Science and Public Policy, 2025, **00**, 1–13
DOI: https://doi.org/10.1093/scipol/scaf065
Article

Public policy considerations of quantum computing

Kim Moloney[1,*] and Saif Al-Kuwari[2]

[1]College of Public Policy, Minaretein Building, Hamad Bin Khalifa University, Education City, Doha, 0000, Qatar
[2]College of Science and Engineering, LAS Building, Hamad Bin Khalifa University, Education City, Doha, 0000, Qatar
*Corresponding author. College of Public Policy, Hamad Bin Khalifa University, Doha, Qatar. E-mail: kmoloney@hbku.edu.qa

Quantum computing has migrated from the desks of theoretical physicists to its operationalization by engineers and scientists. After briefly noting the limited quantum discussions in disciplinary journals specific to public policy, we review the nature of quantum mechanics for a social science audience. We separate the public policy challenges of quantum computers into two categories: its cybersecurity and national security concerns and its concerns for other sectors of public policy. This includes our identification of quantum computers as a wicked and largely unstructured policy problem. This leads to our focus on how the quantum era currently interacts with the agenda-setting and policy formulation steps of the policy cycle. The article concludes by noting potential theoretical implications along with four risks of the quantum computing era for policymakers.

Keywords: quantum computing; quantum era; public policy; wicked policy; policy cycle.

1. Introduction

Despite a United Nations designation of 2025 as the International Year of Quantum Science and Technology, journals specific to the public policy and public administration discipline have infrequently discussed quantum developments. In a desktop search of the top 10 per cent (23 of 233) of journals in 'Public Administration'[1], quantum-focused research articles are infrequent. Our search led to three articles, of which two article focused on the quantum era (Overman 1999; Kong et al. 2024). Specifying further, we added the top Q1 and Q2 journals in the 'Public Administration' category plus the Q1 entrants (of 1,433 journals) in the 'Political Science and Sociology' category but exclusive to the information and communication technology (ICT) policy journals likely to publish quantum era articles. This included *Science and Public Policy*, *Journal of Data and Information Science*, *Information Polity*, *Government Information Quarterly*, *Policy and Internet*, *Information Technology for Development*, *Journal of Information Technology and Politics*, and *Science, Technology and Human Values*. This led to another three articles, of which only one had a quantum-era focus (Wang et al., 2022).

The paucity of quantum-era research in public policy and public administration journals contrasts with extensive quantum-era coverage by cybersecurity and national security scholars (e.g. Tigges et al., 2003; Stix 2005; Bernstein and Lange 2017; Raheman 2022). It also differs from an episodic coverage of quantum-era policy published *outside of* the public policy and/or ICT-focused policy journals. Examples include quantum-focused discussions of the law (Hoofnagle and Garfinkel 2022), smart workforces (Aiello et al., 2021), government tools (Johnson 2019), readiness (Coates and Chhetri 2024; Purohit et al., 2024), societal impacts (Vermaas 2017; Wolbring 2022), stakeholders (Umbrello et al., 2024), democratization (Seskir et al., 2023), international relations (Wendt 2015; Der Derian and Wendt 2022), and the economy (World Economic Forum 2023). Given a gap between the quantum era and its limited mentions in the academic journals specific to the public policy discipline, we have two research questions: (1) 'How do quantum computers vary from classical computers?' and (2) 'How might policy wickedness, (un)structured policy problems, and the policy cycle help public policy scholars approach quantum era studies?'

To start, readers may recall that classical physics has led to major scientific discoveries, including the discoveries that created the classical computers of today. It also includes new outputs that use classical computers such as artificial intelligence, blockchain, cloud computing, internet of things, virtual reality, and more (e.g. Amoore 2018; Van Deursen and Mossberger 2018; Clifton and Pal 2022; United Nations 2023). However, in the last 40 years, quantum researchers have created a new academic discipline: quantum information science (QIS). It is based on quantum physics (aka quantum mechanics). Quantum mechanics describes the behaviour of particles at the microscopic level, where phenomena not considered by classical physics are observed. Technologies based on QIS essentially harness such phenomena, surpassing the limits of counterpart technologies based on classical physics.

Just over 25 years ago, the US-based National Science Foundation (NSF) created its first Quantum Working Group. They defined QIS as 'a new field of science and technology, combining and drawing on the disciplines of physical science, mathematics, computer science, and engineering' (National Working Group 1999). Much has happened since the first Working Group. Research is published in new quantum-specific journals[2] and/or in the journals of the disciplines from

[1] Given no 'public policy' category for SJR/Scimago using Scopus data, we used the 'Public Administration' category and the 'Political Science and Sociology' category to find journal names. Articles were found via journal search engine, by not limiting dates, and by searching for the word 'quantum' in article titles or abstracts.

[2] For example, *Quantum* (2017), *Quantum Science and Technology* (2016), *Advanced Quantum Technologies* (2021), *Quantum Information Processing* (2004), *npj Quantum Information* (2015), and *IEEE Transactions on Quantum Engineering* (2020).

which quantum technologies arose, such as physics, chemistry, engineering, mathematics, and computer science. In its *Strategy for the Quantum Revolution* (2021), the Australian Strategic Policy Institute suggested we are less than 5 years from quantum sensors, less than 10 years from quantum-focused finance, global positioning systems, and quantum clouds, and less than 15 years from wide-range quantum communications and consumer-based sensors (Brennan et al., 2021). Just 3 years later, in 2024, quantum sensors had been commercialized (Huntley 2024; Muradoglu et al., 2025).

Multiple governments fund quantum research. In the National Quantum Initiative Act (NQIA) of late 2018, the USA created a National Quantum Initiative and funded a Quantum Leap Challenge. In the FY2019 and FY2020 National Defence Authorization Acts, new funding was created for quantum-focused national defences. In 2022, the 2018 NQIA was amended to include QIS within the National Science Foundation, to create standards, to integrate quantum into education, and to fund research (National Quantum Institute 2025). In 2018, the European Union (EU) launched a €1 billion budget for its Quantum Technology Flagship to fund research. Other countries with quantum strategies include Australia (Government of Australia 2023), Canada (Government of Canada 2023), China (Quantum Insider 2023), India (Government of India 2023), Japan (Government of Japan 2023), and South Korea (Republic of Korea 2023), among others.

Sections two and three of this article descriptively explain quantum mechanics for a social science audience, along with the quantum challenge to cybersecurity and national security. The foundations of quantum computing are dissimilar to the classical computers used in modern e-government, e-service delivery, digital governance, artificial intelligence, big data, and more. This is a major technological shift that must be understood by non-quantum ICT scholars in public policy. For nearly six decades, the foundation of ICT policymaking was based on the hardware and software of classical computers. Quantum computers are fundamentally different from classical computers in multiple ways, making their impact far greater upon current digital systems. Given the committed roadmaps of major quantum vendors (Swayne 2025), the time is fast approaching for sustained public policy conversations.

This leads to section 4, where we engage the quantum era's 'two-headed problem' for public policy scholars. The first heading is an expectation that fault-tolerant quantum computers will create cybersecurity and national security challenges for public policy (e.g. Adams 2019; Lindsay 2020). The second heading is how quantum computers may impact sectors such as health, finance, transportation, renewable energy, agriculture, manufacturing, telecommunications, and supply chain logistics (e.g. Wright 2017; Orús et al., 2019; Bova et al., 2021; Giani and Eldredge 2021; Cooper 2022; Phillipson 2023, 2024; Rasool et al., 2023; Chen et al., 2024; Maraveas et al., 2024). Both headings fit the definition of a 'wicked' policy problem (Newman and Head 2017). In addition, the first heading, by definition, is a partially unstructured policy problem while the second matches the definition of a wholly unstructured policy problem (Peters 2018: 55). In sections 5 and 6, each claim is defended via examples situated in the agenda-setting and policy formulation steps of the public policy cycle (Knill and Tosun 2008; Howlett 2023). The article concludes by suggesting the implications for theory along with four risks on the quantum horizon.

2. Quantum explained

In one of the very few public policy articles to discuss quantum theory, Overman (1996: 490) wrote that 'gone is the expectation of objective reality, certainty, and simple causality. In its place are intersubjectivity, uncertainty, context, many works and many minds, nonlocal causes, and participatory collusion.' In many ways, he was right. It is a science initially born to explain strange behaviours that classical physics could not explain. It deviates from the classical theories of Isaac Newton and his expectations of objectivity, independence, certainty, and causality.

Quantum mechanics created a profound shift in the early twentieth-century developments within physics. This began with Max Planck's observation of a phenomenon called the ultraviolet catastrophe that was unexplainable by the classical physics of that time. This was later followed by Albert Einstein's explanation of another phenomenon called the 'photoelectric effect' in which theoretical predictions did not match experimental results. Einstein's explanation of this phenomenon established the foundation of a new type of physics that would later be called quantum mechanics. Quantum mechanics gained steam via the work of Erwin Schrödinger, Niels Bohr, Paul Dirac, Wolfgang Pauli, Werner Heisenberg and Max Born. In 1980, physicist Paul Benioff coined the term 'quantum computer' and showed how quantum systems could simulate the operation of classical computers. In the early to mid-1980s, Richard Feynman and David Deutsch expanded the idea into quantum computation, which was quickly followed by the development of important quantum algorithms in 1994 and in 1996 (Shor's algorithm, Grover's algorithm). Since the mid-1990s, quantum computing has migrated from the desks of theoretical physicists and into the labs of experimentalists and engineers.

