



The Quantum Governance Stack: Models of Governance for Quantum Information Technologies

Elija Perrier^{1,2,3,4} 

Received: 16 March 2022 / Accepted: 9 August 2022 / Published online: 12 October 2022
© The Author(s) 2022

Abstract

The emergence of quantum information technologies with potential application across diverse industrial, consumer and technical domains has thrown into relief the need for practical approaches to their governance. Technology governance must balance multiple objectives including facilitating technological development while meeting legal requirements, normative expectations and managing risks regarding the use of such technology. In this paper, we articulate a variety of idealised governance models and approaches for synthesising these complementary and sometimes competing objectives. We set out a comparative analysis of quantum governance in the context of existing models of technological governance. Using this approach, we develop an actor-instrument model for quantum governance, denoted the ‘quantum governance stack’, across a governance hierarchy from states and governments through to public and private institutions. Our model sets out key characteristics that quantum governance should exhibit at each level in the stack, including identification of stakeholder rights, interests and obligations impacted by quantum technologies and the appropriate instruments by which such impacts are managed. We argue that quantum governance must be responsive based on (a) the state of technology at the time; (b) resource and economic requirements for its development; and (c) assessments and estimates of the near-term and future impacts of such technology. Our work provides a pragmatic introduction to quantum governance by (a) specifying a taxonomy of governance actors and instruments and (b) providing examples of how different stakeholders within the stack might implement governance responses to quantum information technologies. It is intended for use by stakeholders in government, industry, academia and civil society to help inform their governance response to the quantum technology revolution.

Keywords Quantum · Ethics · Governance

✉ Elija Perrier
eper2139@uni.sydney.edu.au; elija.t.perrier@student.uts.edu.au

Extended author information available on the last page of the article

1 Introduction

Quantum information technology (QIT) is a dynamic and emerging field with potentially far-reaching economic, geopolitical and even social impacts. While technology governance is a vast discipline Rayfuse (2017), Brownsword and Rights (2008), Brownsword et al. (2017), work focusing specifically on the governance of QIT is nascent by comparison. This is primarily due to the early stage of QIT development and considerable uncertainty regarding the form which QIT will eventually take. As discussed below, despite promising advances and considerable investment in the sector, QIT remains at a prototypical stage of development with the prospect of fully scalable fault-tolerant QIT devices remaining unrealised. Most work on quantum governance has emerged in the context of discussions on either the necessary conditions to support quantum innovation or in the context of security implications of, for example, vaunted cryptographic implications of QIT. Importantly, QIT is not emerging in a vacuum: a raft of existing governance procedures, frameworks, institutions and practices already exist for its regulation. The governance of QIT requires situating QIT within the broader nexus and hierarchy of technology governance in general. Doing so mandates an analysis of how existing governance instruments could relate to QIT and what, if any, novel governance responses are required to meet policy objectives.

1.1 Contributions

Despite uncertainty in the form and shape that scalable QIT will take, a number of works have started to examine the implications of QIT across a variety of governance domains. These include situating the governance of QIT within (i) technology governance more generally Johnson (2018), Kop (2021), (ii) responsible innovation paradigms Ten Holter et al. (2021) and (iii) intellectual property regimes Kop (2021). Other frameworks have also recently emerged seeking to provide guidance on overarching governance principles of use to different stakeholders in QIT sectors World Economic Forum (2022). This paper builds upon such contributions by providing an outline of an (idealised) actor and instrument model of quantum governance. Its focus is upon formal and informal governance instruments as means of mediating benefits and risks of QIT as they affect stakeholder rights, interests and obligations across a hierarchy of international, national, public and private contexts. We denote this hierarchy as the *quantum governance stack* given the hierarchical nature of governance and its direct relationship to information technologies. Our approach adopts the following taxonomy: (a) *states* (governments) as the primary agents of regulation, and their role in (i) *international* and (ii) *national* formal (legislative) regulation; (b) multilateral institution(s); (c) national instrumentalities, such as parliaments and administrative agencies; (d) industrial and commercial stakeholders; (e) universities and academia; (f) individual producers/consumers of QIT and (g) civil society and technical community groups. By *quantum*, we mean quantum information technologies, principally quantum computing, communication and quantum sensing that are fundamentally characterised by their informational processing properties; by *governance*, we mean both ‘hard’ formal

enforceable rules and ‘soft’ power or influence driven by particular objectives or outcomes; by *models*, we mean an idealised methodology and structure for what different parts of the governance stack would ideally resemble. We also aim to make our contribution practical to help guide stakeholders’ thinking about their role in the governance of QIT. Our focus is analysing how existing governance frameworks provide models which may be adapted, reproduced or modified to provide best-practice responses to QIT. To this end, our paper contributes the following: (i) situating the governance of quantum systems within existing technology governance instruments, such as international treaties, legislative regimes and regulation; (ii) a comparative analysis of the governance of QIT by comparison with similar information and engineering technologies; (iii) a survey of different quantum stakeholders, their objectives and their imperatives; and (iv) providing practical guidance for quantum stakeholders.

We argue that our quantum governance stack model, with its focus on stakeholder rights, duties and interests and empirical evaluation, articulates core necessary conditions required for the development of appropriate QIT governance by states, governments, technical communities, private sector participants, public institutions, individuals and civil society groups. This includes providing a systematic means by which stakeholder can frame their participation in QIT governance, a focus on risk management and balancing competing interests. Our contention is that such an empirically focused approach (based upon ongoing assessments of the state of QIT) allows for evolutionary forms of governance that are responsive to the dynamic and highly uncertain trajectory of QIT development in ways that will mitigate risks but also foster development of this critical technology. Our model explicates key characteristics that quantum governance should exhibit, including (i) identification of stakeholders involved in QIT together with an assessment of their rights, interests and obligations which will likely be impacted by QIT; (ii) avenues for stakeholder engagement; (iii) risk-assessment of such impacts; (iv) identification of appropriate instruments by which such impacts are managed and obligations upon stakeholders are encoded; (v) methods for assessing effectiveness; and (vi) processes for dynamically updating the governance architectures as required.

1.2 The What and Why of Quantum Governance

The governance of QIT is likely to be complex and multifaceted. It spans a diverse range of institutional practices and norms across government, corporate, individual and supranational stakeholders. Governance can cover a variety of formal and informal instruments involving complex interconnections among law, regulation, normativity, institutional practice, risk management and discursive power Black (2005, 2012). Quantum governance is therefore naturally a contextual and blended concept. In this paper, we adopt a broad conceptualisation of governance as involving both (i) hierarchical and enforceable rules and decision-procedures together with (ii) normative or discursive approaches.

