هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Preparing for Quantum Technologies

Lessons from AI Policy Development

August 2025

Table of Contents

EXECUTIVE SUMMARY

Quantum technologies (QT) – encompassing computing, sensing, and communication – are rapidly advancing, promising transformative breakthroughs across numerous sectors but also presenting significant and complex risks. The most pressing of these is the threat posed by quantum computers to current cryptographic standards, which underpin global digital security [1]. This paper argues that valuable foresight for navigating the quantum era can be gained by examining the recent, often challenging, development of policy and regulation for Artificial Intelligence (AI). By identifying parallels and distilling lessons from the AI governance experience, this paper offers actionable recommendations for proactive regulatory preparedness for quantum technologies, particularly within the ICT and Space domains.

Quantum technologies leverage fundamental quantum principles like qubits (quantum bits), superposition (where qubits represent multiple states simultaneously), and entanglement (interconnectedness of qubits) to achieve capabilities beyond classical systems [2]. Quantum computing aims to solve problems intractable for current supercomputers [3]; quantum sensing enables ultra-precise measurements [1]; and quantum communication, notably Quantum Key Distribution (QKD), promises enhanced security [4].

The opportunities presented by QT are vast, including breakthroughs in medicine, material science, complex system modelling (e.g., climate, finance), optimisation, and fundamentally secure communication [1], [3]. However, these are counterbalanced by substantial risks. The primary concern is "Q-Day", when quantum computers can break existing encryption, necessitating a global transition to Quantum-Safe, i.e. Post-Quantum Cryptography (PQC) and QKD. The "Harvest Now, Decrypt Later" (HNDL) threat, where encrypted data is stolen today for future decryption, makes this an immediate concern [5]. Advanced quantum sensors also raise privacy and surveillance issues, while securing quantum communication networks themselves presents challenges like hardware imperfections and scalability. Other risks include potential misuse [6], economic disruption [5], and the emergence of a "quantum divide" if access is not equitable.

Proactive regulatory frameworks are imperative, even if widespread impact is years away, to manage systemic risks like the quantum-safe transition, ensure national security, foster responsible innovation, and address ethical considerations early. The journey of AI governance offers crucial parallels: both AI and QT are foundational, uncertain, rapidly evolving, dual-use technologies, subject to investment races, requiring specialized expertise, and posing ethical and global governance challenges.

Key lessons from AI policy development include the necessity of:

	**Early and broad stakeholder engagement** involving diverse voices from industry, academia, civil society, and government.
	**Balancing innovation with risk** through flexible, risk-based, and context-specific governance rather than broad prohibitions.
	**Robust international collaboration** on standards, ethical guidelines, and risk mitigation, given the global nature of these technologies.
	**Addressing the 'pacing problem,'** where technology outpaces regulation, by employing agile tools and ex-ante measures.
	**Embedding principles of transparency, accountability, and fairness** into technology development and deployment.
	**Building policymaker literacy** to ensure informed decision-making.

high priority is developing standards, particularly for PQC [4] and QKD interoperability [7]. Establishing testing and validation frameworks is essential to ensure reliability and security [8]. Promoting R&D in safety, security, and ethics [6] and building regulatory expertise and capacity [4] are crucial. Furthermore, international coordination on standards and risk mitigation is needed [1]. Specific considerations for sectors like ICT, space, finance, healthcare, and defence will also be necessary to tailor responses effectively.

By learning from AI's regulatory journey, policymakers can adopt a more proactive, agile, and potentially more effective approach to governing the diverse landscape of quantum technologies. This involves fostering responsible innovation, managing complex risks, and ensuring that the transformative potential of the quantum era is harnessed for the global good, guided by human-centric values and robust international cooperation. The task is significant, but by learning from hindsight, policymakers are better equipped to apply the foresight necessary to navigate the complexities of the quantum era effectively.

INTRODUCTION

Anticipating the Quantum Era

Quantum technologies (QT) – encompassing computing, sensing, and communication – are advancing rapidly, promising to reshape industries, tackle societal challenges, and influence national security [1]. Their potential impact is vast, prompting significant global investment, with the top five spenders committing between $2 billion and $10 billion USD each, and a race for technological leadership [1]. This confluence of rapid advancement and substantial investment signals that the «quantum era", while still nascent in many respects, requires immediate attention from policymakers.

This paper aims to equip policymakers with foresight by drawing lessons from the recent, and often complex, journey of Artificial Intelligence (AI) policy and regulation. The central argument is that AI›s experience offers a valuable, if imperfect, template for proactively preparing for the governance of QT. The fresh, and sometimes challenging, lessons from global efforts to govern AI create a unique window of opportunity for proactive policy development in the quantum domain. This proactive stance is crucial given the potentially disruptive nature of QT, allowing policymakers to anticipate rather than merely react to technological developments, a pattern often observed in the AI governance landscape.

While QT›s impact will be broad, this paper will pay particular attention to its implications for the Information and Communication Technology (ICT) sector, which forms the foundation of the digital economy [4], and the increasingly critical Space domain. Quantum advancements are poised to revolutionize communication, navigation, and observation capabilities in space [9], areas of profound strategic and economic importance.

The goal is to provide actionable recommendations for building regulatory capacity and fostering an agile, anticipatory governance framework for QT. This will enable a more effective navigation of the quantum era, ensuring that its benefits are harnessed responsibly while mitigating potential risks.

01

DEFINING QUANTUM TECHNOLOGIES

A High-Level Overview

Understanding quantum technologies requires a grasp of certain fundamental principles that differ starkly from classical physics. These principles enable a new generation of devices with capabilities far exceeding their classical counterparts.

Fundamental Quantum Principles

At the heart of quantum technologies are phenomena that occur at the atomic and subatomic levels.

- Qubits and superposition: Classical computers use bits, which can be either a 0 or a 1. Quantum technologies, however, use quantum bits, or qubits [1]. Due to a principle called superposition, a qubit can represent 0, 1, or a weighted combination of both simultaneously until it is measured [2]. This is often analogized to a dimmer light switch that can be fully on, fully off, or in any state in between, representing multiple possibilities at once, whereas a classical bit is like a simple on/off light switch [2]. This ability allows quantum computers to store and process vastly more information than classical computers using the same number of units; for example, a 4-qubit register can handle 16 different numbers simultaneously, scaling exponentially [10].

- Entanglement: Qubits can be linked together through a process called entanglement, creating a strong correlation between them such that their states are interdependent, regardless of the physical distance separating them [2]. If one measures the state of an entangled qubit, one instantly knows certain properties of the other(s). This "spooky action at a distance," as Einstein famously described it, is a critical resource for quantum computation and quantum communication protocols [2].

- Interference: Similar to how waves can reinforce or cancel each other out, quantum states can also interfere [10]. In quantum computing, algorithms are designed to harness interference to amplify the probability of obtaining the correct output while reducing the probability of incorrect outputs [2].

- Decoherence: A significant practical challenge in building quantum devices is decoherence. Qubits are extremely sensitive to their environment; interactions with external factors like vibrations or temperature changes can cause them to lose their quantum properties (superposition and entanglement) and collapse into a classical state (a definite 0 or 1) [10]. Overcoming decoherence and correcting errors are major engineering hurdles in the development of robust quantum computers [4].

- Heisenberg Uncertainty Principle: Formulated by Werner Heisenberg, this is a cornerstone of quantum mechanics. It states that there is a fundamental limit to how precisely certain pairs of physical properties, such as a particle's position and its momentum, can be known at the same time. This is not a limitation of measurement equipment but an intrinsic 'fuzziness' inherent in nature. This principle fundamentally distinguishes the quantum world from the deterministic classical world, where it is assumed all properties can be measured with perfect accuracy [11].

Classes of Quantum Technology

These fundamental principles enable distinct classes of quantum technology, each with unique applications and at varying stages of maturity.

- Quantum computing: This field aims to harness superposition, entanglement, and interference to perform calculations that are intractable for even the most powerful classical supercomputers [4]. Quantum computers are not intended to replace classical computers for all tasks but promise exponential speed-ups for specific types of complex problems, such as factoring large numbers (threatening current cryptography), simulating quantum systems (for drug and material discovery), and solving certain optimization problems [3]. Achieving "quantum advantage" - where a quantum computer solves a problem faster or more accurately than any classical computer could - is a key milestone [3]. While the technology is still considered immature and faces challenges like qubit stability, error correction and scalability, its potential is immense [1].

- Quantum sensing: This technology utilizes the high sensitivity of quantum systems to make ultra-precise measurements of physical quantities like time, gravity, magnetic fields, and temperature, often exceeding the capabilities of classical sensors [1]. Quantum sensors are already finding applications in materials science, the energy industry [1], medical diagnostics (e.g., improved MRI, brain imaging) [12], environmental monitoring, and navigation, particularly in GPS-denied environments. Some quantum sensing applications are already enhancing precision in various fields, with some devices capable of "seeing through barriers" or "around corners" [13].