Specific to quantum computation, two quantum mechanical phenomena anchor analysis. The first is superposition, which is the ability of a quantum particle to exist in multiple states until it is measured, which forces it to collapse to one state. However, measurement in quantum mechanics is a probabilistic process. We can measure the size of an apple today and the same apple tomorrow to discover that the apple's measurement has not changed. But it is not the same if we replace the apple with a quantum particle. In that case, measurement would return a random value. Its measurement cannot be fixed as there is 'no categorical distinction between the observer and the observing apparatus' (Taylor 2020: 3). This contrasts with classical computing[3] and how its bits (of binary digits of 0 or 1) combine to create bytes, kilobytes, megabytes, gigabytes, and terabytes. The digits represent the electrical signals of 'on' and 'off'. The bit is the fundamental unit of computation in classical computing. For quantum computers, qubits are the fundamental unit. Like bits, qubits can be 0 or 1. However, unlike bits, qubits can also be in a superposition state of both 0 and 1 at the same time. The second phenomenon is quantum entanglement. If two particles are entangled, the measurement of one instantaneously influences the other regardless of the distance between the two. Using the apple example, the equivalent would be to

[3] 'Classical computing' refers to today's conventional computers, which largely use transistors. E- governance, digital technology, blockchain, internet of things, virtual reality, artificial intelligence, and more use classical computers. Quantum computers are an altogether new computing device based on quantum mechanics.

assume that the measurement of one apple will influence the measurement of another apple, even if the two are separated by long distances. This is untrue for classical physics, but it is a reality for quantum mechanics.

Quantum computers[4] have the potential to rapidly solve today's most challenging problems in mathematics and science. Unlike a classical computer, the capacity of which increases linearly as more transistors are added, quantum capacity increases exponentially with the number of qubits. Problems that require thousands of years to solve using today's advanced classical computers can potentially be solved in minutes or hours by a quantum computer, depending upon the problem, qubit capacity, and gate fidelity. It is superposition, entanglement, and the other unique quantum properties that give quantum processers their power. Given qubit fragility and the ease with which quantum systems can be altered by their environment (aka quantum decoherence[5]), research is underway to create quantum error correction codes for 'fault-tolerant' qubits, which will pave the way for the rise of 'fault-tolerant quantum computers'. To increase quantum computer effectiveness, scientists are seeking improvements in quantum sizes (number of qubits), quantum coherence (how long a qubit can hold its state), quantum volumes (size of a circuits reliability), and quantum speeds.[6] Nonetheless, error rates remain high. The 'holy grail for technology is to achieve large, highly controlled, coherent, analog or digital quantum computers' (Bova et al., 2021: 2). Continued effectiveness improvements will supercharge our quantum era.

3. Quantum advantage, national security, and cybersecurity

Coined in 2012 and later described as 'two little words that could change the world' (Roush 2020; Preskill 2012), 'quantum supremacy' occurs when a quantum computer completes calculations beyond the reach of a classical computer (Krelina 2021). Since Google first announced quantum supremacy in October 2019 via its 54-qubit processor, the qubit processing size has expanded. In November 2022, IBM showcased a 433-qubit processor (IBM 2022). Seven months later, in May 2023, IBM used the meeting of the G7 Heads of State in Japan to announce its intention to build a 100,000-qubit processor within 10 years (Brooks 2023). As of the time of writing (September 2025), IBM's largest quantum chip, Condor, houses 1,121 qubits (Castelvecchi 2023). Given that qubit capacity grows exponentially, even a 300-qubit processor, assuming reductions in the error rate, could efficiently 'conduct more calculations than there are atoms in the universe' (Herman and Friedson 2018: 3). Given that a human body has an already hard-to-imagine 7×10^{27} atoms, it is even more difficult to comprehend the number of atoms in the universe with billions of observable galaxies (Howell and Harvey 2022; American Museum of Natural History 2024).

Such developments have led to an encryption (and decryption) race for quantum advantage. As noted by the World Economic Forum, 'Quantum computing could make today's cybersecurity obsolete' (Adams 2019). Cryptography protects government and corporate data, along with the data of citizens, consumers, and community groups. Cybersecurity for classical computers relies on encryption via asymmetric (or public key) cryptography. Public key cryptography involves a private key (via RSA)[7] consisting of two large prime numbers known only to the securing party (e.g. companies for medical records, banks, credit cards), while the public key is a single large number produced by multiplying the two private key numbers. Hackers often cannot obtain encrypted information on classical computers secured with public key infrastructure (PKI)[8] as breaking this system would require solving very hard mathematical problems, such as finding the prime factors of large numbers (often more than 2,000 digits long), which is considered infeasible.

As noted by Lindsay (2020: 346) in *Security Studies*, PKI 'importance . . . cannot be overemphasized'. Unlike classical computers, which can only search for a key sequentially, quantum processors make use of a special quantum mechanical property called 'superposition', which allows it to explore multiple possible solutions to a given problem at almost the same time. At present, PKI is used in national defence, secure communications for intelligence, a myriad of government, non-government, corporate, and consumer databases, virtual private networks, banking and financial transactions, medical records, and more. PKI usage helps to secure personal computers and smartphones along with their applications, emails, texts, and documents. The development of quantum-safe cryptography is a public policy priority and thus, first movers have substantial advantage. In the *en*cryption race, first movers can use public-safe cryptography to secure processes and their data. In the *de*cryption race, first movers could potentially read unprotected communications that are typically assumed secure by PKI.

The so-called Q Day is when quantum computers can break the mathematical problems that are the basis of today's cryptographic algorithms and thus (almost completely) break current cybersecurity. There is no consensus on when Q-Day will arrive, but some predictions position it only a few years ahead (Lohrmann 2023; Sridhan 2024). From local to national governments and from the private to the public sector, the citizen, consumer, corporate, and government data that informs modern policy and its administration are at risk. It is a claim that is repeated among cybersecurity and national security scholars (e.g. Adams 2019; Lindsay 2020; Taylor 2020; Gorbanyov et al., 2021).

According to the US National Institute of Standards and Technology (NIST), the current global cybersecurity standard (RSA 2048 bits) has a 'security-strength time frame' of 2030 (Barker 2016: 55). While a 'typical desktop computer would need over six quadrillion years to crack an RSA 2048 key' (Lindsay 2020: 346), a large enough quantum processor could quickly break RSA-2048 encryption (Krelina 2021). Recently, it was suggested that a quantum computer with 1,000,000 qubits and an error rate of less than 0.1% could break RSA

[4] Digital quantum (gate-level) computers are universal programmable computers. An analogue quantum computer (annealing) has limited qubit connectivity. The first is limited by resources to control its decoherence noise, while the second is limited by difficult-to-control noise. A quantum simulator is a single-purpose machine to simulate quantum systems (Krelina 2021: 5–6).

[5] Decoherence is when a prior quantum state can no longer be used.

[6] Scientists are experimenting with different platforms where trapped ions, photons, atoms, topological qubits, and superconducting are used to realize qubits.

[7] RSA is a popular public-key cryptography algorithm based on the hardness of factoring large numbers.

[8] PKI is a system that manages public-key cryptography, mainly to ensure secure handling and distribution of encryption keys.

2048 in under a week (Gidney 2025). This is not only a present-day concern. Historically protected information may also be retroactively accessed via quantum processors (Gorbanyov et al., 2021; Csenkey and Bindel 2023). As such, the NIST currently suggests encryption strengths based on the type of data and its security life. The most cost-effective and straightforward way to address this problem is to find new (hard) mathematical problems that are not susceptible by Shor's algorithm.[9] In 2022, the NIST promised to release its first standards for postquantum cryptography in 2024 (NIST 2022) and in August 2024, the NIST did release its first three postquantum encryption standards (NIST 2024). We expect to see another standard released in 2025, and at least three more algorithm candidates advancing to a subsequent evaluation phase that may lead to future standardization.

4. Public policy in a quantum era: wicked and partially unstructured

We have split the quantum-era challenge for policymakers into two headings. The first heading is its cybersecurity and national security challenges, while the second heading is other policy sectors. We acknowledge the oddness of a second category that includes multiple sectors. However, given limited policy-specific scholarship on the quantum era (and even less on the public policy implications of each sector), we start with the basics. This includes our observation that both headings of the quantum era are 'wicked' policy problems.

A wicked problem is a 'social situation where: (1) there is no obvious solution; (2) many individuals and organizations are necessarily involved; (3) there is disagreement among stakeholders; and (4) where desired behaviour changes are part of the solution' (Ferlie et al. 2011: 308; Rittel and Webber 1973). To be labelled 'wicked', the policy problem must have three traits: complexity, uncertainty, and disagreement (Head 2022). As shown in Table 1, the cybersecurity and national security heading is complex (multiple moving parts, negative externalities), is plagued by uncertainty (helpful information is finite, uncertain impacts, changing stakeholders), and has stakeholder disagreements (Newman and Head 2017). It is particularly wicked for the non-cyber and non-national security sectors as published sector-specific policy discussions and related scholarship are even more limited.