Even before considering the form of governance for QIT, we must address two threshold questions: (1) why, despite uncertainty around QIT’s technological

development, is discussion of QIT governance well-motivated?; and (2) whether QIT requires different, new or novel governance that does not already exist within the technology governance landscape? The answer to the first question is found by reflecting upon the classical Collingridge dilemma Collingridge (1980) of technological governance generally (which we discuss in Sect. 2.4 below), namely that regulation is difficult until technology becomes more developed, widely disseminated and its impact is known, yet by that time regulation can become difficult. Emerging norms of use tend to set the context for later regulation, by embedding ways of using or propagating technology across industry, government and markets. Once such norms are established — and particularly once economic sunk costs associated with them accumulate — it can become difficult for regulatory responses to shift default behaviour. An important way of responding to this dilemma is for stakeholders involved in QIT to concurrently consider appropriate risks, impacts and governance models as the technology is developing, thereby influencing the ongoing use of technology in ways that factor in the objectives of regulation.

The second of these questions can be framed in jurisprudential language: is quantum governance *sui generis*, requiring its own specific governance regimes? The answer is both yes and no. As we discuss in this article, the web of technology governance instruments regulating the use of technology already apply to the various iterations and manifestations of QIT. Technology has since its inception been entwined with governance Solis (2010). Moreover, technology has also consistently been the subject of multilateral initiatives designed towards their regulation, such as treaties banning certain chemical and biological weapons Geneva (1925), United Nations (1972), (1993) and exceedingly injurious weaponry United Nations (1980), (1996). Thus, the regulation of QIT fits within the broad regulation of emergent technologies such as artificial intelligence Solis (2010), Allenby (2014), albeit with its own unique features.

As a number of authors highlight, while much literature in technology governance focuses on finer-grained questions of what regulation is justified or the form of regulation, often a more relevant or a priori question to ask is how existing legal or regulatory responses may be adapted to QIT and their impacts Brownsword and Yeung (2008), Moses (2017). To this end, technology governance is often framed in terms of technology neutrality, responding to the outcomes effects or impact of technology rather than the technological specifics per se Koops (2006). Such technology-neutral approaches also recognise the disruptive nature that technological innovation can present legal systems Brownsword (2008), Maas (2019), which are themselves developed among a backdrop of economic modes of production and social interaction which are evolving. This is particularly the case given attempts to prescriptively list or even predict the impact of technology, let alone define it, can be fraught. The evolving nature of QIT itself therefore requires a dynamic and evolutionary governance response.

Some scholars Moses (2017) argue that the form of technology is in effect irrelevant to justification of regulation — and that rather the focus of regulation is in its effects. However, the material form of technology will affect the form of regulation and thus such material specificity becomes integral to justifying why regulation takes one form or another. For example, the specific capacities and limitations of QIT, such as the

potential regarding decryption and the limited capacity to intervene in quantum systems while maintaining requisite quantum coherences, may mandate that the forms of technical control (and regulatory imperatives) factor in such constraints in novel ways (see Perrier (2021) for a synopsis). While certain risks, such as the downside risks, posed by certain QIT (should they be realised) are not necessarily novel per se (e.g. the risk or harms from access to quantum decryption technology may be adequately covered by laws prohibiting such activities regardless of the technology used), arguably there is a rationale in technology-specific governance regimes beyond mere technical specification. Such rationales include (i) the way in which *sui generis* regimes act to coalesce various forms of governance around a particular technology, effectively enumerating or articulating how broad abstract principles would specifically apply in the case of QIT (rather than leaving such principles abstract and thus potentially less actionable); and (ii) that governance should match the discourses around technology. This is because doing so enables stakeholders to more readily connect their domain expertise or community activity within a technology context to governance itself, rather than relying on such stakeholders to join the dots as it were. It also helps stakeholders realise that their use or development of technology is governed already. Thus, there are plausible arguments for why it may be of practical use to develop quantum-specific regulation. Rationales for regulation include (i) economic rationales, such as performing coordinating functions or facilitating market efficiency, (ii) the protection of stakeholder rights (human rights) and (iii) regulation for maintenance of order Moses (2017), Prosser (2010). For example, the market efficiency rationale of promoting competition, avoiding monopolistic practices and concentrations of market power Blair and Sokol (2017), American Bar Association (2017) is as applicable to the quantum sector as any other. Similarly, as identified in emerging literature on quantum ethics Perrier (2021), World Economic Forum (2022), QIT poses its own unique risks to be managed in proportional ways Rothstein et al. (2006). Furthermore, normative claims regarding the need to ensure democratic accountability in the management of technology, that it be subject to democratic will Feenberg (1999), apply categorically also to QIT.

2 Quantum Information Technology

2.1 Overview

A useful starting point for governance of QIT is to develop a taxonomy of (i) the significant differences with classical technologies; and (ii) the unique risks (upside and downside) that arise consequential upon those differences. In this article, we focus our approach on quantum information technologies and information processing, such as quantum computation, quantum communication and quantum sensing.¹ We set

¹ In terms of working taxonomies, it is useful to partition technology classifications into (i) *classical* technologies, those technologies or manners of manufacture which are not explicitly designed to leverage quantum effects and (ii) *quantum* technologies which explicitly leverage particular quantum mechanical phenomena, such as superposition states and entanglement, in their design.

out a very brief synopsis of the key features of QIT (such as quantum computing and quantum communications) which differentiate QIT from other classical forms of technology. We eschew detailed technical discussion of quantum information processing (for a synopsis, see Nielsen and Chuang (2011), Aaronson (2013)), instead focusing on the most significant characteristics relevant to governance. Firstly, one must specify what it means to classify a technology as *quantum*.²

Since Feynman's conceptual inception of quantum computing as a means of simulating physics with computers Feynman (1982), Preskill (2021), global research and engineering efforts have been focused on developing the theory and hardware for achieving scalable and useful quantum information processing devices, i.e. quantum computers. This search is motivated by the prospect that quantum computers expand the boundaries of computation beyond what is not only currently feasible, but what could ever be achieved using classical information processing. The main distinguishing features of quantum as opposed to classical computation are the availability of (i) superposition states and (ii) entanglement. These two primary quantum phenomena are responsible for the (widely believed) *effective* advantage of quantum computation over classical computation (quantum supremacy). This is the belief that — if certain technical assumptions around scalable fault tolerant quantum computation are met — quantum computing will lead to a drastic expansion in computational resources. As a result, such expansion will (a) enable certain problems that are classically intractable (i.e. cannot be undertaken on any classical computer, no matter its size) to become tractable; and, probably more relevantly, (b) renders practical certain computations which, while theoretically possible for classical computation, in reality exceed available resources on any meaningful spatial or temporal time scale. Quantum sensing Degen et al. (2017) (measurement) and quantum communication (such as quantum key distribution) Rohde (2021) are similarly characterised by enabling activities that are uniquely quantum in nature.³