- Quantum communication: This area leverages quantum phenomena to enable new forms of information transmission, with a primary focus on security. The most prominent application is Quantum Key Distribution (QKD), which uses the principles of quantum physics (like the fact that measuring a quantum state inherently disturbs it) to allow two parties to generate and share a secret cryptographic key with the assurance that any attempt to eavesdrop would be detected [4]. QKD promises theoretically unbreakable encryption, a critical capability as quantum computers threaten to break current cryptographic standards [4]. However, QKD faces challenges in terms of certification and integration into existing communication networks [4], [14].

Discussion

It is important for policymakers to recognize that these three classes of quantum technology are at different stages of development. Quantum sensors are, in some cases, already commercially available and providing benefits [15]. Quantum communication, particularly QKD, is deployable for specific use cases, though broad adoption is hampered by technical and cost hurdles [16]. Fault-tolerant, universal quantum computers, on the other hand, are likely still many years, if not decades, away from widespread practical application [17].

This differentiation is crucial: a monolithic regulatory approach for "quantum technology" will likely be ineffective. Policy interventions must be nuanced, reflecting the specific technological readiness, risk profile, and opportunity landscape of each domain. For instance, policies for QKD might focus on standardization, interoperability, and deployment incentives, while policies for quantum computing might prioritize foundational R&D, ethical guidelines for future applications, and long-term strategies for managing the cryptographic transition.

02

POTENTIAL OPPORTUNITIES AND RISKS OF QUANTUM TECHNOLOGIES

Quantum technologies present a dual-edged sword: they offer the potential for transformative advancements across numerous sectors while simultaneously introducing significant and complex risks that demand careful management. Table 1 below highlights the existing consensus on the potential opportunities that QT offers across a range of sectors and use cases.

Table 1: Potential Opportunities of Quantum Technologies

Opportunity Area	Description
Medicine	Revolutionize drug discovery and development by simulating molecular interactions, reducing time and cost for new medicines [18]. Enable personalized medicine tailored to individual genetic makeup and real-time health data [19]. Lead to higher-resolution medical imaging and more precise surgical tools [1].
Materials science	Enable design of novel materials with bespoke properties (e.g., efficient catalysts, stronger/lighter composites, new semiconductors) through quantum-level modelling and simulation [18].
Complex system modelling	Tackle modelling tasks beyond classical capabilities, including more accurate climate change projections, sophisticated financial risk modelling, and improved economic forecasting [12].
Optimisation	Provide superior solutions for complex optimisation problems in logistics and supply chain management [18], traffic flow, energy grid management (enhancing stability and efficiency) [20], and intricate space mission planning.
Sensing	Offer ultra-sensitive detection for enhanced environmental monitoring [1], efficient resource exploration, highly accurate navigation systems (especially in GPS-denied ICT/Space domains) [21], and improved security screening.
Communication	Enable fundamentally secure communication networks, primarily through Quantum Key Distribution (QKD), crucial for protecting sensitive data in ICT infrastructure and securing command/control links for space assets [1].
Advancements in AI	Quantum Machine Learning (QML) could significantly enhance AI algorithm capabilities, leading to more powerful and efficient AI systems [12].

However, as is often the case when considering emerging technologies and rapid technological advancement, some consideration has already been given to the potential risks to the widespread deployment of QT, this is highlighted in Table 2.

Table 2: Potential Risks of Quantum Technologies

Risk Area	Description
Cryptographic threat ("Q-Day")	Powerful quantum computers could break current public-key cryptography (RSA, ECC), threatening digital communications, financial transactions, and sensitive data [1]. The day a quantum computer can achieve this is often referred to as "Q-Day." This necessitates a transition to Post-Quantum Cryptography (PQC). Includes the "Harvest Now, Decrypt Later" (HNDL) scenario where encrypted data is stolen now for future decryption [4].
Security implications of advanced sensing	**Surveillance and Privacy Erosion:** Highly sensitive quantum sensors could enable mass surveillance, monitor individuals through barriers, detect biometric signatures remotely, and track movements, blurring public/private lines and impacting civil liberties [1]. Military and Espionage: Advanced sensors could provide significant military intelligence, surveillance and reconnaissance (ISR) advantages, potentially exposing covert operations, enabling new espionage forms, altering strategic balances, and escalating security dilemmas [13].
Challenges in securing quantum communication networks sensing	**Hardware Imperfections and Side-Channel Attacks:** Practical QKD implementations can be vulnerable to attacks exploiting hardware flaws or side channels (e.g., power consumption) [22]. Scalability and Integration: QKD faces distance limitations, high deployment costs, and difficulties integrating with existing ICT infrastructure [1]. **Standardization**: Lack of useful QKD standards that support certification and interoperability which hinders practical adoption [1].
Potential for misuse	Quantum computers could be used to design novel weapons, destabilize financial markets, or create advanced deepfakes [6]. The dual-use nature (beneficial civilian and harmful military/illicit applications) is a core governance challenge [6].
Economic disruption	May render existing technologies/business models obsolete, displace workers, and lead to market concentration [5]. The financial sector faces significant PQC transition costs. Estimated economic value: $900M - $2T by 2035 [5].
Equitable access and the "Quantum divide"	High R&D costs and specialized workforce needs risk concentrating capabilities in few advanced countries/corporations, exacerbating global inequalities [5]. Ensuring democratized access is critical.

Whilst it is difficult to pinpoint exactly the financial and societal cost of the risk highlighted above, some modelling has been undertaken which forecasts significant financial damage the national and the global economy (see Figure 1 below).

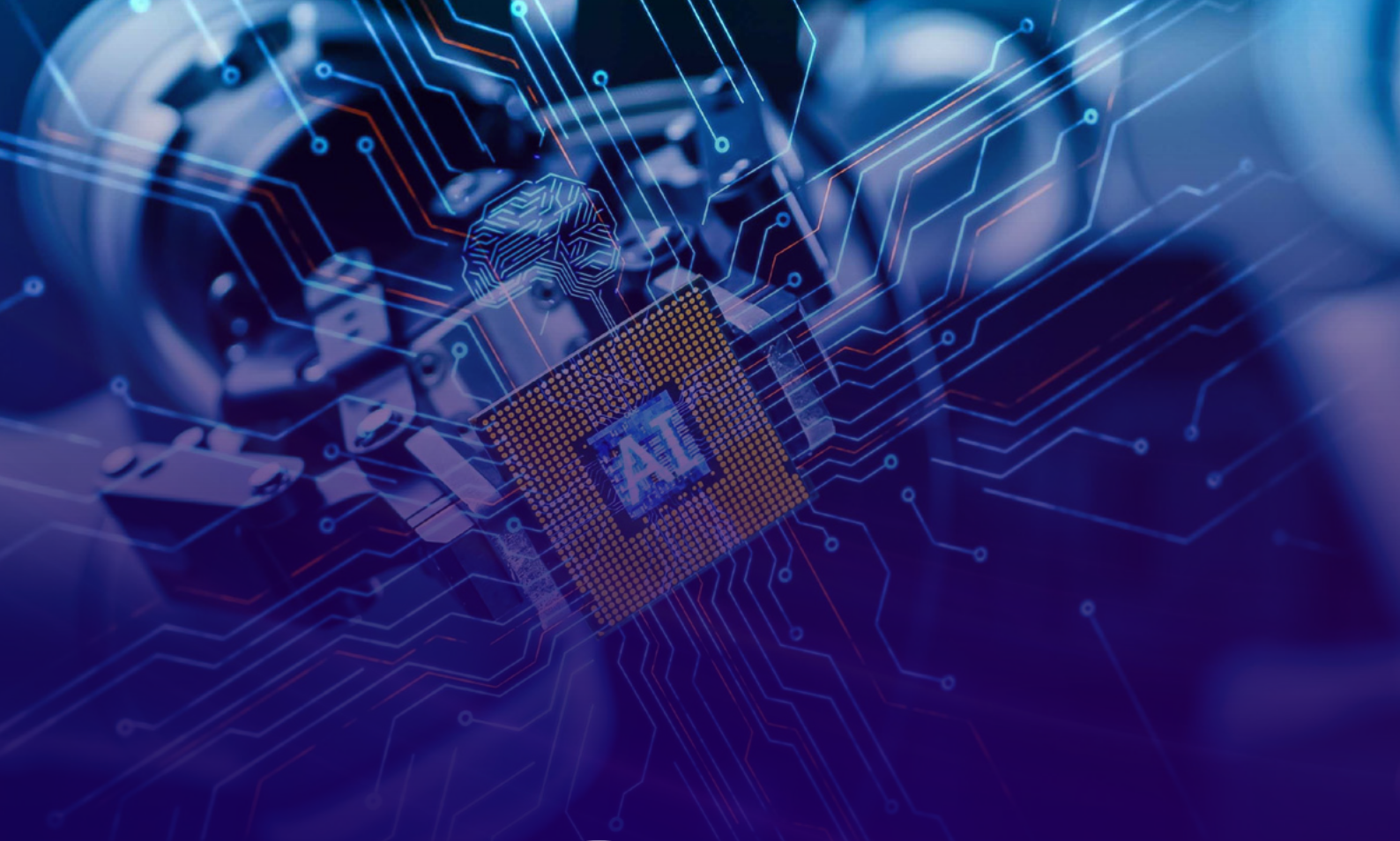
Figure 1: Potential Risks of Quantum Technologies – Illustrative Datapoints