In addition to its 'wickedness', the quantum era is a largely unstructured policy challenge (see Table 1). For cybersecurity and national security, the policy task is partially unstructured. This is because its causalities are clear (cryptography backbone) and there are value agreements on how to respond (constantly refine QKD). However, it is hampered via disagreements on legal–regulatory responses. This includes whether quantum-focused discussions should be global or only among like-minded countries and how to consider dual-use technology. Each has multiple uncertain policy options (Peters 2018: 55; Hisschemöller and Hoppe 1995).

For the second heading of all other policy sectors, the policy problems are even more unclear, unstructured, and wicked. For scholars seeking a rationalist approach to policy design, considerations of the 'other policy sectors' section may appear axiomatic given potentially adjacent policy relationships to prior computing, internet, and digital divide discussions (e.g. McCrohan 1989; Halachmi and Greiling 2013; Owen et al. 2013; Moloney et al., 2026). One challenge is that we do not know whether 'quantum governance is *sui generis*' or if its governance system will be similar to prior technologies (Perrier 2022: 4). It is likely that several concepts and theories specific to ICT public policy scholarship will apply to the quantum era. However, our location of deviation (and where a *sui generis* label may fit) is anchored on the processing speeds of quantum computers when compared to their classical counterpart. This may require an enhanced deliberative speed by policymakers to consider which regulatory guardrails are required for such generational developments.

In situations where there is policy wickedness and a partially unstructured policy problem, Hoppe (2018: 385) encouraged scholars to answer the following question: 'What is the policy designer's task?' Our answer is shared via the first two steps of the policy cycle. The policy cycle helps policymakers understand the 'complexity of decision-making processes, as well as the actors involved in such processes' (Valle-Cruz et al., 2020: 4). It has been used by ICT scholars of public policy in relation to artificial intelligence, big data, cryptocurrency, and e-participation (Coelho et al., 2017; Pencheva et al., 2020; Valle-Cruz et al., 2020). We focus exclusively on the agenda-setting and policy formulation stages of the policy cycle specific to quantum computing.

The agenda-setting stage is rarely 'all issues' but instead 'a limited number of issues or problems to which attention is devoted by policy elites' (Howlett 2023: 38). The identified issues may originate from political, epistemological, and ideological factors, along with societal-level socioeconomic problems. Agenda setting is socially constructed and may occur despite definition ambiguities and shifting political and policy preferences (Kingdon 1984). It may also be characterized as an effort by governments to 'control or attempt to control issue prominence and agenda-entry patterns in an effort to manage or direct their own policy timetables and agendas' (Shivaoki and Howlett 2022: 113).

The second stage, policy formulation, is when 'a range of available options is considered and then reduced to some set that relevant policy actors, especially in government, can agree may be usefully employed to address a policy issue' (Howlett and Mukherjee 2017: 6). It includes tasks such as problem characterization, objective specification, options assessment, and policy design (Turnpenny et al., 2015). The policy formulation step comes after the agenda-setting step of the policy cycle and before the decision-making, implementation, and evaluation steps. Policy formulation is focused on the 'what' and 'how' of policy design, with most scholars largely focused on which policy instruments or policy tools are needed. The five categories of tools are nodal tools, authority tools, treasure tools, organizational tools, and procedural tools (Howlett 2019; Bali et al., 2021). Given the still-early stage of quantum policy development, we focus on authority tools.

Before proceeding, two observations are required. The first is that both headings of the quantum era are challenges hampered by limited quantum literacy among scholars and policymakers (Moloney et al., 2026). While there may be higher quantum literacy within the cybersecurity and national security sectors than in other policy sectors, the outputs are information asymmetries and increased power distance among and between stakeholders and thus, more complicated consultation processes. This limits our ability to create

[9] Shor's algorithm breaks today's cryptography by attacking its underlying mathematical problems. However, when we change these mathematical problems, Shor's algorithm becomes ineffective.

Table 1. Quantum era policy: wickedness and problem structure.

		Cybersecurity and national security	All other policy sectors
Wicked policy problem?	Policy is complex?	Yes, the problem is defined but there are multiple moving parts and multiple negative externalities.	Yes, the problem remains largely undefined as sector-specific particularities are underexplored.
	Policy is plagued by uncertainty?	Yes, fast-paced quantum-era developments with still-unknown policy ramifications	
	Policy has stakeholder disagreements?	Yes, stakeholder categories are increasingly clear but conversations are infrequent, haphazard, and not global.	
Unstructured policy problem?	Policy causality?	Yes, clear risks of not updating cybersecurity and being unaware of national security developments	Yes, the problem remains largely undefined as sector-specific particularities are underexplored.
	Policy values?	Partially as uneven discussions among and within states and non-state actors; NIST dominance as global cybersecurity standard-setter	
	Policy options?	Partially, as unclear legal–regulatory responses at national and global level	

Note: Authors' adaptation from Peters (2018), Hisschemöller and Hoppe (1995), and Newman and Head (2017).

appropriate policy guidance (Aiello et al., 2021; Kong et al., 2022; Seskir et al. 2023).

Due to the speed of quantum-era developments and the concurrent speeds of quantum processors, there may be a shortening of quantum-relevant policy timelines between policy consideration and its implementation when compared to the prior several-decade timelines between the introduction of classical computers, their integration into government life, their role in consumer life, and developments related to e-government, digital governance, and artificial intelligence. Given the current inconsistencies among governments at all levels to understand, to regulate inappropriate use, and to stay ahead of simpler AI-related developments (e.g. Fenwick et al., 2016; Nzobonimpa and Savard 2023; Hartung et al., 2025), our concerns may be amplified for the quantum computing area.

The second observation is to recall differences between classical and quantum computers and the outputs of such differences. The first output is that we do not expect quantum computers to replace the classical computers used for everyday government analysis and policymaking, at least in the foreseeable future. Both computing devices will co-exist and complement each other. Daily government life will continue to function with classical computers, with quantum computers being dedicated for special tasks that classical computers cannot perform efficiently. Quantum processors are not required to handle current artificial intelligence tasks, internet of things systems, and the big data calculations common to the public sector (Wirtz et al. 2019). Nonetheless, even if a policymaker is unlikely to have a desktop quantum computer, they will need to be quantum literate to interact with quantum technology and its societal impacts.

The second output is that quantum processors will be capable of crunching specific types of mathematical problems far beyond the reach of the world's faster supercomputers. This computational advantage is already leading to shifts in how experiments are designed and interpreted in the basic sciences. It is also disruptive as quantum computers are expected to 'shatter computational times by accomplishing tasks at an exponential pace compared to their classical counterparts' (Purohit et al., 2024: 2). Such exponential pacing and a likely increased discovery speed may alter the traditional and deliberative pacing of a responsive policymaking. The deliberative pacing of public policy design may be appropriate for a classical computing era but may be less amenable for the quantum era.

5. Cybersecurity and national security: agenda setting and policy formulation

Specific to cybersecurity and national security, the agenda-setting stage includes three largely agreed upon agenda items: quantum-safe encryption, the limited nature and scope of supranational discussions, and whether quantum is a dual-use technology. The following paragraphs discuss each agenda item jointly with the policy formulation step. To start, there is an agreement among scholars that the cybersecurity and national security challenges of the quantum era cannot be overlooked (e.g. Tigges et al., 2003; Stix 2005; Bernstein and Lange 2017; Raheman 2022). As the global leader in cybersecurity standards, the US-based NIST publicly released three quantum-safe algorithms in 2024 (NIST 2024). The risks may increase among second-mover countries as well as underprepared corporate entities, and they are even higher for countries with limited to no quantum engagements (Moloney et al., 2026).

Unlike ongoing artificial intelligence discussions at the global level (e.g. United Nations 2023; Zaidan and Ibrahim 2024), quantum multilateralism remains 'nascent' (Open Quantum Institute 2024: 5). Despite UNESCO's labelling of 2025 as the International Year of Quantum Science and Technology, the United Nations' first-ever Global Digital Pact does not mention quantum technology (United Nations 2024). To date, the first significant global collaborative effort relates to technical issues, via the International Standardization Organization's creation of a technical committee on quantum technology in early 2024. Co-created with the International Electrotechnical Commission, its goal is a 'coordinated international approach' (International Standardization Organization 2024) to standardization specific to the quantum era. The second is the early Concept Notes written by UNESCO for potential discussions of the quantum era and ethics (UNESCO 2024). To date, there are

limited global agreements to set an agenda and even less agreement on policy formulation.

Moreover, and instead of global discussions, there are growing preferences for 'closed groups emerging among like-minded countries' (Open Quantum Institute 2024: 6). For like-minded groups, an invitation to join is built on allyship, trust, and certain within-group accountabilities. The risks include creating quantum haves and have nots and separately, more reasons for an acceleration of distrust among states. If the fear of a zero-sum race overwhelms the ability to set a global agenda, globally oriented policy formulation may not occur.

The above may lead to other legal responses by states. This includes whether quantum developments are dual-use and thus, the technology becomes a policy agenda item that also has national security implications (Johnson 2019). 'Dual use' means that a technology has military and civilian uses. It also comprises questions about whether a policy tool such as export controls should be considered in the policy formulation step. In 2016, the EU published a Quantum Manifesto, with more than 3,400 endorsing parties. Its goal was to create a quantum flagship for the EU. But when the EU's €1 billion Quantum Technology flagship was announced 2 years later in 2018, its 2030 roadmap used the label of 'international collaboration / export control regulation' to limit any non-EU partnerships to tasks of standardization (Gercek and Seskir 2025).