Understanding the (upside and downside) risks of potential QIT is challenging because the exact form, limitations or constraints on how QIT may be realised are

² Trivially all technology emerges phenomenologically, as the classical world does, from the underlying bedrock of quantum mechanical dynamics. Even rudimentary apparently conventional technologies, such as those facilitating electricity generation, or thermodynamics, involve an element of non-trivial quantum mechanical phenomenology. Technology is more usefully classified as quantum in terms of (a) the design of such technology, namely whether the technology explicitly leverages quantum mechanical (as distinct from classical) dynamics. Even such a design-oriented approach to classification van den Hoven (2017) requires refinement in terms of distinguishing QIT from others. For example, many or even most nuclear, communications and solar technologies, and indeed biotechnologies involve to some extent leveraging quantum effects (such as quantum tunnelling and the quantisation of system energy); thus in this sense, it pays to refine what is meant by 'quantum' in order to motivate quantum governance. Many already have their own well-established governance regimes at international, national and municipal levels (e.g. nuclear governance International Court of Justice (1996); Popp et al. (2016)).

³ Quantum sensing, for example, has the additional impact, again if relevant assumptions are met, in potentially enabling sensing or measurements of physical phenomena which cannot be measured classically — the idea that a more complete picture of quantum phenomena requires quantum sensors itself, reflecting the kernel of Feynman's idea of quantum simulating quantum. The three pillars of QIT, quantum computing, quantum communication and quantum sensing (or metrology) each ground opportunities and risks around which responsive models of governance may be based.

largely unknown. The main goal of QIT research is the development of fully scalable fault-tolerant quantum computers, devices whose computational capacity can scale while remaining robust to errors and noise. However, the current state-of-the-art is a long way from realising such devices. In the field of quantum computation, most demonstrations of high-quality (high fidelity) devices are limited to one- and two-qubit systems or at best so-called noisy intermediate scalable quantum devices (NISQs) (see Preskill (2021) for a recent overview of the state-of-the-art) in the order of tens of qubits. None of these devices exhibits for example the error-correction properties required for scalable quantum information processing. This is a reflection of the immense technical hurdles facing the realisation of QIT. In addition, it is unclear which physical form QIT will likely take in the majority of cases: trapped ion, superconducting, photonic etc., each of which carries its own opportunities and constraints. Nevertheless, consistent with anticipatory thinking on quantum governance, it is useful to spell out the primary impacts or risks if the vaunted ‘best case’ scenarios for QIT are realised. To do so, we need a sense of what form QIT would likely take. To this end, we set out below a few parameters of likely realisations of QIT.

2.2 Technical Impacts of QIT

Fault-tolerant scalable quantum computers (if achievable) are almost certainly only going to be realised in large-scale infrastructural setups within universities, industry or governments. That is, quantum is ‘big science’. It requires large-scale investment and considerable infrastructure to develop and maintain. QIT devices will unlikely be, for example, ubiquitous or portable devices as is the case for classical computing devices such as smartphones, personal computers or laptops. This is directly related to the overheads/infrastructure required to handle the extremely delicate physical conditions that must be maintained to realise quantum effects. The distribution of such QIT devices will probably resemble more super-computing or high-performance computing hubs accessed remotely using cloud-style service infrastructure. Early-stage examples of these types of setups include cloud-quantum offerings by IBM, Amazon, Xanadu and others. This underlying mode of production for QIT then affects who may access QIT resources and how such access would be governed and monitored for example. The availability of superposition states and entanglement contribute to the mooted enhanced computational capacity for QIT (see Perrier (2021) for a review of ethical implications of such issues). Somewhat oversimplifying, these two uniquely quantum properties are at the heart of two of the main impacts of QIT, the impact on computational capacity and communications. With this snapshot of the likely landscape of QIT above, we can proceed to identify a few key impacts that would probably arise if the best-case prognoses of QIT are realised (and assuming that quantum computers do exhibit superior performance relative to classical). We focus on the impacts of quantum computing and quantum communication in relation to QIT.

From a computational standpoint, the primary impact of best-case realisation of QIT would be upon the ability to (a) computationally solve problems which currently cannot be solved efficiently (in a loose sense), i.e. they are too resource intensive or take too long; and (b) solve problems which are intractable, that is, could not

be solved by any classical computer. In general, the availability of superior computational capacity would likely provide an advantage against classical counterparts in a host of domains, including financial, modelling, predictive analytics, engineering, national security and defence. In industry, access to superior computational capacity would provide in principle (*certis paribus*) firms with a competitive advantage (consider financial market trades, product design, chemical synthesis etc.). While having a computational advantage is not necessarily confined to quantum phenomena, the scale at which such QIT devices could outperform classical computers for certain tasks would render this improvement in performance a comparatively unique characteristic of quantum computation. Furthermore, because of the way in which networking quantum computers affects their computational characteristics and capacity, then geostrategic implications may also arise related to how and when/where nation states share computational resources (see Rohde (2021) for a synopsis of such issues).

From a communications' standpoint, the enhanced computational capacity of QIT would have a number of impacts on how communication is undertaken. Two significant impacts upon communication would include (i) the ability to decrypt certain classically encrypted information Gisin et al. (2002), Bernstein and Lange (2017), and (ii) the ability to encrypt data in a way which could not be (or would be unlikely to be) decrypted classically. The ability to decrypt existing or historically classically encrypted data would have profound impacts. Classical encryption is at the bedrock of modern economies and national security apparatuses: financial transactions, credit card transactions, data security etc. all rely upon the inability of classical computers to decrypt (within any meaningful timescale) data that has been encrypted. This is the basis, for example, of RSA and similar encoding protocols. In principle, access to a sufficiently scaled quantum device (under the above assumptions) would enable decryption of such information, rendering it non-confidential. This could and would have profound implications for how information is communicated and in turn upon the fundamental arteries of modern economies and communication networks. Moreover, entanglement-based communication protocols may, if realised, open up enormous potential for a revolution in communications (for example, enabling higher volume or communication across vast distances) Rohde (2021), Preskill (2021). Put another way, if the speculations about QIT capacity are realised, then it would enable those with access to significantly affect modern information systems or develop superior information architectures. Indeed, this is the primary reason why most quantum research has been thus far, directly or indirectly, funded via governments and associated national defence institutions. We explore this particular impact and its associated risk in detail further on. Such considerations then bear upon questions of how QIT should be developed, whom should have access and the types of use-cases available. For example, permitting mass consumer-access to QIT in a way that would enable mass decryption of classically encrypted data would likely be unacceptable. These are all core issues for the governance of QIT.

