power-quantum-computing>.

[91] HCLTech,' HCL Technologies and Sydney Quantum Academy to collaborate on quantum technology ecosystem development', (News, 29 July 2022) <https://www.hcltech.com/newsfeed/news/hcl-technologies-and-sydney-quantum-academy-collaborate-quantum-technology-ecosystem>.

semiconductor supply chain, and talent development', paving the way for government-to-government and industry-to-industry collaborations.[92]

8. The **Australia-India Cyber and Critical Technology Partnership (AICCTP)** to invest in cyber and critical tech collaborations and initiatives aims to support an open, free, rules-based Indo-Pacific region.[93]
9. India is also a member of the **Quad Critical and Emerging Technology Working Group,** a partnership between Australia, US, Japan, and India. Quad partners are working actively together to meet challenges faced by the Indo-Pacific, including in the area of critical and emerging technology.[94]

The latest meeting amongst the Quad heads of state was conducted in May 2023 in Hiroshima, Japan. The Quad has six working groups, one of those is the Critical and Emerging Technology (CET). The CET WG promotes global technology markets and standards based on openness, diversity, trust and resilience. The CET WG cooperates on technical standards; 5G; horizon scanning; and technology supply chains. Quad Leaders have agreed to work together on artificial intelligence; semi-conductor supply chains; and monitoring trends in critical and emerging technologies, including advanced biotechnologies, and Open Radio Access Networks (Open RAN).

The Quad has published a joint statement of **Principles on CET Standards**, broadly these are to 'support industry led, consensus-based multi-stakeholder approaches', 'support technology standards that promote interoperability, competition, inclusiveness and innovation', and 'foster technology standards that support safety, security and resilience'.[95]

The May 2023 meeting published the following updates for the Quad CET division:

- The Quad will develop Open RAN in Palau.
- The Quad welcomed a new report outlining cybersecurity considerations associated with using Open RAN as an approach to developing network architecture.
- Advancing Innovation to Empower Nextgen Agriculture (AI-ENGAGE) is a research collaboration that will leverage joint funding, expertise, infrastructure and other resources to deliver scientific advances to increase crop yield and resilience.
- Quad Technology Business and Investment Forum was launched in December 2022, which laid the foundation for enhanced private-public collaboration across the four governments, industry, investors, academia, and civil society on CET.

---

[92] Harsh V Pant and Pratanshree Basu, 'A 'fab' way to conduct India-Japan tech diplomacy', (News, 19 August 2023) <https://www.thehindu.com/opinion/op-ed/a-fab-way-to-conduct-india-japan-tech-diplomacy/article67210701.ece>.
[93] Assistant Minister for Foreign Affairs (Australia), 'Australia-India Cyber and Critical Technology Partnership grants: Round 3', (Media Release, 31 August 2023) <https://ministers.dfat.gov.au/minister/tim-watts/media-release/australia-india-cyber-and-critical-technology-partnership-grants-round-3>.
[94] Department of Prime Minister and Cabinet (Australia), 'Quad Working Groups', (Web Page) <https://www.pmc.gov.au/quad-2023/quad-working-groups>.
[95] Department of Prime Minister and Cabinet (Australia), 'Quad Principles on Critical and Emerging Technology Standards', (Web Page) < https://www.pmc.gov.au/resources/quad-principles-critical-and-emerging-technology-standards#:~:text=They%20should%20promote%20interoperability%2C%20innovation,free%20and%20fair%20market%20competition>.

10. **Mphasis** has formed a strategic partnership with the University of Calgary and the Government of Alberta to announce the establishment of Quantum City – **Canada**.[96]

[96] Mphasis, 'Celebrating one year of Mphasis' inspiring journey in Calgary, Alberta', (Press Release, 7 September 2023) <https://www.mphasis.com/content/dam/mphasis-com/global/en/news/press_releases/celebrating-one-year-of-mphasis-inspiring-leadership-journey-in-calgary-alberta.pdf>.

15. India Quantum Acronyms

S.no.	Acronym	Body	Description
1.	MEITY	Ministry of Electronics and Information Technology	The Ministry of Electronics and Information Technology oversees policy matters relating to information technology, electronics, and internet
2.	MoS&T	Ministry of Science and Technology	The Ministry of Science and Technology promotes the excellence and reach of India's science and technology so that it can solve global problems with local relevance.
3.	DST	Department of Science and Technology	DST formulates policies relating to S&T, handles matters relating to the Scientific Advisory Committee of the Cabinet (SACC) and promotes new areas of S&T with special emphasis on emerging areas through R&D in its research institutions or laboratories.
4.	C-DAC	Centre for Development of Advanced Computing	The Centre for Development of Advanced Computing is under MEITY and carries out R&D in IT, Electronics and associated areas.
5.	C-DOT	Centre for Development of Telematics	The Centre for Development of Telematics is under MoS&T. It is an autonomous telecom R&D centre and has capabilities to undertake large scale state-of-the-art telecom technologies development programs.
6.	MEA	Ministry of External Affairs	The Ministry of External Affairs is responsible for India's international relations. Territorial divisions deal with bilateral political and economic work while functional divisions look after policy planning, multilateral organizations, regional groupings, legal matters, disarmament, protocol, consular, Indian Diaspora, press and publicity, administration and other aspects.
7.	NEST	New, Emerging and Strategic Technologies	The New, Emerging and Strategic Technologies is a nodal point to evolve and coordinate India's position on global governance norms, standards, architecture, and rules that are expected to come up for emerging technologies in a multilateral context, including at the

			UN and other mechanisms of regional cooperation.
8.	PM-STIAC	Prime Minister's Science, Technology and Innovation Advisory Council	It is an overarching council that facilitates the Principal Scientific Advisor's Office to assess the status in specific science and technology domains, comprehend challenges, formulate interventions, develop a futuristic roadmap and advise the Prime Minister accordingly.
9.	DoS	Department of Space	The Department of Space has the primary objective of promoting development and application of Space Science and Technology to assist in all-round development of the nation.
10.	ISRO	Indian Space Research Organisation	The Indian Space Research Organisation is the space agency of India. The organisation is involved in science, engineering and technology to harvest the benefits of outer space for India and the mankind. ISRO is a major constituent of the DOS
11.	DAE	Department of Atomic Energy	DAE is responsible for the entire spectrum of activities related to nuclear science and technology encompassing power generation, research, development, safety, security, safeguards, environmental protection, international collaborations and societal applications.
12.	DRDO	Defence Research and Development Organisation	DRDO is the R&D wing of Ministry of Defence, Govt of India, with a vision to empower India with cutting-edge defence technologies and a mission to achieve self-reliance in critical defence technologies and systems.
13.	NQM	National Quantum Mission	NQM is India's plan for scaling up scientific and industrial R&D and creating thriving ecosystem for quantum technology. It aims to accelerate quantum technology led economic growth and make India one of the leading nations in the development of quantum technologies.