This matters for global research and development and the creation of (or limitation of) cross-national quantum divides (Ten Holter et al., 2022; Moloney et al., 2026). For example, quantum sensors have a civilian purpose, such as aiding in earthquake and volcano prediction (Parker 2021), while also having warfare applications (Krelina 2021). Specific to the policy tool of export controls, the Wassenaar Arrangement (1995) is a transgovernmental arrangement among 42 states in which participating states agree to export controls on certain munitions and exchange information on nine categories of dual-use goods and technologies among other activities (Wassenaar Secretariat 2025). With calls for the Agreement to consider the quantum era (Seskir et al., 2023), the dual-use potential of quantum developments, an increased use of quantum-specific export controls, and global discussion fragmentation may continue.

6. Other policy sectors: agenda setting and policy formulation

In recent years, scholars have considered quantum computing implications for sectors such as health, finance, transportation, renewable energy, agriculture, advanced manufacturing, telecommunications, and supply chain logistics (e.g. Wright 2017; Orús et al., 2019; Bova et al., 2021; Giani and Eldredge 2021; Cooper 2022; Phillipson 2023, 2024; Rasool et al., 2023; Chen et al., 2024; Ho et al., 2024; Maraveas et al., 2024). This is not the population of policy sectors but instead sectors with multiple published articles that consider sector-specific quantum computing applications (Table 2). As with developments in quantum computing (in general) along with the cybersecurity and national security sectors, such conversations are occurring outside of the journals specific to the public policy discipline as well as outside of ICT-specific policy journals. Similar to cybersecurity and national security, quantum computers are a wicked policy problem for each of the above-mentioned sectors. However, unlike the cybersecurity and national security sectors, the policy problem in each of the above sectors remains largely unstructured (see Table 1).

Quantum computers will provide increased computational power and processing speeds that should lead to sector optimizations via machine learning and other techniques. Concerns in the sector-specific literature include security and cryptography, scalability, access to quantum computers in general and in relation to quantum networks, quantum clouds, and specialized sensors along with a need for sector-specific algorithms. Other concerns include ongoing data bias (e.g. bad data in, bad data out), an altering of traditional practices and knowledge, and a potential overdependency on technology. Given the link among AI, machine learning, and quantum computing, AI-specific risks such as malicious use, rogue AIs, AI races, and organizational risks (Hendrycks et al., 2023) may be amplified in the quantum era.

Key to policymaker responses is their improved quantum literacy. This literacy may encourage a 'general quantum readiness' separate from the 'quantum cyber readiness' specific to cybersecurity and national security sectors (Coates and Chhetri 2024: 62). This leads to our focus on four aspects of the agenda-setting step (consultation with stakeholders, public goods, public values, and the precautionary principle) and two aspects of the policy formulation step (responsible innovation and authority tools). Future researchers may wish to accentuate other aspects in each stage.

6.1 Agenda-setting step

One of the first agenda-setting steps is to identify stakeholders. Coalescing the work of others, Umbrello et al. (2024) identified eighteen potential quantum-interested stakeholder groups: governments (in general) and regulators (specifically), legislative arenas, academics/universities, international organizations, corporations, investors, civil society, technical/professional/scientific associations, student groups, ethics experts, media and journalism, museums, K-12 schools, municipalities and local communities, individual developers, individual consumers, and individual citizens.

Given the policy complexities in a quantum era, it has been argued that 'for a societal debate to be effective, stakeholders need to have a reasonable understanding of the technologies in question' (Vermaas 2017; Umbrello et al., 2024: 7). This includes stakeholder awareness of its public good implications, for understanding responsible innovation, and for quantum literacy (Roberson et al., 2021; Wolbring 2022; Ten Holter et al., 2023). Or, as noted by a *Nature* editorial in 2017, there is also a need to limit one-directional communications from science to the public and to understand 'the needs and employment prospects of taxpayers who have seen little benefit from scientific advances' (Editors 2017: 391).

Initial agenda-setters may have more power to exclude, to increase power differentials between the involved and noninvolved, and to increase their policy monopoly power. This means that good agenda setting also requires an effort to solicit other views. One of the first surveys of a broader public was conducted in 2017 by the UK's Engineering and Physical Sciences Research Council. They found 'wide familiarity with the word "quantum"' but limited understanding of the word or its implications, yet once exposed to more background, participants became 'excited by the range of potential benefits' while raising concerns about who controls development and access along with concerns about its environmental

Table 2. Expected policy sector opportunities.

Policy sector	Sector examples
Agriculture	Improved smart agriculture and precision agriculture, improved robotics in agriculture, improve optimization models for pests/fertilizer/irrigation/water quality, modelling of soil/weather/crop data, greenhouse engineering, plant optimization, crop harvesters with precision sorting, microclimate modelling for greenhouses/vertical farming, crossbreeding/genomics, satellite tech for decision-making
Banking and finance	More comprehensive sector-wide modelling and economic forecasting; improved asset optimization, risk and return predictions, trading strategies, arbitrage opportunities, credit scoring, derivatives pricing
Healthcare	Improved diagnostic speeds, diagnostics via omic datasets, drug research and discovery, price optimization, improved patience adherence, pricing optimization
Manufacturing	Assess manufacturing errors/failure when processes have thousands of steps, reduce downtime, improve efficiency, limit asset turnover. Specific to materials manufacturing, opportunities for atom-specific analysis, chemical pathways, and improved materials science. This includes additive manufacturing techniques for self-sensing technology
Renewable energy	Improved battery chemistries, solar cells, forecasting for wind/solar and hydrodynamic fluctuations, supply and demand modelling, system robustness measures, optimal power flows
Supply chain logistics	Improved optimization in routing, scheduling management (production, job, workforce), network design, cargo loads, fleet optimization, and travelling salesman problem
Sustainability	Improved simulations for energy generation, carbon capture, nuclear energy, and renewables; improved disaster prevention, waste management, and food management
Telecom	Improved planning and operation of networks (radio, wireless, fixed), improved optimization for 6G and beyond, predictive maintenance models, identifying anomalous network behaviours, improved routing and frequency assignments, and power optimization
Transportation	Optimization (travelling salesman problem, bin packing problem), multiobjective routing, improved aggregation of individual behavioural models

Source: Authors' compilation from Bova et al. (2021), Chen et al. (2024), Cooper (2022), Giani and Eldredge (2021), Ho et al. (2024), Maraveas et al. (2024), Orús et al. (2019), Phillipson (2023), Phillipson (2024), Rasool et al. (2023), and Wright (2017).

impact, potential defensive arms races, quantum misuse, and automation-induced job losses (Busby et al., 2017). More recently, Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO) conducted stakeholder surveys on quantum readiness (Coates and Chhetri 2024) and the EU published a survey on public views in relation to the quantum era (European Union 2025).

Another aspect of good agenda setting is understanding public good involvement. The economic definition of a public good focuses on its nonexcludability and nonrivalrous nature. But as Roberson et al. (2021: 4) suggested, this definition 'can too easily slide into a utilitarian focus on the "greater good" in absence of adequate attention to who might be harmed or how'. This led the authors to draft a broader definition drawn from a Callon (1994) question on what is 'in the public good' and 'how it is to be achieved' (Roberson et al., 2021: 4). Their public good 'test' includes 'how research problems are framed', 'the social and institutional arrangements in which research outcomes are expected to unfold and to be used' and 'cultivating diversity of networks between scientists, stakeholders, and research' (Roberson et al., 2021: 4). It should not implicitly assume that all science is good, it should include nonhyped and context-relevant societal benefits, and it should seek relationships between the 'science–industry complex' and citizens. It should also require governments to ensure equity of access to quantum computers so they are 'not restricted to deep-pocketed corporations' and, thus, are less likely to be 'subsumed into technology arms races' (Inglesant et al., 2021; Ten Holter et al., 2023: 853).

The expansion of the public good discussions has a relationship to public values discussions. Public values are the principles upon which good policy is made (Bozeman 2007). This is especially important for disruptive technologies (Bannister and Connolly 2014) in which governments are often managing two paradoxes. The first paradox is how to balance individual rights with a societal agreement to create and enforce contracts and the second paradox is how to use governmental powers to protect individuals while not overlooking 'public concerns and conditions' (Moore 2014: 467; see also Bozeman 2007). The public values identified by earlier ICT scholarship may also apply to the quantum era. As such, policy agenda-setters may wish to include economic values (e.g. efficiency, economy) and noneconomic public values. Noneconomic values include fairness, equity, trust, inclusion, stewardship, accountability, transparency, openness, participation, collaboration, and more (Harrison et al., 2011; Bannister and Connolly 2014; Twizeyimana and Andersson 2019). To date, ICT policy scholars have studied the link between public values and e-government (Twizeyimana and Andersson 2019), open government objectives (Cresswell et al., 2006), digital transformation (Zyzak et al., 2024), the digital economy (Chohan 2021), and blockchain adoption (Rodriguez Müller et al., 2025).