Whether such impacts identified above are realised is an open question: we are far from such scenarios currently. Nevertheless, such potential impacts arise as a result of the unique features of quantum information processing as distinct from classical. Thus, it can be said that QIT, in particular cases, does give rise to uniquely *quantum*

impacts or risks per se. These two sets of impacts would in turn likely give rise to normative or governance imperatives seeking to control the use of technology via imposing obligations upon quantum stakeholders related to the development, distribution and use of such technology. The quantum governance stack we articulate below aims to provide a blueprint for reasoning through who should respond to such impacts and means by which they can do so. It is intended to provide a more granular approach which enables analysis of how these and other implications of QIT may be matched to stakeholder interests, rights and duties and appropriate governance instruments. We discuss such impacts in more detail in later sections of the article (see Table 2 below for an example).

2.3 Quantum Objectives and Risks

Our approach to QIT governance proceeds by taxonomically mapping governance objectives, such as QIT development or ensuring secure communications, to the interests, rights and objectives of stakeholders. Governance of QIT incorporates maintaining or establishing conditions that facilitate and foster the development of QIT. Governance should not be narrowly construed as merely managing or responding to negative risks. Positive objectives that governance should facilitate can be categorised into (i) *development*, facilitating the development of scalable fault-tolerant quantum computer(s) (SFTQC); (ii) *infrastructure*, including for networked SFTQC such as for the quantum internet; (iii) *security*, covering primarily data security and encryption issues; and (iv) *coordination*, covering the use of governance instruments to coordinate behaviour among stakeholders (for example, public-private coordination, or coordination among states, or standardisation and interoperability of technology protocols). Governance must also be cognisant of the milestones and status of QIT development. In this work, rather than seek to enumerate all (speculative) risks of QIT, we instead focus on how existing governance responses could identify, manage and control for such risks as they emerge.⁴

2.4 Development as Objective and Risk

Any approach to quantum governance must factor in the primary objective of developing QIT itself. The development of technology should not be considered separate or parallel to governance. Rather, it should be considered as a primary objective itself to be compared with other fundamental normative objectives, such as maximising social welfare. QIT is technically complex, challenging to develop and uncertain in prospect. Despite enormous advances in QIT over the last several decades, quantum computational devices remain at experimental ‘proof of concept’ stages, largely confined to a few qubits or

⁴ As we discuss, governance of technology will differ for different stages in its development. While theoretical algorithm development for quantum systems continues to progress, current engineered QIT remains at the prototypical noisy intermediate stage of development, with considerable uncertainty as to not only the likely form of any SFTQC but whether a sufficiently scalable quantum computer is actually attainable.

in the order of tens of qubits with limited capacity to undertake meaningful tasks that would not currently be more efficiently undertaken using classical devices. Furthermore, there remains considerable uncertainty regarding the likely form that quantum hardware will ultimately manifest in: while a variety of candidate architectures, such as photonic, trapped ion, superconductor-based, offer promising results, it is unclear as to which of these, if any, will give rise to both sufficiently *scalable* and *fault tolerant* quantum information processing. Such uncertainty about the likely form of SFTQC (indeed whether it is truly achievable) can be reasonably characterised as *development risk*, reflective of how stakeholders involved in QIT must make resource allocation decisions and set priorities in the face of considerable uncertainty (for example, previously mooted topological approaches to quantum computing which received considerable investment Giacomini (2016) have thus far failed to meet certain key thresholds Ball (2021)). Development risks are crucial considerations in any approach that seeks to govern QIT and how it is governed. Put another way, the upsides of technology can and should be framed in terms of risk. Despite its occasional pejorative framing, risk includes *upside* risk, the uncertainty or variation in outcomes leading beneficial or desirable outcomes. By factoring in the uncertainty around development via such a risk-based set of measures, governance of QIT can provide a stronger basis for comparing costs and benefits of the development of QIT. Development is an objective and a risk. Moreover, development risk reflects issues at play in the Collingridge dilemma Collingridge (1980). The exact directions of how a nascent technology will develop are unknown at early stages. Stakeholders cannot usually forecast how a technology should optimally develop and thus attempts to impose governance or even sets of guiding principles early-on can risk frustrating development. By framing development using risk-based analysis, stakeholders can assess how proposed governance responses may increase or decrease or change the uncertainty and prospects for QIT development.

2.5 Dual Use Risks

Other development-related (but not solely technical) risk categories relevant to quantum governance of particular importance include ‘dual use’ risks. These emerge when expected utilities from technological use or development are both positive and negative, i.e. potentially beneficial or detrimental Forge (2010). Dual use risks in the quantum area have been primarily focused on geostrategic risks that may emerge from dissemination or distribution of security-impactful technologies to potential adversaries. A primary focus of quantum computing risks Fedorov et al. (2018), Charu (2008) lies in the potential impact of enabling decryption of certain classically encrypted data. The heightened investment in QIT development by governments on national security grounds evidences at least the prevalence of the perception that such risks are likely to become material if QIT can be realised.⁵ Dual-use

⁵ More recently Hurst (2022); Global Industry Analysts (2021), a number of companies have marketed ‘post-quantum’ encryption Bernstein and Lange (2017) and other related techniques as a means of encrypting data today in a way that could not be decrypted if a sufficiently scalable quantum computer were to become available in the future.

technologies pose conundrums for stakeholders seeking governance responses. On the one hand, international collaboration is at the epicentre of QIT development: quantum is a truly international endeavour. While on the other, QIT research is already considered as highly sensitive, attracting governance responses such as export controls and limitations on collaboration among strategic adversaries. For example, China is emerging as a global quantum powerhouse when it comes to both theoretical and applied QIT. However, strategic competition and mistrust between China and the West is already posing limitations on how researchers in both arenas may collaborate. Lessening the degree of international collaboration on QIT will impact the development trajectories of the technology. Conversely, strategic considerations are important and ultimately take priority in terms of national interest. This presents stakeholders involved in governance with challenging multi-objective optimisation problems: how to optimise for international development of QIT while subject to geopolitical constraints on collaboration. This is a feature not just for government-funded or developed technology, but also for multinational firms operating across the strategic divide. As such, factoring in and potentially solving for dual-use objectives will be a primary feature of much governance for stakeholders with interests or operations across borders.