14.	IIT	Indian Institute of Technology	The Indian Institute of Technology are central government funded technical institutes located across India.
15.	TIFR	Tata Institute of Fundamental Research	TIFR is a National Centre of the Government of India, under the umbrella of the DAE, as well as a deemed University awarding degrees for master's and doctoral programs. It conducts basic research in physics, chemistry, biology, mathematics, computer science and science education.
16.	Quantum EE	Quantum Entanglement Exchange	Quantum Entanglement Exchange program aims to facilitate the exchange of students, researchers, and professionals in the field of quantum technologies.
17.	QCAL	Quantum Computing Applications Lab	MEITY has collaborated with Amazon Web Services (AWS) to establish the QCAL. This lab will assist the scientific, academic, and developer communities in their R&D on quantum technologies.
18.	QuMaC	The Quantum Measurement and Control Laboratory	A quantum lab at TIFR which primarily investigates quantum phenomena in superconducting circuits,18 and has already made a 5-qubit quantum computer.
19.	QuIC	Quantum Information and Computing	A lab at the RRI, it is one of the first labs in India to manufacture and establish the usage of heralded and entangled photon sources towards various applications in quantum technologies. The lab has also collaborated with ISRO.
20.	RRI	Raman Research Institute	RRI is an autonomous research institute engaged in research in basic sciences.
21.	IISc	Indian Institute of Science	IISc is a research university for higher education in science, engineering, design, and management.

22.	CQuICC	Center for Quantum Information, Communication and Computing	Set up by IIT Madras, it has an objective of developing secure quantum communications, including quantum key delivery, quantum random number generation, quantum sensing and metrology, as well as quantum computing-related innovations.
23.	QuICST	Centre of Excellence in Quantum Information Computing Science & Technology	Set up by IIT Bombay for R&D in quantum simulation, computing, sensing and metrology, amongst others.
24.	IISER	Indian Institute of Science, Education and Research	Indian Institute of Science, Education and Research are centrally funded higher education institutes across India.
25.	HRI	Harish-Chandra Research Institute	It is an autonomous institute funded by DAE and conducts research on quantum communication, quantum cryptography, realisable quantum computing devices, especially ultra-cold gases and quantum optical systems, and foundations of quantum mechanics.
26.	NSCS	National Security Council Secretariat	The National Security Council Secretariat is a division under the MEA.
27.	CQuERE	Centre for Quantum Engineering, Research and Education	Established by TCG CREST, it carries out research in quantum computation and information, and train researchers and academia in India and internationally
28.	TCG CREST	The Chatterjee Group Centre for Research and Education in Science & Technology	TCG CREST is a private research institute.
29.	SQ-QuIC	SRMIST Qkrishi Centre of Excellence in Quantum Information and Computing	A quantum development centre set up by SRMIST and Qkrishi, a fintech company using quantum computing for the finance sector

30.	SRMIST	SRM Institute of Science and Technology	A premier institute for science and technology higher education
31.	EON	Energy Optimized Network	A patent filed by the quantum start-up Mphasis
32.	DoT	Department of Telecommunications	DoT oversees developmental policies for telecommunication services
33.	NIC	National Informatics Centre	NIC is under MEITY and has the objective to provide technology-driven solutions to Central and State Governments
34.	DIA 2023	Digital India Act, 2023	A proposed Act that seeks to enforce 'global standard cyber laws' which will have seven objectives, one of which is to 'address emerging technologies and risks'.
35.	DPDP Act 2023	Digital Personal Data Protection Act 2023	An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.
36.	NRF	National Research Foundation	The apex body in the country to provide strategic direction for research, innovation, and entrepreneurship in the fields of natural sciences including mathematics, engineering and technology, environmental and earth sciences, health and agriculture, and scientific and technological interfaces of humanities and social sciences.

37.	BIS	Bureau of Indian Standards	The national standards body of India, it develops standardization, marking, and quality certification of goods and services.
38.	SNAP	Standards National Action Plan	It will steer the national efforts for standards, certifications, and the specifications for future emerging technologies, amongst other sectors
39.	ISO	International Organization for Standardization	ISO is an independent, non-governmental international organization. It brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.
40.	IEC	International Electrotechnical Commission	IEC is a global, not-for-profit membership organization, whose work underpins quality infrastructure and international trade in electrical and electronic goods.
41.	QED-C	Quantum Economic Development Consortium	QED-C is a consortium of international stakeholders that aims to enable and grow the quantum industry. Multiple agencies and a diverse set of industry, academic, and other stakeholders are working together to identify gaps in technology, standards, and workforce and to address those gaps through collaboration.
42.	ITU	International Telecommunication Union	ITU is the United Nations specialized agency for information and communication technologies
43.	IEEE	Institute of Electrical and Electronics Engineers	IEEE is the world's largest technical professional organization dedicated to advancing technology and has highly cited publications, conferences, technology standards, and professional and educational activities.

44.	TIFAC	Technology Information, Forecasting and Assessment Council	TIFAC India guides and catalyses national initiatives in Science and Technology. It publishes technology assessments and techno-market survey reports, technology roadmaps providing in-depth coverage of technology trends, status of technology in India, gap areas and technology linked based business opportunities.
45.	QSim	Quantum Computer Simulator Toolkit	QSim was launched by the Indian government to enable researchers and students to carryout research in quantum computing in a cost-effective manner
46.	PSA	Principal Scientific Advisor	The PSA's office aims to provide pragmatic and objective advice to the Prime Minister and the cabinet in matters of Science and Technology
47.	FTP	Foreign Trade Policy	FTP is the prime policy that lays down simple and transparent procedures which are easy to comply with and administer for efficient management of foreign trade in India
48.	SCOMET	Special Chemicals, Organisms, Materials, Equipment and Technologies	India's SCOMET list details Its dual-use items which must follow strict export and import regulations.
49.	FDI	Foreign Direct Investment	FDI is a category of cross-border investment in which an investor resident in one economy establishes a lasting interest in and a significant degree of influence over an enterprise resident in another economy
50.	iCET	Initiative on Critical and Emerging Technology	A bilateral initiative between India and US, which harbours cooperation between their governments, industry, and academia. It has several undertakings for quantum technology
51.	TCS	Tata Consulting Services	An India-based consultancy with outposts across the world