In its Concept Note for a newly created Ethics of Quantum Computing Commission, UNESCO suggested that 'ethical guardrails should be based on individual dignity and autonomy … ensuring democratic accountability … and ensuring that quantum computing software and hardware and the underlying processes, are understood as a global public good and governed with a view to ensuring and enhancing international solidarity and intergenerational equity' (UNESCO 2024: 4). The importance of public values was noted by *Nature* in 2017 when its editors warned readers that the 'benefits of discovery science arguably deepen the pools of wealth and privilege already in place' (Editors 2017: 391). Given that quantum developments may occur more quickly than the deliberative pace of public policy creation, public value discussions may require additional emphases at the agenda-setting stage.

Another agenda-setting consideration is the precautionary principle. This principle suggests policymakers may engage in risk avoidance when there are 'weakly understood causes of

potentially catastrophic or irreversible events, or threats of harm to human life, property, and/or well-being' (Ricci and Sheng 2013). The range of what is or is not a precautionary action can include requirements for 'absolute proof of safety before allowing new technologies to be adopted' to lesser requirements (Foster et al., 2000: 979). The principle asks policymakers to consider when (1) the principle is arbitrary, burdensome, and innovation-limiting and thus, policymakers should consider lighter touches, and specific to the quantum era (2) how to balance between a narrow focus on cybersecurity and national security and other sector policy considerations.

Specific to AI and the precautionary principle, a one-sentence statement was released by the Center for AI Safety in May 2023. Signed by more than 600 AI leaders, the statement suggested that 'mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks, such as pandemics and nuclear war' (Center for AI Safety 2023). Earlier in 2018, the EU released its own Statement on Artificial Intelligence, Robotics, and 'Autonomous' Systems. While such AI-focused statements did not engage quantum-specific risks, one particular observation deserves a mention. The EU commented that the actions of AI '... are no longer programmed by humans in a linear manner ... In this sense, their actions are often no longer intelligible, and no longer open to scrutiny by humans (European Union 2018: 6). Since today's AI is generally limited by current computational resources, the lack of intelligibility (aka 'explainable AI') may be exacerbated when AI uses even more powerful computing infrastructures such as quantum computers. The enhanced processing speed of quantum computers, when combined with unintelligible AI, may lead to further nontransparency (and at speed) for policymakers. This includes already raised concerns about AI applications to a nonlinear quantum world (Taylor 2020) as well as recently developed hybrid quantum algorithms that mix classical routes with quantum ones, can be run on 'near term quantum hardware', and are expected to eventually outperform classical algorithms (Suchara et al., 2018: 1).

6.2 Policy formulation step

Among the limited scholarship in the broader social sciences specific to the quantum era, responsible innovation (RI) is a frequent mention (e.g. Inglesant et al., 2021; Ten Holter et al., 2023). RI is a 'transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in society)' (Von Schomberg 2013: 63). The simplest way to understand RI is to learn what RI is not. It is not the belief that all technology advances are inherently good, it is not a neglect of ethical principles, it is not the immediate implementation of new technology, and it is not giving insufficient attention to precautionary principles.

We placed RI in the policy formulation stage given a Kop et al. (2024) two-part RI framework in which the authors observed that responsible quantum technology requires social, legal, and policy layers (long term), ethical layers (medium term), and technical layers (short term). 'Long term', 'medium term', and 'short term' refer to time from technology creation. Each is an aspect of policy formulation and the policy tools that may be selected. RI in quantum technology requires policymakers to formulate policies that encourage societal benefit. This includes questioning whether the privacy concerns arising from generative AI, predictive AI, and adaptive AI (three subsets of narrow AI) research (e.g. Manheim and Kaplan 2019) are enhanced or hindered. Given a quantum processing capacity to handle ever more data at greater speeds, narrow AI is the least worrisome of the three AI categories. Instead, given already-current movements towards artificial general intelligence (McLean et al., 2023; Tschirhart and Stockton 2025) and into the future a potential artificial superintelligence, the capabilities of quantum computers may take society into generational developments ahead of our ability to formulate appropriate policies.

One common ICT challenge for policymakers is to find a balance between encouraging research and development and the necessity of regulating technological outputs to preserve the public good. In the quantum arena, some have suggested that self-regulation and multistakeholder initiatives may be sufficient to protect human rights concerns (Krishnamurthy 2022). Others have asked whether 'regulation is difficult until technology becomes more developed, widely disseminated and its impact is known, yet by that time, regulation can become difficult' (Perrier 2022: 4). This leads to questions on whether hard law (treaties, legislation, regulation) or soft law (principles, standards, codes, guidelines) should be preferred (Johnson 2019; Perrier 2022). The challenge in answering such questions arises from insufficient clarity on whether 'quantum governance is *sui generis*' (Perrier 2022; 4). Moreover, with less intelligibility and less open scrutiny, quantum processing powers may accentuate divides between a private actor's ability to quickly innovate and the often slower ability of policy formulators to deliberate and create public policy. This is in addition to our current and already underdeveloped regulatory landscape for simpler developments such as AI and blockchain (Dekker and Martin-Bariteau 2023).

It remains unclear which policy tool mix for quantum governance will balance the public and private interests. Taylor (2020: 9) suggested that the 'likely approach' is to address applications of QC (quantum computing) and QAI (quantum artificial intelligence) on a case-by-case basis, through a combination of technical standards, licensing, regulation, taxation, R&D funding, antitrust law, intellectual property law, tort law, import–export controls. Excluding the treasure and financial tools of taxation and R&D funding, the rest of Taylor's (2020) suggestions are authority-focused policy tools (see also Perrier 2022). It is possible that studies focused on identifying ICT-specific tools for digital transformation (Waller and Weerakkody 2016) may also have value for the quantum era, but further research is needed.

7. In conclusion: theory and risks on the horizon

Quantum computing has moved from the desks of physicists to the labs of engineers and computer scientists. Each newly predicted application of the quantum era may reshape public policies and societal expectations. In our conclusion, we suggest a theoretical question for future researchers as well as four potential risks of the quantum era.

On the theory side, future scholars may wish to investigate whether already-developed models of e-government and digital governance apply to quantum technologies or if

modifications are required. This includes digital governance and e-government models such as the issue–actor–mechanism model, technological acceptance model, organizational capability models, and models of digital progression (e.g. Coursey and Norris 2008; Nasution and Mavondo 2008; Jia and Chen 2022). It includes re-evaluating the Dunleavy et al. (2006: 467) claim that prior eras are 'dead' and thus, 'long live digital-era governance'. This is especially true if the digital era becomes partially or fully replaced by a quantum governance built not via the deterministic realities of classical computers but instead, the probabilistic backbone of quantum processors.

One future policy risk is the potential development of 'policy monopolies' within countries, among transnational coalitions of like-minded states and/or cooperating corporations. Policy monopolies can create institutional stability (Baumgartner and Jones 1993) and may be encouraged by limited quantum expertise. The institutional members of a monopoly may derive data gathering, analyses, and profits away from citizens and/or governmental oversight. In a speech in April 2025, Mark Pritchard (MP, UK) noted, 'The necessary and close relationship between Big Tech and governments is understandable, but it is, I would suggest, nonetheless conflicted,' and thus, he called for smart regulation, a need for governments to distinguish between benign tech and its 'darker elements', and 'recalibration' of the government and Big Tech relationship. He also shared another worry: 'If the relationship between government and Big Tech is conflicted, is it also compromised,' and if this compromise equates 'to a type of corporate kompromat ... and an overreliance ... on Big Tech by governments [that] paradoxically, and over time ... might prove a strategic risk to those governments' (Global Security Forum 2025). Despite his focus on a nonspecific 'Big Tech', his comments are extendable to a quantum era.

The second risk is that newly formulated policies infrequently lead to immediate, complete, and global implementation. Given NIST expectations that quantum-resistant algorithm standards will require a 'rollout to space out for another five to fifteen years' (Herman 2021), it is reasonable to suggest that we will need even longer time frames to implement quantum-safe cryptography in every sector of every country. The bases for this claim are prior (and ongoing) delays in implementing prequantum cryptographic infrastructure (Menezes and Stebila 2021; Joseph et al., 2022). In addition, given delays in conceptualizing and implementing AI-focused regulation (Mergel et al., 2025) and still underexplored questions on whether we can also use AI itself to help ensure compliance with AI regulation (Micklitz and Sartor 2025), it is even further underexplored whether regulators are aware of the quantum era and are ready to regulate and to enforce quantum computing regulations.

There are links between a third risk of trust and a fourth risk of nefarious uses. As noted by Campbell (2023), 'We trust classical computers in part because we can verify their computations with pen and paper. But quantum computers involve such arcane physics, and deal with such complex problems, that traditional verification is extremely tricky. For now, it's possible to simulate many quantum calculations on a traditional supercomputer to check the outcome. But soon will come a time when trusting a quantum computer will require a leap of faith.' The trust question becomes even more important if (or when) the processing speeds of quantum computers advance our current era of narrow artificial intelligence into artificial general intelligence and beyond. Without trust-focused developments, such leaps may occur before protective regulatory guardrails are developed. The necessity of regulatory guardrails becomes even more important if quantum technologies are used for nefarious purposes. This potential fourth risk may include the ability of quantum computers to break the cryptography that keeps blockchain secure, to decrypt confidential financial transactions or healthcare records, to challenge current internet of things security and related 5G network vulnerabilities, to overcome currently secure digital signature schemes, to assist in the rise of 'quantum adversarial machine learning', and for quantum corporations and researchers to 'become targets by cybercriminals and hacktivists' (Faruk et al., 2022: 4–5).