Data point	Why it matters
US $2 – 3.3 trillion modelled loss of US GDP from a single quantum-enabled cyber-attack that disrupts the Fedwire real-time-gross-settlement system (10 – 17 % GDP hit, six-month recession) [23]	Puts a plausible upper bound on macro-economic damage from a single quantum breach - bigger than the 2008 crisis; justifies treating PQC migration as systemic-risk insurance, not IT hygiene
US $10.5 trillion annual global cost of cyber-crime expected in 2025 [24]	Shows the financial scale of today's digital threat surface; a post-quantum "Q-Day" would raise that bill dramatically.
US $4.88 million new global average cost of a single data breach in 2024, up 10 % YoY [25]	Quantifies the "cost of doing nothing" before PQC migration; each breach is already expensive without factoring in quantum-enabled attacks.
US $40 billion deepfake and other gen-AI fraud losses projected for US banking by 2027 (up from $12.3 bn in 2023) [26]	Illustrates how rapidly quantum-accelerated AI tools could magnify deception, financial crime and social-engineering risks.

The interconnectedness of quantum risks demands a holistic governance strategy, as solutions to one threat often introduce new vulnerabilities. While the development of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) is driven by the quantum threat to encryption, these countermeasures are not infallible. PQC's security is conditional, based on resilience to known quantum algorithms [27].This premise is fragile; advances in quantum computing or cryptanalysis could render current standards obsolete, a risk evidenced by the public breaking of NIST candidates like SIKE and Rainbow [28]. Similarly, QKD technology is constrained by its own practical challenges, including hardware vulnerabilities, side-channel attacks, and significant range limitations.

In response to challenges like side-channel attacks, there is a significant international effort to develop formal certification frameworks for Quantum Key Distribution (QKD) systems and networks. This certification is widely seen as a crucial step for the technology's adoption, providing the necessary level of security assurance for its integration into modern ICT infrastructure. However, establishing these frameworks is a complex task. It involves bridging gaps in technical knowledge, building new testing and evaluation capabilities, and creating comprehensive standards that address everything from QKD protocols to theoretical and implementation security [14]. Efforts to develop these capabilities are already underway across academia, industry, and dedicated certification bodies. Achieving robust, globally recognised QKD certification will ultimately require coordinated collaboration among different standards development organisations (SDOs) and stakeholders to ensure a secure and interoperable quantum future.

Within the specific domains of ICT and Space, these risks and opportunities manifest with acuity. For the ICT sector, the overwhelming priority is mitigating the cryptographic threat to data security and communication infrastructure [5]. The integrity of global digital systems hinges on a successful and timely transition to PQC. For the Space sector, quantum technologies offer a paradigm shift. Quantum sensors promise revolutionary improvements in Positioning, Navigation, and Timing (PNT) services, potentially offering alternatives to GPS, which is vulnerable to disruption [29]. This is a significant opportunity for both civilian and military space applications. Quantum communication, via QKD, will be vital for securing satellite command and control links and protecting the vast amounts of data transmitted from space assets [9]. However, the same advanced sensing capabilities that offer benefits could also be used to track friendly space assets or conduct pervasive surveillance from space, posing new national security challenges [13]. Therefore, policy for the ICT sector must focus on cryptographic resilience and the security of network infrastructure. When it comes to the Space sector, policy must navigate a complex balance: eagerly pursuing the immense opportunities afforded by quantum sensing and communication while simultaneously developing safeguards against the national security risks inherent in these powerful new tools and ensuring the overall security and resilience of space-based systems.



03

PARALLELS WITH AI AS AN EMERGING TECHNOLOGY POLICY ISSUE

The challenges policymakers face in preparing for quantum technologies are not entirely unprecedented. The recent and ongoing efforts to govern AI offer numerous parallels, providing a rich source of lessons. Understanding these similarities is key to leveraging AI's experience for more effective quantum governance. Both AI and QT are:

Foundational technologies:

Both possess the potential to fundamentally reshape numerous sectors, scientific disciplines, and aspects of daily life. Their impact is not confined to niche applications but extends across the economy and society [30]

Data points:

AI: McKinsey estimates generative AI alone could unlock US $4.4 trn/yr in productivity gains [31].

QT: McKinsey projects quantum computing could create ≈ US $1.3 trn in economic value by 2035 [32].

Characterized by high uncertainty:

Significant uncertainty surrounds the future development timelines, the ultimate scope of their capabilities, and the full range of their societal impacts for both AI and QT [32]. This makes long-term prediction difficult and complicates traditional, static regulatory approaches.

Data points:

AI: U.S. private AI investment hit US $109.1 bn in 2024 (up 18 % YoY) [33].

QT: Start-ups raised US $1.2 bn in Q1 2025 - a 125 % YoY jump [34].

Driven by a rapid R&D pace:

Research and development in both fields are progressing at a remarkable speed, often outstripping the ability of policy and legal frameworks to adapt. This phenomenon, known as the "pacing problem," poses a persistent challenge to effective governance [35].

Data points:

AI: Google's Gemini 2.0 went from a 128 k-token to 2 million-token context window in <12 months [36].

QT: Global Risk Institute survey puts the chance of a crypto-breaking quantum computer at 17–34 % by 2034 and 79 % by 2044 [37].

Dual-use in nature:

Both AI and QT have significant dual-use potential. Their applications can serve beneficial civilian purposes but can also be adapted for military uses or by malicious actors, raising complex national security and ethical concerns [19].

Data points:

AI: The AI Incident Database logged its 1,000th recorded harm event in Mar 2025 [38].

QT: At least 5 defence-oriented U.S. quantum bills (e.g., S.579, S.1346, H.R.3259) were introduced in 2025 alone [39].

Subject to a significant investment race:

A global competition for leadership in both AI and QT is well underway, marked by substantial government funding initiatives and vigorous private sector investment [1]. This race can drive innovation but also create pressures that might sideline safety and ethical considerations.

Data points:

AI: China is reported to be investing up to $98bn in AI investment in 2025, a 48% increase on 2024. Whilst the US government announced in 2025 it's Stargate Project, which plans to deploy up to $500bn over four years into advanced data centre networks in the US [40].

QT: Governments, corporates and VCs have committed >US $55.7 bn to quantum programmes worldwide as of Jul 2025 (Qureca tracker) [41].

Reliant on specialised expertise:

Effective governance of both AI and QT requires a deep technical understanding that is often scarce among policymakers and within regulatory agencies. Bridging this expertise gap is a critical prerequisite for informed policy.

Data points:

AI: 46% of C-suite executives cite "talent skill gaps" as the #1 barrier to AI scaling (McKinsey US CxO survey, Nov 2024) [42].

QT: Only 1 qualified candidate for every 3 quantum job openings (McKinsey, Mar 2025) [43].

Imbued with ethical dimensions

Both technologies raise profound ethical questions concerning issues such as bias and discrimination (especially in AI, with potential parallels in QML), fairness, accountability, privacy, human autonomy, and broader societal impact [6].

Globally interconnected:

The ecosystems for R&D, talent recruitment, and supply chains for both AI and QT are inherently global. This interconnectedness means that purely national approaches to governance are insufficient; international cooperation is essential [30].

Challenging to existing regulatory structures

Both AI and QT strain existing legal and regulatory frameworks, which were often designed for more static, less complex, and less data-intensive technologies. New models of governance are often required.

To illustrate these parallels more directly, **Appendix 1** provides a comparative overview.