52.	TTC	Trade and Technology Council	TTC facilitates bilateral trade between European Union and India. They will cooperate on quantum and High-Performance Computing research and development projects
53.	DESI	Digitalisation, Education, Sustainability and Innovation initiative	DESI initiative aims to combine the strengths of India and Finland to create new business opportunities, drive innovation, and build a more sustainable future for all.
54.	SQA	Sydney Quantum Academy	SQA is supported by the New South Wales (NSW) government with a vision to build Australia's quantum economy, and is a partnership between four NSW universities. HCL Technologies (India) and SQA aim to bring together their capabilities to create education and development opportunities for students
55.	AICCTP	Australia-India Cyber and Critical Technology Partnership	A bilateral partnership between Australia and India to invest in cyber and critical tech collaborations and initiatives aims to support an open, free, rules-based Indo-Pacific region

Appendix D – UK'S quantum policy and regulation[1]

Contents

[1] Prepared by Catherine Nguyen with contributions from Jennifer Westmorland, UNSW Allens Hub for Technology, Law and Innovation.

1. Legislation/Framework Summary

- **National Security Investment Act 2021**: Requires sensitive business acquisitions to be approved by the government before they are completed. This includes for quantum technologies.
- **Export Control Order 2008**: regulation of dual use goods – applies to some quantum technologies

Possible frameworks

- **Online Safety Act 2023**: gives the law enforcement investigatory powers over 'regulated services' e.g. internet services, social media sites etc., has the potential to impact encryption[2]
- **Investigatory Powers Act 2016**: allows UK government to compel communications providers to remove electronic protection applied to any communications or data
- **Regulation of Investigatory Powers Act 2000**: gives the UK power to authorities to compel the disclosure of encryption keys or decryption of encrypted data

2. What has the UK done to date on Quantum strategy, policy and legislation?

Strategies

- National Quantum Technologies Programme 2014 (NQTP)
- National Quantum Strategy 2023 (NQS)[3]

Notable Programs

- Innovate UK – Commercialising quantum technologies challenge[4]
  - **Budget:** Total of £174 million, supported by £390 million from industry
  - **Duration:** 2018 to 2025

Legislation

- National Security Investment Act 2021

The 2023 UK Integrated Review identified quantum technologies as one of five priority areas of focus for UK Science and Technology.

3. How is the UK approaching quantum technology in strategy and policy?

The UK seem to be approaching their QT strategy in a collaborative fashion with plans for industry, researchers, and academia. They had released one of the earliest quantum policies in the world, the National Quantum Technologies Programme (NQTP) in 2014. The NQTP is a ten-year program that is approaching its end and it's really interesting to see what the UK were able to achieve with 10 years of a quantum strategy.

---

[2] Stewart Room, 'Will U.K. Online Safety Bill Break Encryption For Mass Surveillance?', *Forbes* (21 September 2023) <https://www.forbes.com/sites/stewartroom/2023/09/21/will-uk-online-safety-bill-break-encryption-for-mass-surveillance/>.

[3] Department for Science, Innovation and Technology, *National Quantum Strategy* (Mar 2023) https://www.gov.uk/government/publications/national-quantum-strategy#:~:text=A%2010%2Dyear%20vision%20and,the%20UK's%20prosperity%20and%20security ('NQS').

[4] UK Research and Innovation (UKRI), *'Commercialising quantum technologies challenge'* https://www.ukri.org/what-we-do/our-main-funds-and-areas-of-support/browse-our-areas-of-investment-and-support/commercialising-quantum-technologies-challenge/#:~:text=The%20challenge%20provides%20funding%20for,%2C%20telecommunications%2C%20cyber security%20and%20defence.

National Quantum Technologies Programme 2014

- A ten-year program (2014-2024) representing £1bn of public and private investment to accelerate quantum technologies into the marketplace.
- Delivered in two 5-year phases.
- Phase 1 Achievements: brought 4 products to market:
- Programme is currently in Phase 2

As the NQTP is wrapping up, the UK released another quantum strategy, the NQS, that will take the UK to 2033.

National Quantum Strategy 2023

- Further 10-year programme building off the NQTP
- Investment of £2.5B in government funding, aims to generate additional £1B in private funding.
- Vision: UK to be a leading quantum-enabled economy by 2033

The UK's strategy leans heavily on funding education and research. They are also actively courting private investment by 'leading by example through government signalling and procurement'. The UK's Ministry of Defence was a key stakeholder in the NQTP, they have identified quantum applications for defence.

4. Does the UK have quantum specific legislation? If so, what does it cover? What does it do?

The UK *does not* have quantum specific legislation. However, they have quantum related legislation. The following Acts refer to quantum technology:

- National Security Investment Act 2021: Requires sensitive business acquisitions to be approved by the government before they are completed. This includes for quantum technologies.
- Export Control Order 2008: regulation of dual use goods – applies to some quantum technologies

5. What technologies are mentioned in the UK's quantum strategy and policy?

The UK's quantum strategy mentions five technologies, they are quantum computing, quantum communications, quantum sensing, quantum imaging, and quantum timing.[5] The UK seem to have a more granular definition of their quantum technologies than the US and Australia. The US and Australia usually define three types (computing, sensing, communications); they would class the UK's two extra classifications under the umbrella of quantum sensing.

The UK strategy often mentioned "Position Navigation & Timing" technology alongside in its quantum discussion, this is likely why they specifically define quantum imaging and timing.

"For quantum sensing, timing and imaging, our ambition is to develop the technology so that the UK is in a strong position to play an important role globally in the next generation of sensors and position, navigation and timing (PNT) capabilities, working with international partners."[6]

[5] NQS (n 3) 13.
[6] UKRI (n 4).

6. **What competition/competing interests are mentioned/raised/identified in the UK's quantum strategy and policy?**

- Competition from other sectors for packaging and fabrication capabilities for the commercialisation of QT.
- Competition for quantum enabled workforce.
- Innovation vs security and ethical use policy
- Goal 4: "Create a national and international regulatory framework that supports innovation and the ethical use of quantum technologies and protects UK capabilities and national security."[7]

7. **Is there consideration of the impact of quantum computing and quantum communications?**

Impact mainly discussed terms of economic gain from commercialisation of QT.