This article has attempted to articulate the quantum-era challenge specific to the discipline of public policy, identified its wickedness and its partially unstructured nature for policymakers, and provided examples specific to the agenda-setting and policy formulation steps of the public policy cycle. The future is quantum and its past time for public policy scholars and our discipline-specific journals to engage the topic.

Acknowledgement

We are grateful to the in-depth feedback provided by Dr Leslie A. Pal. Any errors are our own.

Author contributions

Kim Moloney (Conceptualization, Formal analysis, Writing—original draft, Writing—review & editing) and Saif Al-Kuwari (Conceptualization, Formal analysis, Writing—review & editing).

Conflict of interest. None declared.

Funding

None declared.

References

Adams, P. H. (2019) *Why Quantum Computing Could Make Today's Cybersecurity Obsolete*, Geneva: World Economic Forum.

Aiello, C. D. et al. (2021) 'Achieving a Quantum Smart Workforce', *Quantum Science and Technology*, **6**: 030501.

American Museum of Natural History. (2024) *Atoms and Their Sizes*, Washington DC: American Museum of Natural History. https://www.amnh.org/exhibitions/permanent/scales-of-the-universe/atoms, accessed 15 Sep. 2024.

Amoore, L. (2018) 'Cloud Geographies: Computing, Data, Sovereignty', *Progress in Human Geography*, **42**: 4–24.

Bali, A. S. et al. (2021) 'Procedural Policy Tools in Theory and Practice', *Policy and Society*, **40**: 295–311.

Bannister, F., and Connolly, R. (2014) 'ICT, Public Values and Transformative Government: a Framework and Programme for Research', *Government Information Quarterly*, **31**: 119–28.

Barker, E. (2016) *Recommendation for Key Management, Part 1: General (NIST Special Publication 800–57, Part 1, Revision 4)*, Washington: National Institute of Standards and Technology.

Baumgartner, F. R., and Jones, B. D. (1993) *Agendas and Instability in American Politics*, Chicago, IL: University of Chicago Press.

Bernstein, D. J., and Lange, T. (2017) 'Post-Quantum Cryptography', *Nature*, **549**: 188–94. https://doi.org/10.1038/nature23461.

Bova, F., Goldfarb, A., and Melko, R. G. (2021) 'Commercial Applications of Quantum Computing', *EPJ Quantum Technology*, **8**: 2.

Bozeman, B. (2007) *Public Values and Public Interest: Counterbalancing Economic Individualism*, Washington: Georgetown University Press.

Brennan, G. et al. (2021) *An Australian Strategy for the Quantum Revolution*, Canberra: Australian Strategic Policy Institute.

Brooks, M. (2023) '*IBM Wants to Build a 100,000-Qubit Quantum Computer*', Boston MA: MIT Technology Review, https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/, accessed 10 May 2025.

Busby, A., Digby, A., and Fu, E. (2017) *Quantum Technologies Public Dialogue Report*, Oxford: Networked Quantum Information Technologies Hub.

Callon, R. (1994) 'Is Science a Public Good?' *Science, Technology, and Human Values*, **19**: 395–424.

Campbell, C. (2023) 'Quantum Computers Could Solve Countless Problems—and Create a Lot of New Ones', New York NY: Time, https://time.com/6249784/quantum-computing-revolution/, accessed 10 May 2025.

Castelvecchi, D. (2023) 'IBM Releases First-Ever 1,000-Qubit Quantum Chip', *Nature*, **624**: 238–8. https://doi.org/10.1038/d41586-023-03854-1.

Center for AI Safety. (2023) *Statement on AI Risk*. Center for AI Safety, https://safe.ai/work/statement-on-ai-risk#open-letter, accessed 15 Sep 2024.

Chen, D. et al. (2024) 'Additive Manufacturing Provides Infinite Possibilities for Self-Sensing Technology', *Advanced Science*, **11**: e2400816.

Chohan, U. (2021) *Public Value and the Digital Economy*, New York: Routledge.

Clifton, J., and Pal, L. A. (2022) 'The Policy Dilemmas of Blockchain', *Policy and Society*, **41**: 321–7.

Coates, R., and Chhetri, M. B. (2024) 'Quantum readiness: unlocking the quantum advantage for Australian industries', in *IEEE International Conference on Quantum Computing and Engineering*, Montreal. vol. **2**, pp. 61–4. https://doi.org/10.1109/QCE60285.2024.10253

Coelho, T. R., Cunha, M. A., and Pozzebon, M. (2017) 'eParticipation and the policy cycle: designing a research agenda', in *Proceedings of the 18th Annual International Conference on Digital Government Research*. New York, NY: Association for Computing Machinery. 282–92. https://doi.org/10.1145/3543434.3543644

Cooper, C. H. V. (2022) 'Exploring Potential Applications of Quantum Computing in Transportation Modelling', *IEEE Transactions on Intelligent Transportation Systems*, **23**: 14712–20.

Coursey, D., and Norris, D. F. (2008) 'Models of E-Government: Are they Correct? An Empirical Assessment', *Public Administration Review*, **68**: 523–36.

Cresswell, A. M., Burke, G. B., and Pardo, T. (2006) *Advancing Return on Investment, Analysis for Government IT: a Public Value Framework*, Albany, NY: Center for Technology in Government, University at Albany, SUNY.

Csenkey, K., and Bindel, N. (2023) 'Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat', *Journal of Cybersecurity*, **9**: tyad001.

Dekker, T., and Martin-Bariteau, F. (2023) 'Regulating Uncertain States: a Risk-Based Policy Agenda for Quantum Technologies', *Canadian Journal of Law and Technology*, **20**: 179–224.

Der Derian, J., and Wendt, A. (2022) 'Quantum International Relations: the Case for a New Human Science of World Politics', in Der Derian, J., and Wendt, A., (eds.) *Quantum International Relations: A Human Science for World Politics*. pp. 3–26, Oxford: Oxford University Press.

Dunleavy, P., Margetts, H., Bastow, S. et al. (2006) 'New Public Administration Is Dead – Long Live Digital-Era Governance', *Journal of Public Administration Research and Theory*, **16**: 467–94.

Editors (2017) 'Researchers Should Reach beyond the Science Bubble', *Nature*, **542**: 391.

European Union. (2018) 'Statement on Artificial Intelligence, Robotics, and "Autonomous" Systems', Brussels: European Union.

European Union. (2025) 'New survey reveals public support for quantum science and technology', Brussels: EU Quantum Flagship, https://qt.eu/news/2025/2025-04-14_new-survey-reveals-public-support-for-quantum-science-and-technology, accessed 27 April 2025.

Faruk, M. J. H. et al. (2022) 'A Review of Quantum Cybersecurity: Threats, Risks and Opportunities', in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*. Victoria, TX, USA: IEEE, pp. 1–8. https://doi.org/10.1109/ICAIC53980.2022.9896970

Fenwick, M., Kaal, W. A., and Vermeulen, E. P. (2016) 'Regulation Tomorrow: What Happens When Technology Is Faster than the Law', *American University Business Law Review*, **6**: 561–94.

Ferlie, E. et al. (2011) 'Public Policy Networks and 'Wicked Problems': a Nascent Solution?' *Public Administration*, **89**: 307–24.

Foster, K. R., Vecchia, P., and Repacholi, M. H. (2000) 'Science and the Precautionary Principle', *Science*, **288**: 979–81.

Gercek, A. A., and Seskir, Z. C. (2025) 'Navigating the Quantum Divide(s)', *IEEE Engineering Management Review*, 1–19. https://doi.org/10.1109/EMR.2025.3547927.

Giani, A., and Eldredge, Z. (2021) 'Quantum Computing Opportunities in Renewable Energy', *SN Computer Science*, **2**: 393.

Gidney, C. (2025) 'How to Factor 2048 Bit RSA Integers with Less Than a Million Noisy Qubits', arXiv preprint arXiv:2505.15917.

Global Security Forum. (2025) *Rt. Hon. Mark Pritchard [Video File]*. https://vimeo.com/event/5092612/embed/9d5276761f (3:54:28–4:01:17) 15 May 2025.

Gorbanyov, M., Malaika, M., and Sedik, T. S. (2021) 'Quantum Computing and the Financial System: Spooky Action at a Distance?' in *IMF Working Papers, No 2021/071*. Washington: International Monetary Fund.

Government of Australia. (2023) *National Quantum Strategy*, https://www.industry.gov.au/publications/national-quantum-strategy, accessed 7 September 2025.

Government of Canada (2023) *Overview of Canada's National Quantum Strategy*, https://ised-isde.canada.ca/site/national-quantum-strategy/en, accessed 7 September 2025.

Government of India. (2023) *National Quantum Mission*, New Delhi: Government of India. https://dst.gov.in/national-quantum-mission-nqm, accessed 7 September 2025.

Government of Japan. (2023) *Strategy of Quantum Future Industry Development*, https://www8.cao.go.jp/cstp/english/strategy_r08.pdf, accessed 7 September 2025.