This comparative framework underscores why the lessons learned from AI governance are so pertinent to quantum technologies. However, while the parallels are strong, a crucial difference lies in the current state of deployment and accessibility. Many AI tools, from search algorithms and recommendation systems to generative models like ChatGPT and facial recognition technologies, are already widely deployed, consumer-facing, and deeply integrated into critical societal systems [30]. In contrast, most QTs are still in the research and development phase or are confined to early, specialized deployments, often within research labs or for niche industrial applications [1]. This distinction is vital. AI policy has frequently been reactive, attempting to address issues after technologies have achieved widespread adoption and societal impact. QT governance, by virtue of its current stage of development, has a (rapidly shrinking) window of opportunity to be more anticipatory and foundational. Policymakers can endeavor to establish governance principles, ethical guidelines, and risk management frameworks before quantum technologies become pervasively integrated into society - a luxury that was largely unavailable for AI. This proactive posture could lead to more effective and less disruptive governance outcomes for the quantum era.

04

SIX LESSONS LEARNED FROM THE AI POLICY AND REGULATORY PROCESS

The global effort to govern AI, though still evolving, offers a rich tapestry of experiences - both successes and failures - from which valuable lessons can be drawn for quantum technology preparedness. These lessons span process, approach, and principle.

1. Stakeholder Engagement: The Imperative of Inclusivity

The Lesson from AI Governance: Experience with AI has shown that early and inclusive stakeholder engagement is a critical determinant of success. Policies developed through broad consultation are more robust, while those created in isolation often lack public trust. This concern is reflected in public sentiment; a 2023 Pew Research survey found that 52% of Americans are more concerned than excited about the increasing use of AI [44], with many worrying about the pace of change and a lack of oversight by developers and government.

mplication for Quantum Technology: Given its even greater complexity, the need for broad stakeholder engagement is amplified for quantum technology. The process must actively involve a diverse range of experts - from physicists and ethicists to social scientists and potential end-users - to ensure a comprehensive grasp of the challenges and opportunities ahead.

2. Balancing Innovation with Risk: Crafting Agile Governance

The Lesson from AI Governance:

A central challenge has been to strike a balance between fostering innovation and mitigating risk. The scale of this challenge is immense; in 2023 alone, private investment in generative AI surged to $22.4 billion, nearly a ninefold increase from 2022 [45], fuelling rapid progress. A hands-off approach allows harms like bias to proliferate, while overly prescriptive rules can stifle such beneficial research.

Implication for Quantum Technology: Implication for Quantum Technology: Regulators should pursue a risk-based and context-specific approach, focusing attention on high-risk applications (e.g., cryptographically relevant quantum computers) rather than imposing broad restrictions on all R&D [46]. Flexible governance structures, such as principles-based codes of conduct, standards, and adaptive regulations, can provide necessary guardrails without unduly hindering innovation. Furthermore, "smart regulation" should not only aim to restrict undesirable outcomes but also to actively incentivize responsible behaviors and the development of "Responsible Quantum Technology (RQT) by design" [30].

3. International Collaboration: Building Global Norms

The Lesson from AI Governance:

The global nature of AI has underscored the necessity of international cooperation. While initiatives like the OECD AI Principles have aimed to create global frameworks, progress has been complicated by geopolitical competition. This is evident in the concentration of development; in 2023, institutions in the United States were responsible for producing 61 notable AI models, far outpacing the European Union (21 models) and China (15 models), illustrating the competitive dynamics that can challenge unified governance [46].

Implication for Quantum Technology: Given its profound global implications, particularly for cybersecurity, building an international consensus on foundational principles is crucial. This requires proactive coordination on standards for critical technologies like Post-Quantum Cryptography (PQC) and collaboration on mitigating global risks. Existing international fora (e.g., OECD, UN) should be leveraged, and novel cooperative mechanisms, potentially including a "UN Quantum Treaty" or an "Atomic Agency for Quantum-AI" as proposed by some analysts, could be considered for high-stakes areas [30].

4. The 'Pacing Problem': Keeping Governance Ahead of Technology

The Lesson from AI Governance:

AI's rapid advancement has consistently outpaced the ability of legal systems to adapt, creating a significant "pacing problem." The scale of this is stark: according to Stanford's 2024 AI Index, the training time for top image-classification systems has plummeted from 6.2 minutes in 2018 to just 12 seconds in 2023, a pace of change that legal systems are ill-equipped to match [46]. Governance must become more agile, prioritizing proactive measures that shape development.

mplication for Quantum Technology: A similar, if not accelerated, pacing problem must be anticipated. Governance frameworks for quantum must be designed with agility and adaptability as core features from the outset, enabling regulators to guide the ecosystem responsibly before the technology is widely deployed. This involves prioritizing ex-ante measures, especially for the foundational layers of quantum technology such as hardware development and core algorithmic research, to guide the ecosystem responsibly [30].

5. Transparency, Accountability, and Fairness: Core Principles for Trust

The Lesson from AI Governance: Transparency, accountability, and fairness are the central tenets of responsible AI. However, a major challenge has been retrofitting these principles onto "black box" systems, where a lack of transparency makes it difficult to address algorithmic bias after the fact. Landmark U.S. government research confirmed this risk, finding that top facial recognition algorithms could have false positive rates for Asian and African American faces that were 10 to 100 times higher than for Caucasian faces [47].

mplication for Quantum Technology: These principles are even more critical for quantum systems, where the underlying physics can make "explainability" exceptionally challenging. It is vital to embed these values early by promoting transparency about capabilities, establishing clear accountability frameworks, and proactively addressing potential biases in applications like Quantum Machine Learning (QML). Frameworks promoting 'Responsible Quantum Technology (RQT) by design' are vital for embedding these values early [30].

6. Building Policymaker Literacy: Bridging the Knowledge Gap

The Lesson from AI Governance:
A persistent knowledge gap between developers and policymakers has hindered the creation of effective regulations. This information asymmetry is particularly challenging as the volume of policymaking increases; the Stanford AI Index identified a surge in AI-related regulations globally, with the number of legislative bodies passing such rules rising from just 1 in 2016 to 37 in 2023 [48]. Ensuring these numerous regulations are technically sound is a monumental task

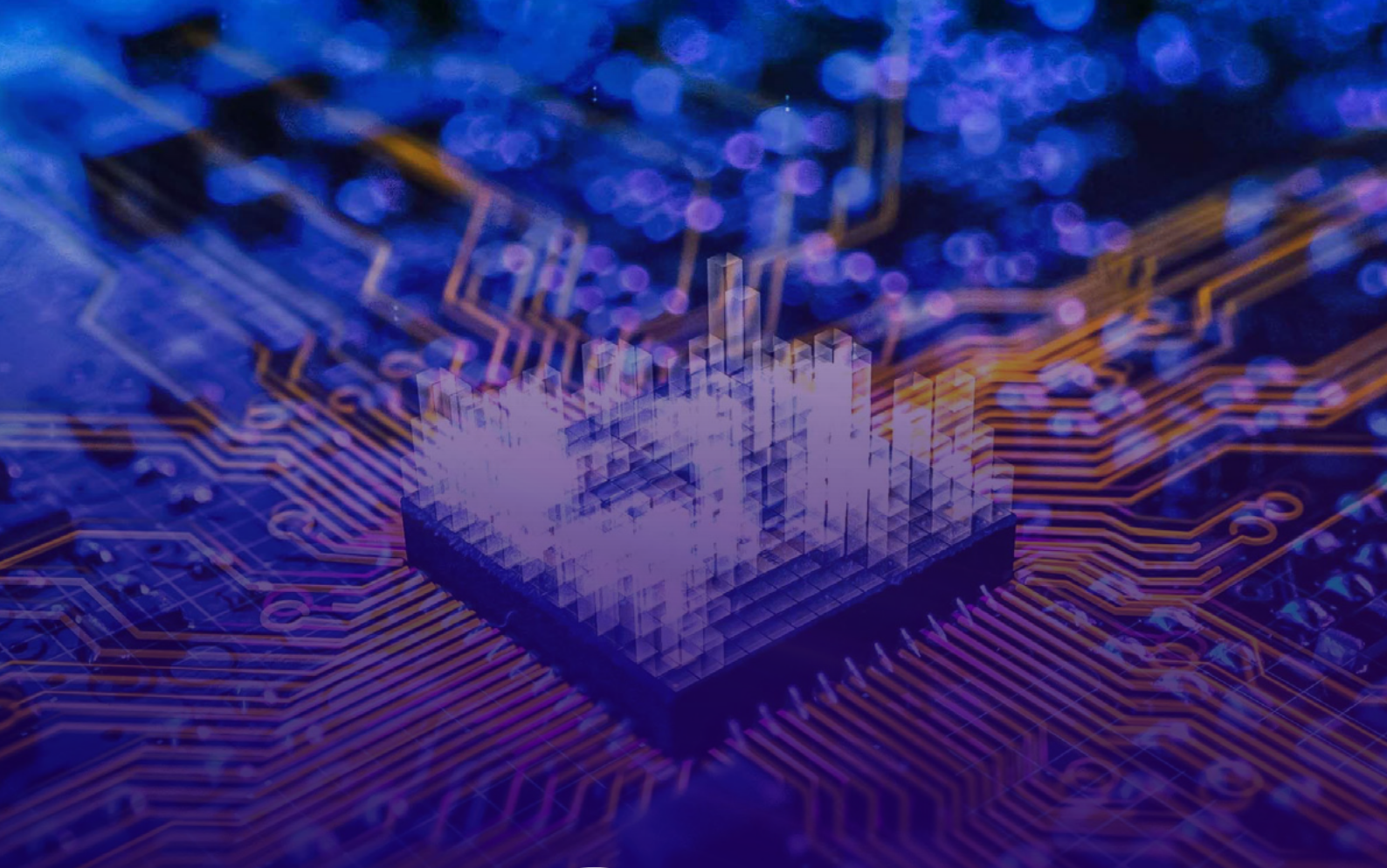
mplication for Quantum Technology: The technical barrier to understanding quantum mechanics is significantly higher than for AI. Therefore, a sustained and substantial investment in educating policymakers and regulators about quantum principles, applications, and risks is a paramount and urgent requirement for effective governance [1].