3 Governance Models

3.1 Overview

Framing the objectives of and process of governance is itself a complex and multifaceted process, contingent upon underlying values, institutional and social factors and stakeholder interests. Quantum governance comprises heterogeneous objectives, many of which are not necessarily consistent with each other or in form and substance require consideration of trade-offs and compromise.⁶ In this work, we organise the governance stack around different governance instruments for managing multiple stakeholder rights, interests, duties and obligations. We first provide a high-level overview of the stakeholder-driven model for governance of QIT implicit in the governance stack. We then proceed to elaborate on each step of the proposed model and different parts of the governance stack in later sections. We do so in order to adopt an instrumentalist Christopher (2019) approach to governance, concentrating upon the types of instruments, such as treaties, legislation, protocols, policies and procedures, which can be used to regulate (formally and informally)

⁶ At the more abstract Rawlsian end of the spectrum Rawls (1999, 1993), governance concerns theories of justice and means of reaching a functional equilibrium among competing or complementary stakeholders within a policy. Governance thus concerns rights and obligations of participant stakeholders within a multiplicitous polity, characterised by individual and collective interests and preferences. The objectives of governance are thus naturally neither consistent among such diverse constituencies nor conceptually self-consistent. Governance involves decision-procedures or at the very least the formation of judgments that both discursively classify topics or subjects, prescriptions and proscriptions on how such stakeholders or agents should act or omit to act.

relations among stakeholders, including by providing means by which rights and obligations are negotiated and disputes or differences resolved. In concrete terms, our approach involves (1) identifying categories of ‘quantum stakeholders’; (2) engaging with stakeholders around QIT; (3) identifying the interests (objectives), rights and duties of such stakeholders; (4) identifying how QIT affects such stakeholder rights and what stakeholder duties are with respect to QIT; (5) undertaking risk management assessments of such impacts; (6) identifying existing or newly required governance instruments appropriate or relevant to managing, mitigating and controlling such risks; (7) drafting or building such instruments in a consultative manner; (8) reviewing such proposed instruments for consistency, feasibility and checking they are fit for purpose and (9) finalising such governance architecture along with undertaking its implementation (involving monitoring, reporting, auditing). Such QIT governance procedures are for use by multiple stakeholders (not just governments) and reflect an adaptation of typical deliberative and inclusive governance. A diagram of this approach is set out in Fig. 1.⁷ The underlying idea of our quantum governance stack model is that the procedure summarised in Fig. 1 can be adopted by the various stakeholders identified in Fig. 2. Each stakeholder can adopt the method as a way of identifying the interests, rights and responsibilities of itself and other stakeholders whose actions it may affect. The types of instruments such stakeholders may respond to such risks are set out in the boxes in Fig. 2. For each stakeholder group, we run through examples of existing governance instruments which can provide examples to draw upon for QIT governance. For example, in Fig. 3, we provide a diagrammatic summary of how firms adopting risk-management techniques may factor in QIT risks into their overall governance response.

3.2 A Duties and Rights-Based Approach

The practical basis for governance of QIT is then usefully parsed by a taxonomic classification of the objectives, rights, duties and obligations of different quantum stakeholder groups. We pitch such an approach as the *duties and rights-based* approach of quantum governance: any quantum governance initiative must clearly articulate the rights, interests and duties of stakeholders. Such an account aims to provide pragmatic guidance or idealised models of governance for such stakeholders. It provides examples of the ways in which governance practices can be embedded within the specific priorities of stakeholders themselves. A duties-based approach also enables for example other stakeholders to assess their rights and duties vis-à-vis other stakeholders of different categories. It is also useful because it enables obligations and rights to be mapped as relations among stakeholders who in turn will have their own objectives and interests. Stakeholders may have rights, say

⁷ Throughout this article, for concision and clarity, we deliberately conceptually group ‘objectives’ of a stakeholder with the significant ‘risks’ to be managed on the basis that doing so more easily enables us to render how particular instruments, such as treaties or policies, serve complementary functions in terms of facilitating objective attainment and management of risks.

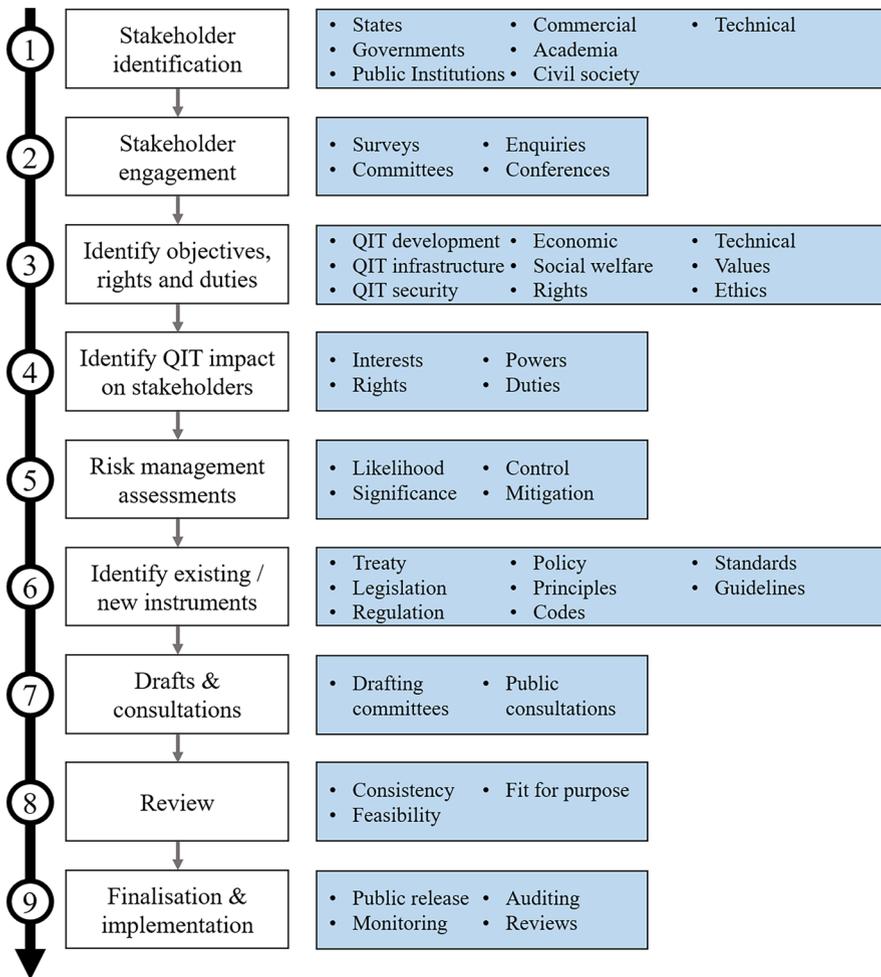


Fig. 1 A stepwise QIT governance process: (1) identification of stakeholders, (2) engagement with stakeholders via surveys to help (3) identify objectives, rights and duties of stakeholders relating to QIT; (4) the impact of QIT on stakeholders is then assessed with (5) a formal risk assessment of such impacts undertaken; (6) identification of existing or new governance instruments to manage such risks occurs followed by (7) draft/deliberative consultation to prepare the governance instrument (e.g. legislation, policy, principles), followed by (8) review and (9) implementation

to privacy, but such rights may be manifest as the obligation of a government to an individual, rather than as between individuals. Similarly, treaties may espouse rights of individuals, but not commensurate obligations to manifest such rights as between individuals using QIT. In formal jurisprudence, duties-based approaches are presaged by the concept of legal personality, recognised subjects at law, who may be accorded obligations or rights such that they have standing to seek enforcement of