Halachmi, A., and Greiling, D. (2013) 'Transparency, e-Government, and Accountability', *Public Performance and Management Review*, **36**: 562–84.

Harrison, T. M. et al. (2011) 'Open Government and E-Government: Democratic Challenges from a Public Value Perspective', in *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*. New York NY: Association for Computing Machinery, pp. 245–53. https://doi.org/10.1145/2037556.2037597

Hartung, T. et al. (2025) 'Is Regulatory Science Ready for Artificial Intelligence?' *npj Digital Medicine*, **8**: 200. https://doi.org/10.1038/s41746-025-01596-0.

Head, B. W. (2022) *Wicked Problems in Public Policy: Understanding and Responding to Complex Challenges*, Cham: Springer International Publishing.

Hendrycks, D., Mazeika, M., and Woodside, T. (2023) *An Overview of Catastrophic AI Risks*. San Francisco CA: Center for AI Safety.

Herman, A. (2021) 'Q-Day is Coming Sooner Than We Think', New York NY: Forbes, https://www.forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/, accessed 15 September 2024.

Herman, A., and Friedson, I. (2018) 'Quantum Computing: How to Address the National Security Risk', Washington: Hudson Institute.

Hisschemöller, M., and Hoppe, R. (1995) 'Coping with Intractable Controversies: the Case for Problem Structuring in Policy Design and Analysis', *Knowledge and Policy*, **8**: 40–60.

Ho, K. T. M. et al. (2024) 'Quantum Computing for Climate Resilience and Sustainability Challenges', in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, **2**. pp. 262–267, Montreal, QC: IEEE. https://doi.org/10.1109/QCE60285.2024.10289

Hoofnagle, C. J., and Garfinkel, S. L. (2022) *Law and Policy for the Quantum Age*, Cambridge: Cambridge University Press.

Hoppe, R. (2018) 'Heuristics for Practitioners of Policy Design: Rules-of-Thumb for Structuring Unstructured Problems', *Public Policy and Administration*, **33**: 384–408. https://doi.org/10.1177/0952076717709338.

Howell, E., and Harvey, A. (2022) 'How Many Galaxies Are There?', https://www.space.com/25303-how-many-galaxies-are-in-the-universe.html, accessed 15 September 2024.

Howlett, M. (2019) *Designing Public Policies: Principles and Instruments*. New York NY: Routledge.

Howlett, M. (2023) 'Where Tools Are Deployed in the Policy Process: Policy Instruments and the Policy Cycle', in Howlett, M., (ed.) *The Routledge Handbook of Policy Tools*. pp. 36–46, Milton Park: Routledge.

Howlett, M., and Mukherjee, I. (2017) 'Policy Formulation: Where Knowledge Meets Power in the Policy Process', in Howlett, M., and Mukherjee, I., (eds.) *Handbook of Policy Formulation*. pp. 3–22. Cheltenham UK: Edward Elgar Publishing.

Huntley, R. (2024) 'Quantum Sensing: Unlocking New Opportunities,' in *EE Times Europe*, https://www.eetimes.eu/quantum-sensing-unlocking-new-opportunities/, accessed 15 September 2024.

IBM. (2022) 'IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two', https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two, accessed 15 September 2024.

Inglesant, P. et al. (2021) 'Asleep at the Wheel? Responsible Innovation in Quantum Computing', *Technology Analysis and Strategic Management*, **33**: 1364–76.

International Standardization Organization (2024) *IEC and ISO Launch a New Joint Technical Committee on Quantum Technologies*, Geneva: International Standardization Organization.

Jia, K., and Chen, S. (2022) 'Global Digital Governance: Paradigm Shift and an Analytical Framework', *Global Public Policy and Governance*, **2**: 283–305.

Johnson, W. G. (2019) 'Governance Tools for the Second Quantum Revolution', *Jurimetrics*, **59**: 487–522.

Joseph, D. et al. (2022) 'Transitioning Organizations to Post-Quantum Cryptography', *Nature*, **605**: 237–43. https://doi.org/10.1038/s41586-022-04623-2.

Kingdon, J. W. (1984) *Agendas, Alternatives, and Public Policies*, Boston: Little, Brown.

Knill, C., and Tosun, J. (2008) 'Policy Making', *Comparative Politics*, **2**: 373–88.

Kong, I. I., Janssen, M. M., and Bharosa, N. N. (2022) 'Challenges in the Transition towards a Quantum-Safe Government', in Charles C. Hinnant, Adegboyega Ojo (eds), *The 23rd Annual International Conference on Digital Government Research*. Staten Island, NY: Association for Computing Machinery. 368–376. https://doi.org/10.1145/3085228.3085277

Kong, I. I., Janssen, M. M., and Bharosa, N. N. (2024) 'Realizing Quantum-Safe Information Sharing: Implementation and Adoption Challenges and Policy Recommendations for Quantum-Safe Transitions', *Government Information Quarterly*, **41**: 101884.

Kop, M. et al. (2024) 'Towards Responsible Quantum Technology: Safeguarding, Engaging and Advancing Quantum R&D', *UC Law Science and Technology Journal*, **15**: 63–85.

Krelina, M. (2021) 'Quantum Technology for Military Applications', *EPI Quantum Technology*, **8**: 1–53.

Krishnamurthy, V. (2022) 'Quantum Technology and Human Rights: an Agenda for Collaboration', *Quantum Science and Technology*, **7**: 044003.

Lindsay, J. R. (2020) 'Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage', *Security Studies*, **29**: 335–61.

Lohrmann, A. (2023) 'Quantum Computers: What Is Q-Day? And What's the Solution? Government Technology', https://www.govtech.com/blogs/lohrmann-on-cybersecurity/quantum-computers-what-is-q-day-and-whats-the-solution, accessed 15 September 2024.

Manheim, K., and Kaplan, L. (2019) 'Artificial Intelligence: Risks to Privacy and Democracy', *Yale Journal of Law and Technology*, **21**: 106–88.

Maraveas, C. et al. (2024) 'Harnessing Quantum Computing for Smart Agriculture: Empowering Sustainable Crop Management and Yield Optimization', *Computers and Electronics in Agriculture*, **218**: 108680.

McCrohan, K. F. (1989) 'Information Technology, Privacy, and the Public Good', *Journal of Public Policy and Marketing*, **8**: 265–78.

McLean, S. et al. (2023) 'The Risks Associated with Artificial General Intelligence: a Systematic Review', *Journal of Experimental and Theoretical Artificial Intelligence*, **35**: 649–63.

Menezes, A., and Stebila, D. (2021) 'Challenges in Cryptography', *IEEE Security and Privacy*, **19**: 70–3.

Mergel, I. et al. (2025) 'Implementing AI in the Public Sector', *Public Management Review*, 1–14.

Micklitz, H. W., and Sartor, G. (2025) 'Compliance and Enforcement in the AIA through AI', *Yearbook of European Law*, **43**: 297–341.

Moloney, K., Al-Kuwari S., and Abassi, A. A. (2026, under review). 'Implications of Quantum Computing, Quantum Capacity Gaps, and Quantum Divides'.

Moore, M. (2014) 'Public Value Accounting: Establishing the Philosophical Basis', *Public Administration Review*, **74**: 465–77.

Muradoglu, M. et al. (2025) 'Quantum-assured magnetic navigation achieves positioning accuracy better than a strategic-grade INS in airborne and ground-based field trials', arXiv preprint arXiv:2504.08167.

Nasution, H. N., and Mavondo, F. T. (2008) 'Organisational Capabilities: Antecedents and Implications for Customer Value', *European Journal of Marketing*, **42**: 477–501.

National Quantum Institute. (2025) 'About the National Quantum Institute', Washington DC. https://www.quantum.gov/about/, accessed 10 May 2025.

National Working Group (1999) *Quantum Information Science: an Emerging Field of Interdisciplinary Research and Education in Science and Engineering*, Arlington: National Science Foundation.

Newman, J., and Head, B. W. (2017) 'Wicked Tendencies in Policy Problems: Rethinking the Distinction between Social and Technical Problems', *Policy and Society*, **36**: 414–29.

NIST. (2022) 'NIST Announces First Four Quantum-Resistant Cryptographic Algorithms', Washington: National Institute of Standard and Technology.

NIST. (2024) 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards', Washington: National Institute of Standard and Technology.

Nzobonimpa, S., and Savard, J. F. (2023) 'Ready but Irresponsible? Analysis of the Government Artificial Intelligence Readiness Index', *Policy and Internet*, **15**: 397–414.

Open Quantum Institute (2024) *Intelligence Report on the Multilateral Governance of Quantum Computing for SDGs*, Geneva: CERN.

Orús, R., Mugel, S., and Lizaso, E. (2019) 'Quantum Computing for Finance: Overview and Prospects', *Reviews in Physics*, **4**: 100028.

Overman, E. S. (1996) 'The New Sciences of Administration: Chaos and Quantum Theory', *Public Administration Review*, **56**: 487–91.

Overman, E. S. (1999) 'The New Science of Management: Chaos and Quantum Theory and Method', *Journal of Public Administration Research and Theory*, **6**: 75–89.