8. **Does the UK's approach to quantum consider/mention quantum-safe encryption, quantum cryptography?**

Yes, the UK's strategy briefly mentions quantum safe encryption. The National Cyber Security Centre has published a guidance on the transition to quantum-safe cryptography. (see Q9)

"Quantum technologies also pose potential national security challenges, not least the expectation that quantum computers will be capable of undermining the cryptography used to secure internet data."[8]

9. **What does the UK's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?**

Yes, the UK states that quantum has the potential to break current encryption in the future.

"One of the most well documented is the risk quantum computing will pose to national cyber security in the future by threatening the security of much of the existing public-key cryptography, upon which the information sharing and trust mechanisms of most modern systems depend."[9]

The NCSC has identified that the key threat is that encrypted data could be collected *now*, stored, and then decrypted in the future once a CRQC has been developed. They state that quantum computers that exist today are not a threat to public key cryptography.

Quantum Key Distribution (QKD) is one method for mitigating the quantum threat however, the NCSC does not endorse QKD for any government or military applications due to its specialist hardware requirements. Rather, they believe that Quantum Safe Cryptography (QSC) will provide the most effective mitigation. QSC will algorithm, a standard for which have not been finalised. The NCSC's advice is that users should "follow normal cyber security best practice and wait for the development of standards-compliant QSC products." (Preparing for Quantum-Safe Cryptography, NSCS). Early adoption of non-standardised QSC is not recommended.

This indicates that UK's current encryption practices and processes are inadequate to deal with CRQCs. However, they do not seem to have a concrete plan for transition to new standards, this likely has to do with the fact that they are most likely to adopt non-national standards from bodies such as NIST (US) and the European Telecommunications Standards

[7] NQS (n 3) 47.
[8] NQS (n 3) 15.
[9] NQS (n 3) 50.

Institute and only have estimates of when their standards will be published. Shortcomings discussed in Q14.

Note: as at Nov 2023, NIST has only published a *draft* of their quantum resistant algorithms.

10. Does the UK'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?

The UK's strategy explicitly mentions the following key regulatory frameworks:

- Trusted Research Guidance for Academia: Advice produced in consultation with research and university community, particularly relevant to research in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas.
- If any research is derived from the US, it could be subject to US export control laws i.e. Export Administration Regulations
- Secure Innovation: NPSA company guidance for security in innovation areas. Secure innovation principles: know the threats, secure your environment, secure your products, secure your partnerships, secure your growth.
- Academic Technology Approval Scheme:
- National Security and Investment Act: Requires sensitive business acquisitions to be approved by the government before they are completed. This includes for quantum technologies.
- Export Controls: see Q13

The regulations mentioned in the UK strategy deal with either tech development processes e.g. research integrity, OR export. There is no mention of frameworks for the application of quantum technologies.

The following acts could have relevance to quantum:

- Regulation of Investigatory Powers Act 2000: gives the UK power to authorities to compel the disclosure of encryption keys or decryption of encrypted data
- Online Safety Act 2023: gives the law enforcement investigatory powers over 'regulated services' e.g. internet services, social media sites etc., has the potential to impact encryption[10]
- Investigatory Powers Act 2016: allows UK government to compel communications providers to remove electronic protection applied to any communications or data

See Q13 for dual use frameworks.

In February 2024, the Regulatory Horizons Council published an independent report to the UK Government titled "Regulating Quantum Technology Applications".[1] The recommendations in this report are aligned with the strategic objectives set out in the UK's National Quantum Strategy, The report makes 14 recommendations categorised into three broad themes:

[1] https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf

[10] Room (n 2).

1. Regulatory frameworks and governance

To develop a regulatory framework that is adaptable and proportionate to quantum innovation.
To establish a Quantum Regulatory Forum
To implement foresight methods for regulatory requirements
To implement awareness training

2. Standards and international collaboration

To enhance the UK Quantum Standards Pilot Network
To advocate for the UK's strategic involvement in international regulatory forums
To develop interoperability standards in quantum communications
To address security concerns related to quantum communication
To advocate a balanced approach based on standards and responsible innovation

3. Innovation funding and market development.

To establish testbeds and sandboxes with regulatory components
To leverage procurement strategies to create markets for quantum technologies
To tailor the translational funding environment to support quantum innovation
To stress the importance of regulatory policies and funding for mature quantum applications
To ensure compliance with legal frameworks such as the Online Safety Act

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

- The UK has established the Quantum Standards Network Pilot[11]
    - They will encourage direct involvement in standards development; comment on proposals and draft standards, discuss UK standards policy and strategy.
    - Will develop roadmaps for standards requirements for QT
    - Enable UK to coordinate strategic priorities and drive engagement with international standards systems.

Note: does not seem that the Quantum Standards Network Pilot will be developing their own standards for the UK

The NCSC has mentioned waiting on NIST (US) and the European Telecommunications Standards Institute post quantum standards.

- UK is engaging in conversations on technical standards with organisations such as the Institute of Electrical and Electronics Engineers Standards Association, International Organization for Standardization and International Electrotechnical Commission.[12]

12. Does the UK's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected?

The UK strategy has identified the following challenges:

[11] NPL (National Physical Laboratory), 'Quantum standards network pilot' https://www.npl.co.uk/quantum-programme/standards/network-pilot accessed 24 April 2024.
[12] NQS (n 3) 30.

- QT is an emerging technology and there is uncertainty around how it can best brought to market.
- Commercialising QT will require sustained investment (commercialisation valley of death).
- Quantum sector must compete with more established sectors to access packaging and fabrication capabilities.
- Despite investment, the demand for quantum skills is greater than supply. Global competition for skills is increasing. Salaries for top quantum professionals are more than double the UK average in the US.
- Growing international competition, the US, China, and EU are all ramping up funding for quantum.
- Potential risks for technology transfer and trade restrictions as quantum corporations establish HQs overseas.

13. Does the UK's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

Neither the NQTP nor the NQS have discussed quantum technology as dual use.

Dual-use regulatory frameworks

- Export Control Order 2008: The UK's main export legislation.
    - Dual-Use List [Annex IV]: quantum cryptography is mentioned

Following the UK's departure from the EU, broader measures were introduced including activities related to restricted goods (critical-industry goods, dual-use goods, military goods, aviation and space goods, oil refining goods, quantum computing and advanced materials goods, defence and security goods, and maritime goods), and energy related goods and technology. In 2022, 14 OITALs were issued covering technical assistance for energy related goods under the Russia sanctions, none were refused and one was revoked.[13]

14. Are there any gaps identified in the UK's approach to quantum technology? Are there any barriers and challenges identified in the UK's approach? Are there any advantages to the UK's approach?