Appendix 2 summarizes these key lessons.

Discussion

A recurring pattern in the AI governance experience is the difficulty of retrofitting ethical considerations, safety measures, and governance frameworks onto technologies that have already been widely deployed and deeply integrated into societal structures [49]. This often leads to attempts to address issues like algorithmic bias, misuse of AI for surveillance, or lack of transparency in systems that are already operational and scaled, which is invariably more complex and less effective than addressing these concerns during the design and development phases. Quantum technologies, being largely at an earlier stage of the innovation lifecycle, present a strategic opportunity to invert this pattern. There is a chance to embed ethical frameworks, safety protocols, and principles of responsible innovation (such as RQT by design [30]) into the very fabric of quantum R&D and initial deployment strategies. This proactive integration can shift the paradigm from "ethics as an afterthought" to "ethics by design," potentially leading to a more responsible and societally aligned technological trajectory.

Furthermore, the AI experience has starkly highlighted the inherent tension between national ambitions for technological leadership and economic competitiveness, on the one hand, and the imperative for global cooperation in technology governance, on the other [30]. For quantum technologies, which possess even more direct and potentially disruptive national security implications - ranging from code-breaking capabilities that could undermine global cybersecurity to advanced military sensing applications - this tension is likely to be significantly amplified. The lesson here is that while national competition in fostering quantum ecosystems is a natural and expected development, there are specific areas of shared existential risk where international cooperation becomes indispensable, even among geopolitical rivals. The potential for a global cryptographic collapse due to quantum computers, or the risk of an unconstrained quantum arms race [6], necessitates a level of diplomatic engagement and the establishment of international guardrails that may need to exceed those attempted for AI.



05

RECOMMENDATIONS FOR QUANTUM TECHNOLOGY PREPAREDNESS

Translating the lessons drawn from artificial-intelligence governance, as well as an understanding of quantum technologies' distinctive characteristics, into actionable strategies requires a genuinely multi-pronged approach. Policymakers must build foundational capacities, foster responsible development and ensure effective international coordination. At the same time, these strategies must be sequenced according to the differing technology-readiness levels across the quantum landscape: fault-tolerant quantum-computing prototypes are edging towards practical, if still narrow, applications, whereas global quantum-communication networks remain at an earlier, capital-intensive pilot stage. The recommendations that follow therefore place immediate emphasis on domains closest to market deployment while laying groundwork for those that will mature later.

Developing Standards

The establishment of robust, widely accepted standards is fundamental for interoperability, security, and market confidence. Targeting PQC, QKD interoperability and quantum-computing benchmarks first is a matter of leverage: these three domains sit closest to the "root of trust" for the entire quantum stack, so clear, harmonised standards here cascade stability and confidence into every downstream application. By locking in common security primitives, interface conventions and performance yardsticks at the outset, governments and industry can channel resources efficiently, avoid vendor lock-in, and create a predictable roadmap that accelerates - not fragments - the broader quantum-technology ecosystem.

- Post-Quantum Cryptography (PQC): The highest priority is to accelerate and coordinate the global transition to PQC standards to protect digital infrastructure from the future threat of quantum computers [4]. Governments should actively support and adopt the standards emerging from bodies like the U.S. National Institute of Standards and Technology (NIST) [50]. International alignment on these standards is critical to prevent a fragmented global cryptographic landscape, which would complicate security for multinational organizations and cross-border data flows [51]. The urgency is underscored by timelines suggesting PQC migration for high-priority assets by 2030 and full deprecation of vulnerable algorithms by 2035 [52].

- QKD interoperability and certification: For quantum communication, particularly QKD, developing international standards for system interfaces and protocols is crucial to ensure interoperability between equipment from different vendors and to facilitate the integration of QKD into existing and future ICT and Space communication networks [7]. Efforts by organizations like the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU) in this area are central to this [7]. They are creating standards that support QKD certification, with key examples including ETSI's QKD protection profiles (e.g., ETSI GS QKD 016), the criteria in ISO/IEC 23837, and the QKD protocol frameworks under development in the ITU-T.

- Quantum computing benchmarks: While the field of quantum computing is still in its early stages, making it difficult to establish formal standards, developing common benchmarks is important for assessing performance [53]. Given the current technological immaturity, initial benchmarking efforts will likely focus on foundational metrics such as qubit count, gate fidelities, and coherence times. As the technology matures, this focus will likely need to shift towards more holistic, application-centric benchmarks that can assess the practical capabilities of different hardware and software platforms [54]. This evolving approach to benchmarking is vital for guiding investment decisions, tracking real-world progress, and managing expectations in a rapidly advancing field.

Establishing Testing and Validation Frameworks

Rigorous testing and validation are essential to ensure the reliability, security, and performance of quantum technologies before widespread deployment. Initially, frameworks should concentrate on near-term quantum-computing devices and software, expanding to quantum communication and sensing as those technologies mature.

- Frameworks and methodologies must be developed for testing and validating quantum hardware (e.g., qubit quality, coherence times), software (e.g., algorithm correctness, compiler efficiency), and complete systems [8]. This is particularly critical for applications in sensitive sectors such as finance, healthcare, and defence.
- Drawing lessons from AI, these frameworks should also incorporate assessments for ethical considerations, such as potential biases in quantum machine learning algorithms or privacy implications of quantum data processing.
- NIST's Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP), which are being extended to PQC algorithms, can serve as valuable models for establishing similar validation schemes for other quantum technologies [55].

Promoting R&D in Safety, Security, and Ethics

Investment in research should not only focus on advancing quantum capabilities but also on understanding and mitigating associated risks..

- Governments should allocate dedicated funding for R&D specifically aimed at quantum safety (e.g., ensuring the reliable control of complex quantum systems), security (extending beyond PQC to include the physical security of quantum devices and resilience against novel quantum attacks), and the ethical, legal, and social implications (ELSI) of quantum technologies [56].
- Publicly funded research programs should actively promote and incentivize the integration of "Responsible Quantum Technology (RQT) by design" principles, ensuring that safety, ethical considerations, and security are considered from the earliest stages of R&D [30].
- Support should be provided for foresight studies and research into potential misuse scenarios of quantum technologies to inform proactive risk mitigation strategies [6].

Building Regulatory Expertise and Capacity

Effective governance of quantum technologies requires that policymakers and regulatory bodies possess sufficient understanding and expertise.

- Invest in comprehensive and ongoing programs to enhance quantum literacy among policymakers, regulators, legal professionals, and their staff [1]. This includes understanding fundamental quantum principles, the capabilities and limitations of different quantum technologies, and their potential societal impacts.
- Cultivate multidisciplinary expertise within regulatory agencies, bringing together individuals with backgrounds in quantum science, engineering, computer science, law, ethics, and public policy [6].
- Support the development of "public interest quantum" professionals - individuals with legal, ethical, and social science expertise who can bridge the gap between technology developers and societal concerns [57].

Fostering International Coordination on Standards and Risk Mitigation

Given the global nature of quantum technology development and its implications, international cooperation is indispensable.

- Actively participate in and strengthen international dialogues and initiatives (e.g., through the OECD, World Economic Forum, UN bodies like the Geneva Science and Diplomacy Anticipator (GESDA)'s "Quantum for All" [58] initiative to develop shared norms, common technical standards, and coordinated approaches to risk management and ethical oversight [1].
- Collaborate internationally on monitoring global quantum technology advancements, identifying emerging threats, and sharing best practices for governance.
- Explore mechanisms for international oversight and verification for particularly sensitive dual-use quantum technologies, potentially drawing inspiration from models like the International Atomic Energy Agency (IAEA), especially for convergent quantum-AI capabilities [30].