Owen, R. et al. (2013) 'A Framework for Responsible Innovation', in R. Owen, J. Bessant, and M. Heintz (eds) *Responsible Innovation:*

Managing the Responsible Emergence of Science and Innovation in Society, pp. 27–50. Chichester, UK: Wiley.
Parker, E. (2021) *Commercial and Military Applications and Timelines for Quantum Technology*, Santa Monica: Rand.
Pencheva, I., Esteve, M., and Mikhaylov, S. J. (2020) 'Big Data and AI–a Transformational Shift for Government: So, What Next for Research?' *Public Policy and Administration*, **35**: 24–44.
Perrier, E. (2022) 'The Quantum Governance Stack: Models of Governance for Quantum Information Technologies', *Digital Society*, **1**: 1–22.
Peters, B. G. (2018) *Policy Problems and Policy Design*, Cheltenham: Edward Elgar.
Phillipson, F. (2023) 'Quantum Computing in Telecommunication—a Survey', *Mathematics*, **11**: 3423.
Phillipson, F. (2024) 'Quantum computing in logistics and supply chain management an overview', arXiv preprint arXiv:2402.17520.
Preskill, J. (2012) 'Quantum computing and the entanglement frontier'. https://arxiv.org/abs/1203.5813v3
Purohit, A. et al. (2024) 'Building a Quantum-Ready Ecosystem', *IET Quantum Communication*, **5**: 1–18.
Quantum Insider. (2023) 'Chinese Quantum Companies and National Strategy 2023', Quantum Insider, https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/, accessed 7 September 2025.
Raheman, F. (2022) 'The Future of Cybersecurity in the Age of Quantum Computers', *Future Internet*, **14**: 335.
Rasool, R. U. et al. (2023) 'Quantum Computing for Healthcare: a Review', *Future Internet*, **15**: 94–130.
Republic of Korea. (2023) *Korea's National Quantum Strategy*. Seoul, South Korea: Republic of Korea. https://quantuminkorea.org/wp-content/uploads/2024/06/Koreas-National-Quantum-Strategy-2023_c.pdf, accessed 7 September 2025.
Ricci, P. F., and Sheng, H.-X. (2013) 'Benefits and Limitations of the Precautionary Principle', in J. O. Nriagu, (ed.) *Encyclopedia of Environmental Health*. pp. 276–85. Amsterdam: Elsevier. https://doi.org/10.1016/B978-0-444-52272-6.00230-0
Rittel, H., and Webber, M. (1973) 'Dilemmas in a General Theory of Planning', *Policy Sciences*, **4**: 155–69.
Roberson, T., Leach, J., and Raman, S. (2021) 'Talking about Public Good for the Second Quantum Revolution: Analysing Quantum Technology Narratives in the Context of National Strategies', *Quantum Science and Technology*, **6**: 025001.
Rodriguez Müller, A. P., Martin Bosch, J., and Tangi, L. (2025) 'An Overview of the Expected Public Values Arising from Blockchain Adoption in the European Public Sector', *International Journal of Public Sector Management*, **38**: 53–76.
Roush, W. (2020) 'The Google-IBM Quantum Supremacy Feud [Podcast]', in *Deep Tech*, https://www.technologyreview.com/2020/02/26/905777/google-ibm-quantum-supremacy-computing-feud/, accessed 15 September 2024.
Seskir, Z. C. et al. (2023) 'Democratization of Quantum Technologies', *Quantum Science and Technology*, **8**: 024005.
Shivaoki, R., and Howlett, M. (2022) 'Agenda-Setting Tools in Theory and Practice', in M. Howlett (ed.) *The Routledge Handbook of Policy Tools*, pp. 113–24. London: Routledge.
Sridhan, S. (2024) 'The Quantum Race: Quantum Day 2025 Has Ignited a Global Race, Reshaping Computing and Cybersecurity', in *Financial Express*, https://www.financialexpress.com/opinion/the-quantum-race-quantum-day-2025-has-ignited-a-global-race-reshaping-computing-and-cybersecurity/3399085/, accessed 15 September 2024.
Stix, G. (2005) 'Best-Kept Secrets', *Scientific American*, **292**: 78–83.
Suchara, M. et al. (2018) 'Hybrid Quantum-Classical Computing Architectures', in *3rd International Workshop on Post-Moore Era Supercomputing*, Dallas: SC.
Swayne, M. (2025) 'Quantum Computing Roadmaps: a Look at the Maps and Predictions of Major Quantum Players', Quantum Insider, https://thequantuminsider.com/2025/05/16/quantum-computing-roadmaps-a-look-at-the-maps-and-predictions-of-major-quantum-players/, accessed 8 September 2025.
Taylor, R. D. (2020) 'Quantum Artificial Intelligence: a "Precautionary" U.S. Approach?' *Telecommunications Policy*, **44**: 101909.
Ten Holter, C. T. et al. (2022) 'Bridging the Quantum Divides: a Chance to Repair Classic(al) Mistakes?' *Quantum Science and Technology*, **7**: 1–5.
Ten Holter, C. T., Inglesant, P., and Jirotka, M. (2023) 'Reading the Road: Challenges and Opportunities on the Path to Responsible Innovation in Quantum Computing', *Technology Analysis and Strategic Management*, **35**: 844–56.
Tigges, C. P. et al. (2003) 'Quantum Computing Accelerator I LLRD 52750 Final Report', Albuquerque: Sandia National Laboratories.
Tschirhart, P., and Stockton, N. (2025) 'Can the US Prevent AGI from Being Stolen?' in *AI Frontiers*, https://www.ai-frontiers.org/articles/can-the-us-prevent-agi-from-being-stolen, accessed 10 May 2025.
Turnpenny, J. R. et al. (2015) 'The Tools of Policy Formulation: An Introduction', in Jordan, A. J., and Turnpenny, J. R., (eds.) *The Tools of Policy Formulation*. pp. 3–30. Cheltenham: Edward Elgar.
Twizeyimana, J. D., and Andersson, A. (2019) 'The Public Value of e-Government - Literature Review', *Government Information Quarterly*, **26**: 167–78.
Umbrello, S., Seskir, Z. C., and Vermaas, P. E. (2024) 'Communities of Quantum Technologies: Stakeholder Identification, Legitimation and Interaction', *International Journal of Quantum Information*, **22**: 2450012.
UNESCO (2024) *Concept Note of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) on the Ethics of Quantum Computing*, Geneva: UNESCO.
United Nations (2023) *Governing AI for Humanity*, New York: United Nations.
United Nations (2024) *Pact for the Future, Global Digital Compact, and Declaration on Future Generations*, New York: United Nations.
Valle-Cruz, D. et al. (2020) 'Assessing the Public Policy-Cycle Framework in the Age of Artificial Intelligence: from Agenda-Setting to Policy Evaluation', *Government Information Quarterly*, **37**: 101509.
Van Deursen, A. J., and Mossberger, K. (2018) 'Anything for Anyone? A New Digital Divide in Internet-of-Things Skills', *Policy and Internet*, **10**: 122–40.
Vermaas, P. E. (2017) 'The Societal Impact of the Emerging Quantum Technologies: a Renewed Urgency to Make Quantum Theory Understandable', *Ethics and Information Technology*, **19**: 241–6.
Von Schomberg, R. (2013) 'A Vision of Responsible Research Innovation', in R. Owen, J. R. Bessant, and M. Heintz (eds) *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, pp. 51–74. Chichester UK: Wiley.
Waller, P., and Weerakkody, V. (2016) *Digital Transformation through Policy Design with ICT-Enhanced Instruments*, London: Brunel University London.
Wang, Y. et al. (2022) 'A Novel Metric for Assessing National Strength in Scientific Research: Understanding China's Research Output in Quantum Technology through Collaboration', *Journal of Data and Information Science*, **7**: 39–60.
Wassenaar Secretariat. (2025) 'About Us', https://www.wassenaar.org/about-us/, accessed 10 May 2025.
Wendt, A. (2015) *Quantum Mind and Social Science: Unifying Physical and Social Ontology*, Cambridge: Cambridge University Press.
Wirtz, B. W., Weyerer, J. C., and Geyer, C. (2019) 'Artificial Intelligence and the Public Sector – Applications and Challenges', *International Journal of Public Administration*, **42**: 596–615.
Wolbring, G. (2022) 'Auditing the "Social" of Quantum Technologies: a Scoping Review', *Societies*, **12**: 41–70.
World Economic Forum. (2023) 'Global Future Council on the Future of Quantum Economy', World Economic Forum, https://initiatives.weforum.org/quantum/home, accessed 2 November 2025.

Wright, J. (2017) 'Quantum-Based Agriculture: the Final Frontier', in *Organic World Congress 2017*. pp. 107–11. Thunen: Johann Heinrich von Thünen-Institut. https://doi.org/10.3220/REP1510907717000

Zaidan, E., and Ibrahim, I. A. (2024) 'AI Governance in a Complex and Rapidly Changing Regulatory Landscape: a Global Perspective', *Humanities and Social Sciences Communications*, **11**: 1121.

Zyzak, B., Sienkiewicz-Małyjurek, K., and Jensen, M. R. (2024) 'Public Value Management in Digital Transformation: a Scoping Review', *International Journal of Public Sector Management*, **37**: 845–63.

Science and Public Policy, 2025, 00, 1–13
DOI: https://doi.org/10.1093/scipol/scaf065
Article