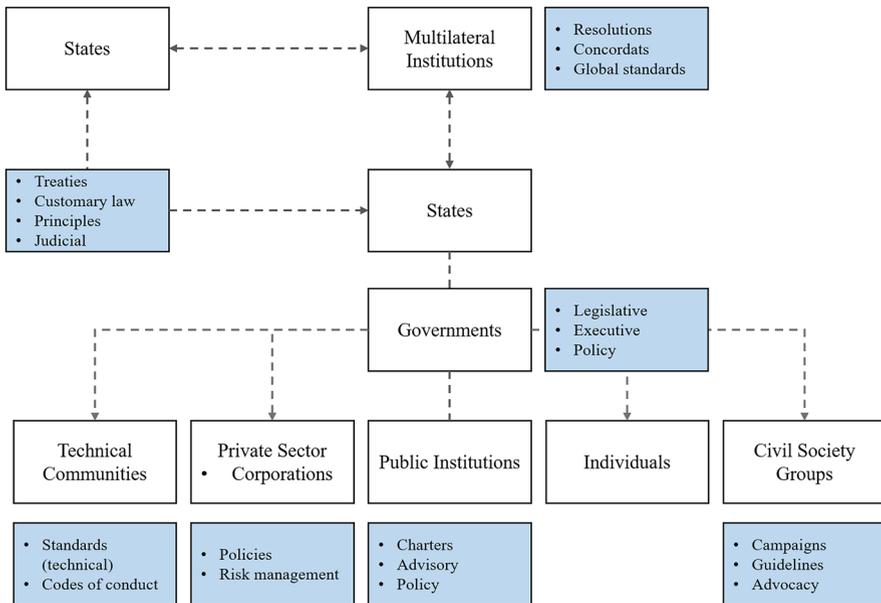


Fig. 2 Quantum governance stack: (i) inter-state relations are mediated via public international law or multilateral instruments; (ii) government instruments include legislation, executive instruments or policy. Within states, various institutions may contribute to the governance stack, including (iii) technical communities, (iv) commercial private sector organisations, (v) public institutions, (vi) individuals and (vii) civil society groups

such rights according to law. In a normative context, such stakeholder identification is also important in establishing who may ‘speak on behalf’ of communities.⁸

3.3 Formal and Informal Governance

Typical paradigms of governance contrast ‘hard’ or ‘formal’ approaches, characterised by formal legal obligations, prescription of specific procedures or regulatory criteria and delegated administrative oversight Abbott and Snidal (2000), with ‘soft’ or ‘informal’ governance, characterised by normative or unenforceable instruments. Governance literature often represents regulation along such a spectrum Ayres and Braithwaite (1992) with ‘harder’ or more formal governance characterised by formal instruments (e.g. treaties or legislation, dependent upon the relevant governance hierarchy), followed by a mixture of policy-driven government regulation and

⁸ A duties-based approach is advisable because not all QIT-related risks are the responsibility of all stakeholders to manage: the types of risks a quantum engineer should actively manage will differ from those of a policy officer or legislator. Often ethics’ guidelines or frameworks fail to set out a division of labour, relying instead on abstract principles essentially of improving social welfare.

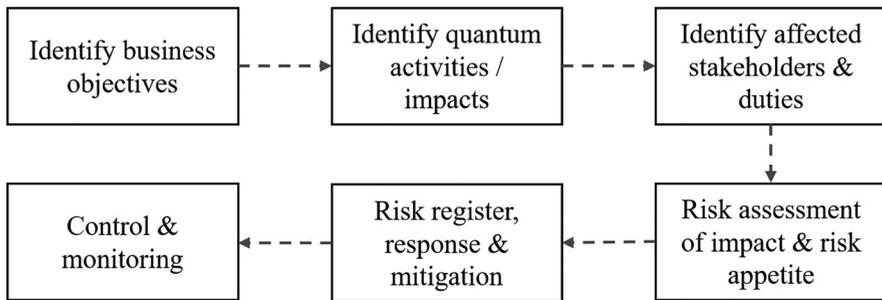


Fig. 3 Quantum risk management flow for commercial and private sector stakeholders

instruments to motivate private compliance (such as sanctions, punishments or incentives). Softer methods involve, at the communal level, industry codes or conduct or at the firm level Gunningham et al. (1998), Gunningham and Rees (1997), integrated risk management frameworks. Such methods are relevant considerations at step 6 in the governance stack model as set out in Fig. 1 for example.⁹ QIT governance therefore necessitates a consideration of formal and informal instruments.¹⁰

Instruments of governance can take a variety of forms. These include (i) legislation, treaties, regulatory oversight and advice bodies; (ii) formal stakeholder consultation; (iii) national strategies, agendas and plans; (iv) policy intelligence (evaluations and forecasts); (v) networking and collaborative platforms; (vi) standardisation procedures; and (vi) public instrumentalities. Idealised models of QIT should recognise the importance of socialising the rationales, motivations and drivers of governance among populations and stakeholder communities. Doing so is important to both (x) the process by which governance is developed and evolves and (y) the adherence to and enforceability of governance that is implemented, such as via legislation. Well-established deliberative procedures in modern democratic nations Dryzek (2012) are, when they do function, suited to addressing governance issues in QIT. Such practices tend to involve alerting governmental or parliamentary stakeholders to issues, either via expert or industry lobbying or community activism. This is followed by enquiries

⁹ Soft governance approaches, such as principles or other instruments that fall short of formal enforceability do obviously have the potential to exert influence beyond the jurisdictional limits of legislation Marchant et al. (2011), though it should be noted that formal legislative-style instruments can themselves exert such tacit or soft-power influence (and routinely do). While principles, governance frameworks and the like serve an important purpose, ultimately they lack the formal (potential) enforceability that characterises actual regulation Bernstein (2011). Other problems with self-regulation or relying on such soft approaches to governance include (i) illegitimacy as a result of irreconcilable conflicts of interest in self-regulation, (ii) erosion of public trust subordinated to firm or industry imperatives Karlsson-Vinkhuyzen and Vihma (2009) and (iii) inconsistency of approach or outcome which itself can lead to disruption of other imperatives, such as certainty needed for industry coordination.