Specific Sector Considerations

Tailored strategies will be needed for sectors uniquely impacted by quantum technologies.

- ICT: The absolute priority is the timely and comprehensive transition to PQC for all digital infrastructure to safeguard data and communications [4]. This involves developing and implementing standards for secure quantum communication protocols (including QKD and Quantum Random Number Generators - QRNGs) and addressing the security of supply chains for critical quantum components.
- Space: Develop policies to enable and secure satellite communications using QKD and PQC [9]. Establish clear guidelines for the responsible use of quantum sensing capabilities from space, balancing the benefits for earth observation and scientific research against potential surveillance risks. Promote R&D in quantum PNT systems to enhance resilience against GPS vulnerabilities, a critical concern for both civilian and military space operations [29]. The rapid advancements in space-based quantum communication, exemplified by China's Micius satellite experiments [59], highlight the urgency of developing international norms in this domain.
- Finance: Regulatory bodies should guide, and where necessary mandate, the PQC transition to protect sensitive financial data, transactions, and critical market infrastructure [60]. The regulatory implications of using quantum algorithms for trading, risk assessment, and portfolio optimization also require careful examination [8]. The World Economic Forum's roadmap for quantum security in the financial sector offers a valuable phased approach for industry and regulators [61].
- Healthcare: Develop robust ethical guidelines and regulatory frameworks for the use of quantum-enhanced diagnostics, quantum simulations for drug discovery, and QAI applications in medicine [19]. Ensuring the privacy and security of highly sensitive health information in the quantum era is paramount, alongside promoting equitable access to quantum-driven medical advancements.
- Defence: Responsibly integrate quantum technologies (sensing, communication, computing) into military applications while upholding international law and ethical norms [21]. Implement and enforce robust export controls on sensitive quantum technologies to prevent proliferation and establish clear protocols for protecting federally funded quantum research from foreign espionage or interference [29]. A key focus should be on leveraging quantum PNT for resilient navigation in contested environments [29]

Table 3 provides a summary of these recommendations.

Table 3: Actionable Recommendations for Quantum Technology Preparedness

Recommendation Category	Specific Action	Key Actors	Relevance to ICT/ Space
Standards development [4]	Accelerate PQC transition; develop QKD interoperability standards; establish QC benchmarks.	NIST, ETSI, ITU, ISO, national standards bodies, industry consortia.	Critical for ICT security (PQC, QKD); essential for secure Space comms (PQC, QKD) & QC assessment.
Testing & validation frameworks [8]	Develop methodologies for QT hardware/ software validation (performance, security, ethics).	National metrology institutes, research labs, regulatory agencies.	Ensures reliability/ security of ICT components & Space systems.
R&D (safety, ethics, security) [6]	Fund R&D in QT safety, security (beyond PQC), ethics; incentivize RQT by design; research misuse scenarios.	Funding agencies, universities, research institutions, industry.	Underpins secure/ ethical use in ICT (e.g., QML bias) & Space (e.g., sensor misuse).
Regulatory capacity building [1]	Enhance quantum literacy for policymakers/ regulators; develop multidisciplinary expertise; foster "public interest quantum" professionals.	Governments, educational institutions, professional organizations.	Essential for informed governance of QT in ICT (e.g., data privacy) & Space (e.g., PNT regulation).
International coordination [1]	Engage in global dialogues (OECD, WEF, UN) for shared norms, standards, risk mitigation; explore oversight for dual-use QT.	Governments, international organizations, diplomatic channels.	Crucial for global PQC, QKD standards impacting ICT/ Space; managing transboundary risks (e.g., satellite security).
Sector-specific actions: ICT [4]	Prioritize PQC transition; develop secure quantum comms protocols; address supply chain security.	Telecom regulators, cybersecurity agencies, industry.	Core to ICT infrastructure resilience and data protection.

Recommendation Category	Specific Action	Key Actors	Relevance to ICT/ Space
Sector-specific actions: Space [9]	Policies for secure satellite comms (QKD/PQC); guidelines for quantum sensing from space; promote quantum PNT R&D.	Space agencies, defence departments, international space bodies.	Revolutionizes Space capabilities (PNT, comms, observation) but requires careful risk management.
Sector-specific actions: Finance [60]	Guide/mandate PQC transition; regulate quantum algorithms in trading/risk.	Financial regulators, central banks, industry bodies	Protects financial stability and data integrity.
Sector-specific actions: Healthcare [19]	Ethical guidelines for quantum diagnostics, drug discovery, QAI; ensure data privacy & equitable access.	Health regulators, ethics committees, research funders.	Balances innovation with patient safety and rights.
Sector-specific actions: Defence [21]	Responsible QT integration; robust export controls; protect funded research; focus on PNT resilience.	Defence departments, intelligence agencies, export control authorities.	Enhances national security but requires strict oversight of dual-use aspects.

Discussion

Many of these recommendations - particularly those related to establishing standards, funding cutting-edge R&D, and building a skilled workforce - require significant and sustained public investment. The long-term development horizon for many quantum technologies, coupled with the sheer scale of challenges like the PQC transition (with initial estimates for U.S. non-National Security System federal government upgrades alone reaching $7.1 billion [51]), underscores this need. Securing consistent financial support is a foundational prerequisite for the effective implementation of a comprehensive quantum preparedness strategy. Legislative initiatives, such as the proposed Department of Energy (DOE) Quantum Leadership Act in the U.S. which aims to authorize over $2.5 billion for DOE quantum R&D programs [62], exemplify the scale of commitment required. Without such robust and long-term public investment, the ability to execute many of the specific actions outlined will be severely constrained.

Furthermore, achieving the "human-centric and values-based" development and use of quantum technologies, as advocated by organizations like the OECD [63], extends beyond the implementation of technical standards and formal regulations. It calls for a broader societal dialogue about the kind of future that should be built with these powerful new tools and the ethical guardrails that are necessary to guide their trajectory. This connects back to the importance of stakeholder engagement but also implies a proactive role for governments and public institutions in fostering public education and facilitating deliberative processes. Such efforts are essential to ensure that the development and deployment of quantum technologies align with broadly shared societal values and serve the public good, rather than being driven solely by narrow technical or economic objectives [6].

06

CONCLUSION

Learning from Hindsight to Apply Foresight

CONCLUSION

The emergence of quantum technologies presents humanity with a familiar challenge in a new guise: how to govern powerful, uncertain, and potentially transformative innovations in a way that maximizes their benefits while responsibly managing their risks. This paper has argued that the recent, and often turbulent, journey of AI policy and regulation offers a rich source of lessons - a form of hindsight that can be invaluable in cultivating the foresight needed for the quantum era.

The parallels between AI and quantum technologies as policy issues are striking: both are foundational technologies with dual-use potential, characterized by rapid R&D, high uncertainty, significant investment, a need for specialized expertise, profound ethical dimensions, and global interconnectedness that challenges existing regulatory structures. By recognizing these commonalities, policymakers can anticipate similar governance challenges for quantum technologies and, more importantly, leverage the strategies and avoid the pitfalls observed in the AI domain.

Key lessons from AI governance - such as the critical importance of early and broad stakeholder engagement, the need for agile and risk-based regulatory approaches that balance innovation with safety, the indispensability of international collaboration for addressing global challenges, the urgency of tackling the 'pacing problem' where technology outstrips regulation, the centrality of principles like transparency and accountability, and the necessity of building policymaker literacy - provide a robust toolkit for quantum preparedness.

The recommendations outlined offer a pragmatic roadmap. Prioritizing the development and adoption of standards, especially for post-quantum cryptography and QKD interoperability, is crucial for securing our digital infrastructure, particularly in the vital ICT and Space sectors. Establishing rigorous testing and validation frameworks, promoting R&D in quantum safety and ethics, building regulatory expertise, and fostering international coordination are all essential components of an effective strategy. Sector-specific considerations for finance, healthcare, and defence further tailor this approach to address unique vulnerabilities and opportunities.

Ultimately, the challenge of quantum governance is not merely technical or legal; it is also societal. It requires a commitment to anticipatory action, a willingness to learn from past experiences, and a collaborative spirit that transcends national and disciplinary boundaries. While the quantum future remains uncertain, the lessons from AI provide a clearer view of the path ahead. By embracing these insights, policymakers can shape the development and deployment of quantum technologies in a manner that is more proactive, agile, and aligned with human values, fostering a quantum future that is both innovative and responsible. The task is significant, but by learning from hindsight, policymakers are better equipped to apply the foresight necessary to navigate the complexities of the quantum era effectively.