Gaps

- There is limited discussion of quantum's cryptography breaking abilities compared to the US strategy. There is limited discussion of how UK agencies will use quantum technologies. Seems to be a greater focus on education and industry.

Barriers

See Q12

Advantages

- The UK's early movement in the quantum field is likely building private industry's confidence in the field. The Innovate UK – Commercialising quantum technologies challenge was supported by £390 million from industry. The UK expected an additional £1B of industry investment over the span of the NQS.
- The UK invested in quantum hubs and now have four quantum hubs:

[13] Department for Business and Trade and Export Control Joint Unit, *UK Strategic Export Controls Annual Report 2022* (19 July 2023) https://www.gov.uk/government/publications/uk-strategic-export-controls-annual-report-2022, 24

1. Quantum Hub for sensors and metrology
2. Quantum Communications Hub
3. NQIT: Quantum hub for Networked Quantum Information Technologies
4. QuantIC: Quantum hub for quantum enhanced imaging

15. What is UK's commitment to international collaboration?

The UK has issued statements of cooperation with Australia, the US and Canada.

- Joint Statement of the United Kingdom and Australia on Cooperation in Quantum Technologies
- Joint Statement of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Quantum Information Sciences and Technologies
- Joint Statement of Canada and the United Kingdom of Great Britain and Northern Ireland on cooperation in Quantum Science and Technologies

16. What are the UK's considerations as they attempt to regulate quantum technologies?

"Quantum regulation will need to be:

- Stable, coherent and predictable
- Agile enough to move quickly with technological development • Simple to understand and inexpensive to implement • Where possible, co-designed with industry
- Focussed on innovation and industry-needs
- Champion the transparent and ethical use of quantum technologies."[14]

17. Comparison with USA

UK approach is wholistic – hubs, private companies, broader strategy, private investment, R&D outside of government agencies, started quantum transformation in 2014 (just coming to an end) 10 year strategy. What their goals were – focused on building up 4 Hubs. Launched another 10 year plan – national quantum strategy, next 10 year plan. More funding. Looking at funding education and research, private investment and government procurement. Contracting out. Defence (but not as much as US). UK defines quantum technology differently. Quantum imaging and timing in addition to communications, cryptography and computing. Navigation and timing – Position, Navigation and Timing (clustered). Leadership in PNT sector. Timing & Imaging is usually grouped with sensing (Australia and the US group it with sensing).

UK Standards – deferring to NIST and possibly EU. Post-Quantum Encryption standards. But a week ago (Nov 2023) created 'Quantum Standards Network Pilot' and that's to engage with standards bodies and other countries on quantum standards.

USA is more closed. Government focused – department of Energy and defence. Defence heavy, encryption heavy.

[14] NQS (n 3) 48.

18. UK Quantum Acronyms

Acronym	Body	Description
EPSRC	Engineering and Physical Sciences Research Council	The Engineering and Physical Sciences Research Council is a British Research Council that provides government funding for grants to undertake research and postgraduate degrees in engineering and the physical sciences, mainly to universities in the United Kingdom
NCSC	National Cyber Security Centre	The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. NCSC is part of the Government Communications Headquarters.
NPL	National Physical Laboratory	The National Physical Laboratory (NPL) is a world-leading centre of excellence that provides cutting-edge measurement science, engineering and technology to underpin prosperity and quality of life in the UK.
NPSA	National Protective Security Authority	The National Protective Security Authority, formerly the Centre for the Protection of National Infrastructure, is the national technical authority in the United Kingdom for physical and personnel protective security, maintaining expertise in counter terrorism as well as state threats.
NQCC	National Quantum Computing Centre	The NQCC is the UK's national lab for quantum computing. We work with businesses, government and the research community to deliver quantum computing capabilities for the UK.
NQTP	National Quantum Technologies Programme	The UK National Quantum Technologies Programme is a programme set up by the UK government to translate academic work on quantum mechanics, and the effects of quantum superposition and quantum entanglement into new products and services.
NSSIF	National Security Strategic Investment Fund	The UK Government’s corporate venture capital arm for dual-use advanced technologies. NSSIF invests commercially in advanced technology firms, alongside other investors, to support long-term equity investment.
QSNP	Quantum Standards Network Pilot	Network Pilot that provides a focal point for quantum standards in the UK.

QTFP	Quantum Technologies for Fundamental Physics	Quantum technologies for fundamental physics' (QTFP) is a £40 million Strategic Priorities Fund (SPF) programme part of the NQTP.
UKRI	United Kingdom Research and Investment	Launched in April 2018, UK Research and Innovation (UKRI) is a non-departmental public body sponsored by the Department for Science, Innovation and Technology (DSIT).

Appendix E USA Quantum Policy and Regulation[1]

Table of Contents

[1] Prepared by Catherine Nguyen with contributions from Jennifer Westmorland, UNSW Allens Hub for Technology, Law and Innovation.

1. Legislation Summary

The USA has passed several pieces of legislation dealing with different aspects of their quantum mission. The first piece of legislation directly related to quantum was the **National Quantum Initiative Act** (NQI Act) passed in 2018. The NQI Act was passed to enable the NIST, DOE and NSF to develop and operate programs related to QIS in the US. These programs have included the establishment of research centres, institutes, and a National Quantum Initiative Advisory Committee.

Each year since the passing of the NQI Act, the **National Defense Authorization Act** (NDA Acts FY 2019, 2020 and 2022) which specifies the annual budget for the Department of Defense (DOD), have legislated QIS related activities. Examples from the 2022 NDA Act include a grant program for QIS education in the Junior Reserve Officers' Training Corps and activities to 'accelerate the development and deployment of dual-use quantum capabilities'.

The **CHIPS and Science Act 2022** was passed to provide $280 billion in funding for semiconductor chips and makes mention of quantum networking and communications applications of chips.

The **Export Control Reform Act 2018** deals with emerging and 'foundational' dual use technologies which include quantum technologies, however, the NDA Acts will likely be more informative on dual-use quantum technologies.

The **Quantum Computing Cybersecurity Preparedness Act 2022** required federal agencies to maintain an inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers within 6 months of the Act. It then requires federal agencies to develop a plan to migrate their systems to post-quantum cryptography within 1 year of NIST issuing their post-quantum cryptography standards.

Potential legal frameworks for quantum include:

Communications Assistance for law Enforcement Act 1994 (CALEA) is a wiretapping law that enhances the ability of law enforcement agencies to conduct lawful interception of communication by requiring telecoms to modify their equipment to have targeted surveillance capabilities.