¹⁰ (a) Formal characteristics encompass formal (that is, *enforceable*) obligations upon stakeholders in law, regulation or policy to assess, analyse or conduct risk assessments (and act accordingly) in relation to material risks that may arise due to a stakeholder's involvement with or use of QIT; and (b) informal elements encompass heuristics, strategy or guiding principles (not specific to quantum contexts per se) which steer how technology is used, the allocation of resources and distribution of technologies.

or committees that seek to examine the issues and conduct, to differing degrees of formality, usually qualitative or heuristic risk-assessments. These findings can then form the basis for recommendations and regulatory responses ranging from policy adjustments to legislative proposals. Thus, the general policy transmission mechanism Rosen and Gayer (2010), Fisher et al. (2006), Richardson (2003) provides a ready-made and tested method for handling responses to the effects of QIT. Deliberative governance is also central to how other institutions and stakeholders, such as private sector, multilateral or civil society groups respond to QIT. As noted in Holter et al. (2021), developing stakeholder engagement strategies is important in any approach to responsible innovation in the quantum sector, particularly as a method to synthesise or resolve conflict among competing objectives. Deliberative approaches to governance are crucial for effective governance of QIT at each level in the quantum governance stack.

3.4 Principles, Prescriptions and the Precautionary Principle

The ideal form of QIT governance varies between differing degrees of specificity and abstraction, involving both prescriptive and principles-based approaches. Governance requires auditing its effectiveness over time Hemenway (1980). For QIT (as others), specification of purpose or outcomes sought along with prescribing how technology should function is therefore central to the auditing and controllability of technology. Yet the extent to which such requirements can be prescribed (including in advance when the technology remains unproven) is uncertain. The challenge of specificity and generality manifests the uncertainty inherent in technological innovation Paddock (2010), with early iterations of regulation having potentially significant effects in shaping its development. The anticipatory regulation of QIT, legislatively and normatively, is an exemplary case of regulation in the face of uncertainty. QIT, while promising, are several years' from realisation with considerable uncertainty over the developmental pathways and manifestations the technology will take. Quantum governance therefore requires careful consideration of the application of the precautionary principle Harding and Fisher (1999), the form and manner in which must balance competing trade-offs of anticipatory regulation while fostering research and development Mandel (2009).¹¹¹²

One of the key elements of development risk is how governance responses can handle developmental uncertainty. A quantum governance stack approach (as we set-out herein) is particularly adapted to governance in the face of uncertainty. It

¹¹ Such 'pacing problems' where innovation outpaces regulatory oversight themselves may often require both a soft-regulatory and technological set of solutions themselves Marchant et al. (2011).

¹² Applications of the precautionary principle dovetail into broader questions around anticipatory governance that trades the need for anticipatory regulation of material technological risks before they become too embedded or difficult to manage against thwarting the benefits of such technological development itself Guston (2014). In technology governance, especially with prospective or as yet unproven technologies, there is a trade-off between the desire for prescriptive or pre-emptive governance and over-regulation which may interfere with innovation or misweight risks (such as downside or pejorative characterisations of technology) Graham (2004); Einstein (2014). Such a dilemma is sometimes referred to as the 'Collingridge dilemma' Collingridge (1980), where early-stage or anticipatory regulation faces difficulty in identifying longer-term impacts or risks of technology.

proceeds via an understanding of stakeholder rights, interests and duties and how these fit with overall objectives of quantum development. Thus at this early stage of quantum development, activities like carrying out audits or taxonomies of quantum stakeholders as envisaged below help to specify the particular objectives, motivations and interests of stakeholders at this early stage. Such methodologies would also enable mapping of likely *stakeholder trajectories*, that is, likely ways in which stakeholder interests for example may evolve as the technology evolves. This might include how the interests of a quantum startup differ as their technology matures, how the interests of an academic research institution evolve as the quantum sector/industry around them develops (see for example Caltech's partnership with Amazon) or how and where quantum investment may be prioritised by governments as the technology reaches various stages of maturity. By doing so, hard or soft governance responses (and instruments by which they occur) can be adapted appropriately to the degree of uncertainty in QIT development and stakeholder interests. Indeed given the considerable uncertainty of the developmental trajectory of QIT, soft-governance approaches are particularly useful instruments given their flexibility. Thus at early stages of QIT, policy intelligence or other soft-instrumentalist approaches such as internal policies (see Sects. 5.3 to 5.5 below) can be used to, for example, require consideration by QIT developers of potential impacts early-on. Other soft governance instruments, such as principles developed by civil society groups (e.g. see Sect. 5.6 below) or within academia can also be useful ways of shaping normative development contexts without imposing hard-instrument governance that may be inappropriate or stifle innovation. Moreover, as we argue below, empirical approaches to governance can too be important elements in managing uncertainty in how a technology like QIT develops. Such approaches involve developing dynamic governance models that respond, adjust and update according to the changing status and impact of technology.

3.5 Risk-Based Models

Governance principles and frameworks usually, owing to their generality and the discursive environments in which they are produced, subsist at a level of abstraction beyond operational specificity. A commonplace means of bridging the semantic gap between discursive governance values and operational task, goal and assurance processes is via risk management protocols. These provide variegated approaches to management of risk by or related to institutions, organisations and projects. A risk-management approach specifies methods and decision procedures for how abstract objectives, such as ethical constraints, may be operationalised by stakeholders. The use of risk-management techniques is integrated into our proposed quantum governance stack process as item 5 in Fig. 1 for very specific reasons. Risk management is a mature, ubiquitous and well-known set of techniques familiar to a plethora of stakeholders throughout governance hierarchies and within firms. Thus, it provides an ideal set of familiar methods which can incorporate QIT risks. In modern risk management literature, risk concerns decision-making under uncertainty and the effect of uncertainty upon objectives Purdy (2010). It encompasses both upside

(positive) and downside (negative) risks. Risk management also ties in closely with multilateral governance in the form of international standards, including the International Standards Organisation (ISO). For example, ISO 31000 Purdy (2010) and related risk management protocols set out practical guidelines for risk assessment, management of legal risk and institutional risk.¹³ These protocols Calder (2019) provide ready-made and adaptable means applicable to identifying and responding to risks including those associated with unique features of QIT. Risk management for QIT therefore requires operationally (i) an accounting of the objectives of the particular institution or activity (e.g. the policy objectives sought or the business objectives), (ii) how constraints are encoded within those objectives. Moreover, such an approach to governance in effect requires an accounting (at each level within the hierarchy) of heterogeneous objectives. this in turn enables (x) identification of how those objectives give rise to identifiable *rights* different stakeholders (be they individual, collective or other) and concurrently (y) how such normative rights then in turn give rise to specific, identifiable and proportionate *duties* of stakeholders as means by which those rights, objectives or outcomes are realised to be identified (such as the duties of say researchers in quantum theory, or engineers, or managers or policy makers).¹⁴ Pre-existing risk management procedures which are already commonplace and standard means of operationalising governance and executing on objectives can be adapted for quantum-specific risks.