07

APPENDICES

APPENDICES

Appendix 1: Comparative Overview of AI and Quantum Technology Governance Challeng

Governance Challenge Area	AI Manifestation	Quantum Manifestation
Foundational potential [6]	Transformation of industries (e.g., healthcare, finance, transport), science, and daily life.	Potential for similar breadth of transformation (e.g., medicine, materials, finance, computing paradigms).
High uncertainty & pace [6]	Rapid evolution of models (e.g., generative AI), unpredictable emergent capabilities, fast adoption cycles.	Uncertain timelines for fault-tolerant QC, evolving hardware/ software, rapid discovery in algorithms and applications.
Dual-use nature [21]	Autonomous weapons, surveillance tools, disinformation campaigns vs. beneficial applications.	Code-breaking (cryptography), advanced military sensing, secure communications for illicit actors vs. scientific and industrial breakthroughs.
Investment & competition [1]	Intense global race for AI supremacy, massive private and public investment.	Similar global race for quantum leadership, significant national initiatives and funding.
Expertise gap [1]	Policymakers struggling to keep up with AI's technical complexities and implications.	Even higher technical barrier for quantum physics and engineering, requiring specialized knowledge for effective oversight.
Ethical dimensions [13]	Bias in algorithms, job displacement, privacy erosion, accountability gaps, "black box" problem.	Surveillance via quantum sensors, equitable access to quantum resources, ethics of QML, security of quantum data, misuse potential.
Global interconnectedness [1]	International R&D collaborations, global talent pool, cross-border data flows, multinational tech companies.	Global scientific community, international supply chains for specialized components (e.g., cryogenics), need for global standards.
Regulatory lag (Pacing Problem) [35]	Laws and regulations struggling to adapt to AI's rapid deployment and evolving capabilities.	Potential for even faster divergence if governance is not proactive, especially given long-term implications (e.g., HNDL).

Appendix 2: Key Lessons from AI Policy Development for Quantum Governance]

AI Policy Lesson Area	Key Learning from AI	Implication/Application for Quantum Governance
Stakeholder engagement [64]	Early, broad, and inclusive engagement with diverse stakeholders leads to more robust and legitimate policies.	Essential for QT due to complexity; must include scientists, ethicists, industry, users (ICT, Space), and public.
Balancing innovation & risk [3]	Risk-based, context-specific approaches are better than broad prohibitions; flexible governance needed.	Adopt adaptive, principles-based regulation for QT; focus on high-risk applications; incentivize "Responsible Quantum Technology by design."
International collaboration [30]	Global nature of tech requires cooperation on standards and ethics, though geopolitical tensions are a challenge.	Proactively seek international consensus on QT norms, PQC, risk mitigation (e.g., non-proliferation); leverage existing fora and explore new models.
Addressing the 'Pacing Problem' [35]	Tech outpaces regulation; agile tools and ex-ante measures are more effective than reactive ex-post enforcement.	Design agile QT governance from the start; prioritize ex-ante measures for foundational layers; encourage information sharing between developers and regulators.
Transparency, accountability, fairness [30]	These are core principles for responsible AI, vital for trust and mitigating harm (e.g., bias).	Directly transferable and critical for QT; "explainability" may be harder. Embed in RQT by design.
Building policymaker literacy [1]	Knowledge gap hinders effective regulation; AI literacy programs for policymakers are crucial.	Even higher technical barrier for QT; sustained investment in educating policymakers and regulatory staff on quantum concepts and implications is paramount.

08

REFERENCES

REFERENCES

[1] OECD, "A policymaker's guide to quantum technologies in 2025," February 2025. [Online]. Available: https://www.oecd.org/en/blogs/2025/02/a-policymakers-guide-to-quantum-technologies-in-2025.html .

[2] IBM, "What Is quantum computing?," June 2025. [Online]. Available: https://www.ibm.com/think/topics/quantum-computing.

[3] ITI, "ITI's Quantum Technologies Policy Principles and Essentials for Global Policymakers," April 2025. [Online]. Available: https://www.itic.org/documents/emerging-technologies/ITI_QuantumPolicyGuide_042025.pdf.

[4] S. Ramesh, A. Sarkar and B. Sun, "Quantum Technologies: Key Strategies and Opportunities for ICT Leaders," WEF, 2025. [Online]. Available: https://reports.weforum.org/docs/WEF_Quantum_Technologies_Key_Strategies_and_Opportunities_for_ICT_Leaders_2025.pdf.

[5] S. Ramesh and A. Sarkar, "Embracing the Quantum Economy: A Pathway for Business Leaders," WEF, January 2025. [Online]. Available: https://reports.weforum.org/docs/WEF_Embracing_the_Quantum_Economy_2024.pdf.

[6] R. Wibmer, "A First Quantum Governance Reader: Literature, Principles, Reports," Universität Innsbruck, Future Law Working Papers, Innsbruck, 2025.

[7] M. Luken, "Quantum Key Distribution & the Path to Post-Quantum Computing," CISCO, 6 February 2025. [Online]. Available: https://blogs.cisco.com/security/quantum-key-distribution-and-the-path-to-post-quantum-computing.

[8] A. Ramachandran, "Quantum Computing for Portfolio Optimization and Risk Analysis: Transformative Approaches and Practical Frameworks in Financial Services," November 2024. [Online]. Available: https://www.researchgate.net/publication/385822616_Quantum_Computing_for_Portfolio_Optimization_and_Risk_Analysis_Transformative_Approaches_and_Practical_Frameworks_in_Financial_Services.

[9] Quantum Computer Report by GQI, "IonQ and Intellian Sign MoU to Explore Quantum Networking Applications in Satellite Communications," 16 April 2025. [Online]. Available: https://quantumcomputingreport.com/ionq-and-intellian-sign-mou-to-explore-quantum-networking-applications-in-satellite-communications/.

[10] AWS, "What is Quantum Computing?," [Online]. Available: https://aws.amazon.com/what-is/quantum-computing/.

[11] J. Hilgevoord and J. Uffink, "The Uncertainty Principle," Stanford Encyclopedia of Philosophy Archive, no. Winter, 2016.

[12] Cigent, "Quantum Computing Explained | Cigent Technology Inc.," 20 June 2023. [Online]. Available: https://www.cigent.com/federal/blog/quantum-computing-explained-history-implications-and-important-concepts.

[13] M. Ivezic, "Ethical and Privacy Implications of Quantum Sensing," PostQuantum, 9 August 2023. [Online]. Available: https://postquantum.com/quantum-sensing/ethics-privacy-quantum-sensing/.

[14] ITU, "ITU Workshop on "Insights on QKD & QKDN certification: Recent developments and challenges"," 17 May 2024. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2024/0517/Pages/default.aspx.

[15] E. e. a. Oh, "A Perspective on Quantum Sensors from Basic Research to Commercial Applications," July 2024. [Online]. Available: https://arxiv.org/abs/2407.00689.

[16] N. e. a. Aquina, "A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography," EPJ Quantum Technology, vol. 12, p. 51, 2025.

[17] Cybersecurity & Information Systems Information Analysis Centre, "Are Fault-Tolerant Quantum Computers on the Horizon?," 2 March 2022. [Online]. Available: https://csiac.dtic.mil/articles/are-fault-tolerant-quantum-computers-on-the-horizon/.

[18] Q. Memon, M. Al Ahmad and M. Pecht, "Quantum computing: navigating the future of computation, challenges, and technological breakthroughs," Quantum Reports, vol. 6, no. 4, pp. 627-663, 2024.

[19] M. e. a. Kop, "A Brief Quantum Medicine Policy Guide," 6 December 2024. [Online]. Available: https://petrieflom.law.harvard.edu/2024/12/06/a-brief-quantum-medicine-policy-guide/.

[20] Sustainability Director, "Ethical Implications of Quantum Grid Management," 14 April 2025. [Online]. Available: https://prism.sustainability-directory.com/scenario/ethical-implications-of-quantum-grid-management/.

[21] A. Perry, "Quantum Computing in Defence: Enhancing Military Strategy and Security," 29 November 2024. [Online]. Available: https://www.dcicontracts.com/quantum-computing-in-defence-enhancing-military-strategy-and-security/.

[22] S. Swami, "Security Challenges in Quantum Communication," International Journal of Scientific Research & Engineering Trends, vol. 11, no. 2, 2025.

[23] A. Herman and A. Butler, "Prosperity at Risk: The Quantum Computer Threat to the US Financial System," 3 April 2023. [Online]. Available: https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system.

[24] Virtasant AI Today, "AI Cybersecurity: How Companies Are Fighting $10.5T in Crime," 10 March 2025. [Online]. Available: https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system.

[25] IBM Security & Ponemon Institute, "Cost of a Data Breach Report 2024," July 2024. [Online]. Available: https://www.ibm.com/reports/data-breach.

[26] S. Lalchand, V. Srinivas, B. Maggiore and J. Henderson, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," 29 May 2024. [Online]. Available: https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html.