The **Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Bill** and **Lawful Access to Encrypted Data Bill** attempted to restrict E2EE and could have impacts on quantum.

2. What has the USA done to date on Quantum strategy, policy and legislation?

The USA's quantum policy started with the National Quantum Initiative Act (2018) enacted by the Trump Administration. The National Quantum Initiative is a whole-of-government approach to ensuring American leadership in QIS, their strategy is outlined in a number of strategy documents including:

- National Strategic Overview for Quantum Information Science 2018
    - first strategy document – six areas of policy: science, workforce, industry, infrastructure, economic security, and international cooperation.
- Bringing Quantum Sensors to Fruition 2022
- A Coordinated Approach to Quantum Networking 2021
- Quantum Frontiers 2020
- A Strategic Vision for America's Quantum Networks 2020
- National Security Memorandum on Quantum-Resistant Cryptography 2022
- The Role of International Talent in Quantum Information Science Report 2021
- QIST Workforce Development National Strategic Plan 2022

These published strategies have been assisted by legislation (see Q4) and presidential directives/memos to action the formation of QIS committees, roundtables, research centres and QIS programs.

3. How is the USA approaching quantum technology in strategy and policy?

The USA are focussed on being the global leaders in quantum technology. The quantum.gov website states that 'the National Quantum Initiative is a whole-of-government approach to ensuring American leadership in QIS'. (see further in Q15)

Their strategy for R&D and related activities is set out in the 'National Strategic Overview for QIS'[1]. The Strategic Overview states that the strategy focusses on: 'getting the science right', 'enhancing competitiveness', and 'enabling people'.

The USA seem to have established a top-down government approach to quantum technology. Compared to Australia, their strategy documents make little mention of specific private companies in the quantum space rather, they pinpoint plans for pre-existing federal agencies. The key piece of legislation regarding quantum serves to COORDINATE existing federal bodies NIST, NSF and DOE.

4. Does the USA have quantum specific legislation? If so, what does it cover? What does it do?

The USA has both quantum specific legislation and quantum-related legislation.

- **Quantum – specific**:

National Quantum Initiative Act (2018): established the National Quantum Initiative; accelerated quantum research and development by authorizing new activities, programs, and centers at NIST, NSF and the DOE. The Act expired in September 2023.

Post-Quantum Cybersecurity Standards Act[2]**: t**his bill was introduced in September 2023. The purpose is to amend the National Quantum Initiative Act and the Cyber Security Research and Development Act to advance the rapid deployment of post quantum cybersecurity standards across the United States economy and support United States cryptography research. The Director of NIST, in consultation with the Secretary of Homeland Security and the heads of sector risk management agencies, is to promote the voluntary adoption and deployment of post-quantum cryptography standards. These efforts will be supported by the granting of funds, dissemination of publicly available guidance and resources. Technical assistance will be provided to entities that are at high risk of quantum cryptoanalytic attacks.

Quantum Instrumentation for Science and Engineering Act[3]**:** This Bill was introduced to the House of Representatives in October 2023. The purpose is to amend the National Quantum Initiative Act in order to accelerate quantum research and development in the United States. It directs the NSF to award grants to upgrade and support research and development in quantum information science, technology, and engineering. This bill will also enable better access to resources, materials, devices and the critical services needed to enable cutting-edge research on quantum information science, as well as to train the next generation of quantum scientists and workers. It will also support the translation of research into commercial products and services.

National Quantum Initiative Reauthorisation Act[4]**;** the bill was introduced November 2023, to reauthorise the expired National Quantum Initiative Act. Requires the White House Office of Science and Technology Policy to develop a strategy for carrying out cooperative

[2] https://www.congress.gov/bill/118th-congress/house-bill/5759/history?s=1&r=18
[3] https://www.congress.gov/bill/118th-congress/house-bill/5950/text?s=1&r=34
[4] https://www.congress.gov/bill/118th-congress/house-bill/6213

quantum research efforts with allies of the United States to bolster competitiveness against China and Russia. Directs the Secretary of Energy to develop a strategy for promoting the commercialization of quantum computing. Facilitates interagency partnerships to advance quantum technology. Authorizes the DOE to support the development of resources to meet the needs of the quantum supply chain. Requires the creation of a Quantum Institute at NASA. Authorizes NIST to establish centres to advance research in quantum sensing, measurement, and engineering. Strengthens educational and workforce programs at NSF.

The Support For Quantum Supply Chains Act[5]: introduced to the House of Representatives in November 2023. This bill will amend the National Quantum Initiative Act to accelerate the development of supply chain supporting technology for quantum information science, technology, and engineering; support United States competitiveness and reduce risks in the quantum supply chain.

Expanding Capacity in Quantum Information Science, Engineering, and Technology Act, or the "Expand QISET Act"[6]: this bill was introduced in November 2023. It is designed to increase research capacity, education, infrastructure capacity and participation in quantum information science, engineering, and technology and related disciplines. It directs the National Science Foundation (NSF) to make awards and grants that support curriculum development and to fund quantum education pilot programs. The NSF is tasked with securing a talent pipeline to meet the quantum workforce needs of industry, government, and academia.

Defence Quantum Acceleration Act of 2024[7]: this bill was introduced in April 2024. The primary purpose is to direct the Secretary of Defense to accelerate the implementation of quantum information science technologies within the DoD, including the development of prototypes. This is landmark legislation in that it specifically requires quantum technology to become an integral part of USA Defence capabilities. It authorises the establishment of a multi-disciplinary QIS Centre of excellence. It also establishes a new Quantum Advisor role in the DoD, who will coordinate with the armed forces commands on the use and challenges of quantum technology within the DoD, as well as with industry, academics and allies such as AUKUS and NATO.

- **Quantum – related:**

Cyber Security Research and Development Act (2002):[8] authorizes appropriations to the National Science Foundation and to the National Institute of Standards and Technology to establish new programs, and to increase funding for computer and network security research and development, including research fellowships.

Export Control Reform Act (2018): regulates the export of emerging and 'foundational' dual use technologies which includes some QT but NDAA will be more relevant.

National Defense Authorization Act (FY 2019, 2020): authorises DOD to increase technology readiness level of QIS tech, authorisation to coordinate all QIS and technology R&D within the DOD. The FY 2024 Act requires the Pentagon to establish a pilot program on near-term quantum computing applications[9].