[27] Y. Jestin, "Quantum Communication Networks – The Next Frontier in Secure And Efficient Data Transfer," 19 February 2025. [Online]. Available: https://thequantuminsider.com/2025/02/22/guest-post-quantum-communication-networks-the-next-frontier-in-secure-and-efficient-data-transfer/.

[28] D. Geer, "NIST Post-Quantum Cryptography Candidate Cracked," 24 January 2023. [Online]. Available: https://cacm.acm.org/news/nist-post-quantum-cryptography-candidate-cracked/.

[29] C. M. Vidal Bustamente, "Accelerate America's Quantum Technology Leadership," Center for a New American Security, 20 January 2025. [Online]. Available: https://www.cnas.org/publications/commentary/accelerate-americas-quantum-technology-leadership.

[30] M. Kop, "Towards an Atomic Agency for Quantum-AI," 5 May 2025. [Online]. Available: https://www.researchgate.net/publication/391487957_Towards_an_Atomic_Agency_for_Quantum-AI.

[31] McKinsey & Company, "The economic potential of generative AI: The next productivity frontier," 14 June 2023. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier. [Accessed 11 July 2025].

[32] McKinsey & Company, "What is quantum computing?," 31 March 2025. [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing. [Accessed 11 July 2025].

[33] Stanford Institute for Human-Centered AI, "2025 AI Index Report: Economy," 2025. [Online]. Available: https://hai.stanford.edu/ai-index/2025-ai-index-report/economy. [Accessed 11 July 2025].

[34] M. Swayne, "Q1 2025 Quantum Technology Investment: What's Driving the Surge in Quantum Investment?," 27 May 2025. [Online]. Available: https://thequantuminsider.com/2025/05/27/q1-2025-quantum-technology-investment-whats-driving-the-surge-in-quantum-investment/. [Accessed 11 July 2025].

[35] T. N. Narechania and G. Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence," Yale Law and Policy Review, vol. 43, no. 1, 2024.

[36] K. Kavukcuoglu, "Gemini 2.0 is now available to everyone," 5 February 2025. [Online]. Available: https://blog.google/technology/google-deepmind/gemini-model-updates-february-2025/. [Accessed 11 July 2025].

[37] K. Townsend, "Cyber Insights 2025: Quantum and the Threat to Encryption," 3 February 2025. [Online]. Available: https://www.securityweek.com/cyber-insights-2025-quantum-and-the-threat-to-encryption/. [Accessed 11 July 2025].

[38] D. Atherton, "AI Incident Roundup – February and March 2025," 3 April 2025. [Online]. Available: https://incidentdatabase.ai/blog/incident-report-2025-february-march/. [Accessed 11 July 2025].

[39] US Congress, "S. 579 — A bill to amend the National Quantum Initiative Act..., 119th Cong., Congressional Record S974," 13 February 2025. [Online]. Available: https://www.congress.gov/119/crec/2025/02/13/171/30/CREC-2025-02-13-pt1-PgS974-2.pdf. [Accessed 11 July 2025].

[40] D. Kour, "China to deploy $98bn in AI investment this year amid US tech rivalry," 26 June 2025. [Online]. Available: https://techwireasia.com/2025/06/china-ai-investment-98-billion-2025-us-rivalry/.

[41] Qureca, "Quantum Initiatives Worldwide 2025," 9 July 2025. [Online]. Available: https://www.qureca.com/quantum-initiatives-worldwide/. [Accessed 11 July 2025].

[42] H. e. a. Mayer, "Superagency in the workplace: Empowering people to unlock AI's full potential," 28 January 2025. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work. [Accessed 11 July 2025].

[43] N. e. a. Mohr, "Five lessons from AI on closing quantum's talent gap—before it's too late," 1 December 2022. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/five-lessons-from-ai-on-closing-quantums-talent-gap-before-its-too-late. [Accessed 11 July 2025].

[44] M. Faverio and A. Tyson, "What the data says about Americans' views of artificial intelligence," Pew Research Center, 21 November 2023. [Online]. Available: https://www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/.

[45] V. Samborska, "Investment in generative AI has surged recently," Our World in Data, 30 August 2024. [Online]. Available: https://ourworldindata.org/data-insights/investment-in-generative-ai-has-surged-recently.

[46] Stanford University Institute for Human-Centered Artificial Intelligence, "The AI Index Report 2024: State of AI in 10 Charts," Stanford University Institute for Human-Centered Artificial Intelligence, 2024.

[47] P. Grother, M. Ngan and K. Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NIST Interagency Report 8280, 2019.

[48] Stanford University Institute for Human-Centered Artificial Intelligence, "The AI Index Report 2024: State of AI in 10 Charts," 2024.

[49] R. e. a. Coates, "Quantum Computing," January 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf.

[50] Industrial Cyber, "NIST advances post-quantum cryptography standardization, selects HQC algorithm to counter quantum threats," 12 March 2025. [Online]. Available: https://industrialcyber.co/nist/nist-advances-post-quantum-cryptography-standardization-selects-hqc-algorithm-to-counter-quantum-threats/.

[51] B. e. a. LaMacchia, "2024-2025 CRA Quadrennial Paper. The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead," Computer Research Association, 2024.

[52] D. e. a. Moody, "Transition to Post-Quantum Cryptography Standards," 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

[53] A. Barreneche and E. Thomas-Raynaud, "A policymaker's guide to quantum technologies in 2025," 3 February 2025. [Online]. Available: https://www.oecd.org/en/blogs/2025/02/a-policymakers-guide-to-quantum-technologies-in-2025.html.

[54] T. e. a. Lubinski, "Application-Oriented Performance Benchmarks for Quantum Computing," IEEE Transactions on Quantum Engineering, vol. 4, 2021.

[55] Industrial Cyber, "UK NCSC guidance focuses on quantum-resistant encryption to protect critical sectors by 2035," 20 March 2025. [Online]. Available: https://industrialcyber.co/regulation-standards-and-compliance/uk-ncsc-guidance-focuses-on-quantum-resistant-encryption-to-protect-critical-sectors-by-2035/.

[56] Clifford Chance, "Quantum State of Play," March 2025. [Online]. Available: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/03/quantum-state-of-play.pdf.

[57] M. Swayne, "RAND Europe: Quantum's Future Workforce Needs More Than Physicists," 14 April 2025. [Online]. Available: https://thequantuminsider.com/2025/04/14/rand-europe-quantums-future-workforce-needs-more-than-physicists/.

[58] gesda, "Quantum for All," 2025. [Online]. Available: https://www.gesda.global/quantum-for-all/.

[59] Asia and Pacific Research Center, "Policy and R&D trends of quantum technology in the leading countries of the Asia and Pacific Regions," Japan Science and Technology Agency, 2023.

[60] Deloitte Center for Financial Services, "Industry spending on quantum computing will rise dramatically. Will it pay off?," 2025. [Online]. Available: https://www2.deloitte.com/content/dam/insights/articles/us176540_cfs_fsi-predictions_quantum-capabilities-in-financial-services/DI_FSI-Predictions_Quantum-capabilities.pdf.

[61] Clearly Gottlieb, "Quantum Computing and the Financial Sector: World Economic Forum Lays Out Roadmap Towards Quantum Security," 30 January 2024. [Online]. Available: https://www.clearygottlieb.com/news-and-insights/publication-listing/quantum-computing-and-the-financial-sector-world-economic-forum-lays-out-roadmap-towards-quantum-security.

[62] M. Swayne, "Senators Introduce $2.5 Billion Bill to Expand U.S. Quantum Research," 14 February 2025. [Online]. Available: https://thequantuminsider.com/2025/02/14/senators-introduce-2-5-billion-bill-to-expand-u-s-quantum-research/.

[63] A. Barreneche and E. Thomas-Raynaud, "A quantum technologies policy primer," 6 February 2025. [Online]. Available: https://one.oecd.org/document/DSTI/DPC/STP(2024)3/FINAL/en/pdf.

[64] T. Nugraha, "AI Governance and Ethics: Lessons from the U.S. Visa Revocation Policy," 11 March 2025. [Online]. Available: https://moderndiplomacy.eu/2025/03/11/ai-governance-and-ethics-lessons-from-the-u-s-visa-revocation-policy/.

Acknowledgement

This white paper has been prepared in collaboration with the National Quantum-Safe Network (NQSN), National University of Singapore.

Co-author

Dr. Hao Qin

Senior Researcher, National Quantum-Safe Network

Centre for Quantum Technologies, National University of Singapore

Disclaimer

This paper is intended to provide an informative analysis of the subject matter from technical, commercial, and regulatory perspectives. It does not, by any means, represent CST's views or regulatory directions.

هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

www.cst.gov.sa