[5] https://www.govtrack.us/congress/bills/118/hr6207/text
[6] https://www.congress.gov/bill/118th-congress/house-bill/6384/text?s=1&r=31
[7] https://www.congress.gov/bill/118th-congress/senate-bill/4105/text
[8] https://www.congress.gov/bill/107th-congress/house-bill/3394#:~:text=Cyber%20Security%20Research%20and%20Development%20Act%20%2D%20Authorizes%20appropriations%20to%20the,programs%2C%20for%20computer%20and%20network
[9] https://www.govinfo.gov/content/pkg/CRPT-118hrpt125/pdf/CRPT-118hrpt125.pdf

CHIPS and Science Act (2022): amended NQIA to authorise R&D in quantum networking infrastructure development of standards in quantum networking and communication, integration of QIS and engineering into STEM curriculum for all.

Quantum Computing Cybersecurity Preparedness Act (2022): Requires agencies to establish an inventory of information technology that is vulnerable to decryption by quantum computers. Later requires agencies to develop a plan to adopt NIST post quantum cryptography standards.

The Department of Defense Appropriations Act 2024[10]: provides FY2024 appropriations to the Department of Defense for military activities and includes multiple budget increases for quantum technology programs.

5. What technologies are mentioned in the USA's quantum strategy and policy?

The USA generally groups the quantum technologies into the following 3 or 4 categories: quantum **sensing**, quantum **communications**, quantum **simulations**, quantum **computing**. (quantum simulation and quantum computing are sometimes combined).[2]

Quantum Sensing

- Atomic clocks
- Atom interferometers
- Optical magnetometers
- Devices utilising quantum optical effects
- Atomic electric field sensors

Quantum Communications

- Quantum networks`

Quantum Computing/Simulations

- Quantum cryptography

6. What competition/competing interests are mentioned/raised/ identified in the USA's quantum strategy and policy?

Innovation v security is the main debate in the USA's strategy and policy. The USA's goal is to lead the world in the quantum industry, and this would necessarily mean that policy should not stifle innovation and competition. China is frequently mentioned as a key competitor to USA's leadership in quantum. (see Q15 for more on international competition). However, quantum technology has been identified as dual use technology that can have military use and therefore needs to be subject to regulation. This competition of interests can be seen in the enactment of the Export Control Reform Act 2018 (see Q13).

7. Is there consideration of the impact of quantum computing and quantum communications?

The impact of quantum computing and communications is mainly discussed in relation to national security interests.

> The nation that harnesses quantum communications technology first may be able to decode — in a matter of seconds — every other nations' most sensitive encrypted national security information as well as proprietary technologies and even the personal information of individuals.[11]

[10] https://www.congress.gov/bill/118th-congress/house-bill/4365

[11] John Thune, 'U.S. must win the race against China and Europe on quantum computing', John Thune U.S. Senator for South Dakota (*Opinion Editorial*, 26 July 2018) < https://www.thune.senate.gov/public/index.cfm/op-eds?ID=B5B2BC8E-8551-4731-A52D-7B583199F782>.

8. Does the USA's approach to quantum consider/mention quantum-safe encryption, quantum cryptography?

Yes, see Q9 for further.

The Department of Homeland Security issued a policy directive in 2021 about preparing for post-quantum cryptography. It states that

> DHS has significant national security concerns across mission spaces including critical infrastructure, law enforcement, privacy, and counterintelligence that could be harmed by insufficient preparation for a transition to post-quantum cryptography.[3]

9. What does the USA's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?

The USA has made it clear that their current encryption standards are vulnerable quantum computing cryptography breaking.

> Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC (cryptographically relevant quantum computer[12]

Their strategies make it a priority to mitigate the risk by transiting to quantum resistant cryptography which will be released by NIST (see Q11).

10. Does the USA'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?

US academia has flagged the following legislation as possible regulatory frameworks for quantum:

Communications Assistance for law Enforcement Act (CALEA)

- purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance

Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Bill

- Attempted to outlaw strong encryption/E2EE
- Failed to pass in 2020, reintroduced in 2022, and for a third time in 2023.

Lawful Access to Encrypted Data Bill

- Introduced to congress but seems to have stalled ~ 2020

This bill requires certain technology companies to ensure that they can decode encrypted information on their services and products in order to provide such information to law enforcement. It also establishes requirements and procedures for assisting law enforcement agencies in accessing encrypted data.

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

From their strategy documents, the USA seems to primarily rely on national standards developed by its own standards body, the National Institute of Standards and Technology

[12] White House, 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (*Memorandum*, 4 May 2022).

(NIST). The most significant standard released by NIST thus far of three draft quantum-resistant cryptographic algorithms. The draft was publicly released in August 2023 and NIST is seeking feedback until November 2023. They are expected to release the formal standard in 2024. Additionally, some current standards applying to true random number generators (eg NIST SP 800-90B and NIST-800-22) can be used to assess quantum random number generators.[13]

The National Security Agency has released quantum algorithm requirements for national security systems in 2022.

The USA does not seem to mention the implementation of international standards such as those developed by the IEEE Standards Association.

12. Does the USA's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected?

The main challenge of quantum *cryptography* is the transition to the new algorithms, which includes:

- Replacement of algorithms requires changing or replacing cryptographic libraries, implementation validation tools, hardware changes, dependent operating system, and application code communication devices, protocols and user and administrative procedures.
- Security standards, procedures, and best practice documentation need to be changed or replaced, as do installation, configuration, and administration documentation.

The challenges of adopting and using post-quantum algorithms is explored in the NIST White Paper titled 'Getting Ready for Post-Quantum Cryptography'[14]

More generally, the US Quantum Strategy 2018 Paper identified 4 key challenges:

1. Coordinating government action with the public and private institutions
2. Requiring a broad and viable workforce to enact R&D
3. Strong interdisciplinary connections
4. Maintaining strong industrial engagement

The above challenges will need be addressed to maintain and expand American leadership in QIS technology.

13. Does the USA's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

Critical Technology (refer to Q16 for critical infrastructure)

Dual Use Regulation and Frameworks

- There is brief mention of the Export Control Reform Act 2018 deals with emerging and 'foundational' dual use technologies which include quantum technologies.

[13] Leilei Huang et al, 'Quantum Random Number Cloud Platform' (2021) 7(1) *npj Quantum Information* 1.

[14] Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms – NIST – 28 April 2021

14. Are there any gaps identified in the USA's approach to quantum technology? Are there any barriers and challenges identified in the USA's approach? Are there any advantages to the USA's approach?

The DHS Secretary stated that much of the US's critical infrastructure is in the private sector's hands and says that the DHS should work with the private sector to protect American interests. I think there may be a gap in USA's strategy in their more limited recognition of the private sector. As discussed earlier, the US strategy focusses heavily on their existing federal agencies and there is less emphasis on the private sector. There is also less discussion of commercialisation of QIS tech compared to Australia's strategy.

15. Has the USA strategy mentioned other countries?

The USA seem to be most worried about Chinese progress on quantum technologies. Security concerns are usually cited as the reason for this worry. China has stated that one of its main goals is to surpass the USA in the quantum field.
'In testimony before Congress, expert witnesses have warned that as other nations around the world rapidly advance their own quantum programs, the U.S. faces a real threat of falling behind.'[15]

16. Does the USA's strategy consider critical infrastructure and supporting technologies? eg cryogenics (for QC cooling)

The USA's strategy recognises that QIS R&D will rely on the availabilities of tools, facilities, and infrastructure and that these will be sourced from supporting industries. The strategy recommends expansion of Federal and industrial infrastructure and support activities to accelerate progress in the QIS field.

> Agencies will be encouraged to explore mechanisms to provide the QIS research community with increased access to existing and future Federal facilities, including manufacturing facilities that can be repurposed and expanded as well as systems and testbeds for post-quantum applications.[16]

[15] John Thune, 'U.S. must win the race against China and Europe on quantum computing', John Thune U.S. Senator for South Dakota (Opinion Editorial, 26 July 2018) < https://www.thune.senate.gov/public/index.cfm/op-eds?ID=B5B2BC8E-8551-4731-A52D-7B583199F782>.
[16] Subcommittee On Quantum Information Science, *National Strategic Overview For Quantum Information Science* (Report, September 2018).

17. Legislation

NQIA	National Quantum Initiative Act 2018	Authorises research activities for NIST, NSF, and DOE
NDDA	National Defense Authorization Act	Authorises DOD to increase technology readiness level of QIS tech, authorisation to coordinate all QIS and technology R&D within the DOD.
CHIPS-Plus	CHIPS (Creating Helpful Incentives to Produce Semiconductors) and Science Act 2022	Authorises $110 billion for basic and advanced technology research over 5 years (including quantum computing)

18. Coordinating Bodies

SCQIS	Subcommittee on Quantum Information Science	The National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science (SCQIS) coordinates Federal research and development (R&D) in quantum information science and related technologies under the auspices of the NSTC Committee on Science. The aim of this R&D coordination is to maintain and expand U.S. leadership in quantum information science and its applications over the next decade. The SCQIS is co-chaired by the Office of Science and Technology Policy (OSTP), the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF) and the Department of Energy (DOE).
ESIX	NSTC Subcommittee on Economic and Security Implications of Quantum Science	The National Science and Technology Council (NSTC) Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) was established to ensure that economic and security implications of QIS are understood across the agencies. The subcommittee provides a national security perspective to QIS related research. The ESIX Subcommittee coordinates with NSTC subcommittees, such as the SCQIS, to ensure that the economic and national security implications of basic research and development in QIS, along with derived technologies are fully understood. The subcommittee is co-chaired by the Office of Science and Technology Policy (OSTP), Department of Defense (DOD), Department of Energy (DOE), and the National Security Agency (NSA).
NQCO	National Quantum Coordination Office	The National Quantum Coordination Office (NQCO) is legislated by the NQI Act to carry out the daily activities needed for coordinating and supporting

		the NQI. The Coordination Office is tasked with providing technical and administrative support to the SCQIS, ESIX and the NQIAC as well as overseeing the interagency coordination of the NQI Program. The NQCO serves as the primary point of contact on Federal civilian quantum information science and technology activities and conducts public outreach, including the dissemination of findings and recommendations of the SCIQS and the Advisory Committee, as appropriate. The NQCO staff are federal employees on detail assignments from across the government.
NQIAC	National Quantum Initiative Advisory Committee	The National Quantum Initiative Advisory Committee (NQIAC) is the Federal Advisory Committee called for in the NQI Act. The NQIAC is tasked to provide an independent assessment of the NQI Program and to make recommendations for the President, Congress, and the NSTC Subcommittee on QIS to consider when reviewing and revising the NQI Program. The NQIAC consists of leaders in the field from industry, academia, and the Federal laboratories. The NQIAC was first established by Executive Order 13885 on August 30, 2019. It was subsequently enhanced by Executive Order 14073 on May 4, 2022.

19. Agencies

NIST	The National Institute of Standards and Technology	Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic prosperity. As authorized by the NQI Act, NIST is coordinating consortia focusing on quantum technologies, and maintaining fundamental QIS R&D programs. NIST has been a leader in QIS R&D for over three decades., including a seminal workshop on QIS at its Gaithersburg campus in 1994.
DOE	The Department of Energy	Ensures America's prosperity and security through several mechanisms including basic and applied scientific research, discovery and development of new technologies, and scientific innovation. The Energy Department's National Laboratories are a system of intellectual assets unique among world scientific institutions and serve as regional engines of economic growth for states and communities across the country. As authorized by the NQI Act,

		DOE is strengthening core programs and establishing new Centres focusing on QIS research.
NASA	The National Aeronautics and Space Administration	Drives advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality and stewardship of Earth. NASA's research portfolio includes some activities focusing on, and motivated by, quantum information science.
DOD	The Department of Defense	Engages in basic research, defined as the 'systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind.' DOD has supported fundamental QIS research for three decades, and continues to invest in basic QIS R&D activities via several DOD offices, agencies, and laboratories. These include: the Office of the Under Secretary of Defense for Research and Engineering (OUSDRE); the Defense Advanced Projects Agency (DARPA); the Army Research Laboratory (ARL), the Army Research Office (ARO); the Naval Research Laboratory (NRL); the Office of Naval Research (ONR), the Air Force Research Laboratory (AFRL); and the Air Force Office of Sponsored Research (AFOSR).
LPS	Laboratory for Physical Science	University, industry, and federal government scientists collaborate on research in advanced communication, sensing, and computer technologies, the LPS currently houses four main divisions related to information science and technology, including Solid-State and Quantum Physics.
IARPA	The Intelligence Advanced Projects Activity	Sponsors several applied research programs that explore quantum computing.
NSF	National Science Foundation	The National Science Foundation is an independent agency of the United States federal government that supports fundamental research and education in all the non-medical fields of science and engineering. NSF co-chairs the SCQIS.