4 Technology Governance Models

4.1 Norms, Ethics and Values

Technology governance is by its nature entwined with normative and ethical assumptions about the types of objectives or outcomes that such governance seeks to achieve. Governance inherently expresses a preference (even if abstract) for one state of affairs or set of duties or obligations over another. The concept of embedding values principles or moral/ethics within technological design and governance is common across related fields that touch upon technology governance. Examples include statements of purpose or intent within formal governance instruments

¹³ Such approaches emphasise risk management frameworks and risk management processes, namely the ways in which (i) systematic application of policies/procedures affects (i) communication, consultation, analysis, monitoring and review of risk, maintaining of risk registers and accountability/allocation of oversight responsibilities. For example, ISO 31000 sets out recommended or ideal institutional hierarchies and divisions of labour and responsibility for different parts of an organisational hierarchy, such as (i) executive level stakeholders, (ii) enterprise risk management groups, (iii) risk analysts and management officers, (iv) line managers and project managers and (v) auditors and compliance functionaries.

¹⁴ Different individuals or stakeholders will have different roles and degrees of responsibility for risk management; usually in organisations this is managed by way of risk and compliance functions, such as risk and compliance committees; with delegated authority to specific risk managers. In addition, typically risk management then manifests in policies and procedures that to which, for example, individual employees or agents must adhere. An example is within financial institutions, which (as a result of supervening regulation) have complex and developed anti-money laundering and sanctions-based risk management divisions and procedures.

(e.g. legislation or treaties Vienna (1969)), case law on technological governance, scholarly jurisprudence Moses (2017), Van Grembergen (2004), Winickoff and Pfothenauer (2018), design ethics literature Hoven et al. (2015), and ethics' literature The Forum Network OECD (2017), Friedman (2008), Friedman et al. (2006), Lessig (2000). Ethical approaches to embedding constraints within QIT are understandably often compared with analogous and burgeoning literature on the ethics of artificial intelligence. It is important that assumptions about what values ought to be enshrined in governance or technology designed are themselves debated.¹⁵ As we set out in item 3 of our quantum governance stack process in Fig. 1, ethics forms an important consideration when identifying the objectives, rights and duties of stakeholders. This is because often stakeholder interests are encoded in collective norms or ethical principles prevalent within societal responses to governance. Ethical statements or principles, for example, can encode certain values of stakeholders subscribing to such principles which otherwise may not be apparent from other analyses. Governance responses should consider prevailing ethical contexts relating to, for example, technological regulation, which entails considering prevailing ethical standards in like technologies (such as AI).

A recent first-pass at a set of governance principles for quantum computing is the World Economic Forum's *Quantum Computing Governance Principles* World Economic Forum (2022) which set out a set of guiding taxonomy and set of principles to inform quantum stakeholders' governance activities. These high-level principles are addressed to different stakeholder groups, such as governments, academic institutions, corporations and individuals. The principles are structured around a number of core ethical values, which are then explored via a focused analysis on different themes related to quantum governance. These include (i) transformative impact, (ii) innovation, (iii) development, (iv) privacy and security and (v) standardisation, within which objectives, opportunities, risks and recommendations are provided. The role of values in governance as abstract guiding heuristics is a feature of governance and risk frameworks generally. Principles of social benefit, accountability and transparency, equity and access, harm-minimisation tend to be ingrained in many formal and informal instruments Dworkin (1988), Raz (1986). However, governance also involves trade-offs with other stakeholder interests. Of course the nature of 'values' let alone which values or outcomes should be prioritised are contestable propositions. While abstract and sweeping statements about technology only being used for 'social good' or to meet some standard of 'fairness' are commonplace, in practice, the appropriateness of the values that governance might seek to encode is contested either in theory or indeed in practice. Moreover, use, deployment and dissemination of technology involves trade-offs in terms of opportunity costs. So too do decisions over

¹⁵ QIT-specific governance will also benefit from gap analysis that identifies gaps World Economic Forum (2020) including (i) limited or lack of regulation; (ii) adverse effects of technology (through use or misuse); (iii) absence of clear chains of accountability or mechanisms to attribute liability; (iv) methods to facilitate explainability and interpretability; (v) access to and use of QIT by law enforcement; (vi) privacy, data sharing and cybersecurity; (vii) controllability and the extent of human supervision. Other multilateral gaps also include inconsistent standards, protocols or governance regimes across borders.

resource allocation given the desire to reconcile scarcity of technology resources with demand for resources.¹⁶

4.2 Empirical and Responsive Governance

QIT governance methods must also be dynamic, both guiding and responding to the evolution of QIT. Fundamentally this necessitates an empirical and experimental approach to ensure, as much as possible, that governance remains agile, responsive and reflective of overall priorities and objectives. Such ‘responsive regulation’ paradigms Ayres and Braithwaite (1992), Black and Baldwin (2010) aim to bypass typical debates over prescriptive (‘command and control’) approaches to regulation on the one hand and *laissez-faire* deregulated approaches on the other. Approaches involving decentralised regulation Black (2001) are responses to the fact that the complexity of governance means that no prescriptive model can hope to account for all possible or even all realistic technological evolutions of circumstances Baldwin et al. (2010). Importantly the coordination inimical to governance relies upon the self-policing behaviour of agents, institutions and stakeholders involved; hence, deliberative and inclusive models of governance formation are critical for effective regulation of stakeholder rights.¹⁷ Responsive governance is evolutionary, based on estimations of the types of prospective risks envisaged at one stage of QIT development will in all likelihood require revision as QIT develops.¹⁸¹⁹

¹⁶ From a stakeholder and rights-based perspective, finding compromises among the values, rights and obligations of different stakeholders itself necessitates a deliberate process according to which governance equilibria may be found. This is the lifeblood of organised polities via the deliberative governance institutions of parliaments and so on globally. Such an approach is also philosophically essentially a Rawlsian framing of governance Rawls (1999), whereby while stakeholder constituencies may hold dear certain values, ultimately the encoding of values in governance reflects compromises via politically mandated procedures for resolution of differences. Thus, values such as ‘social good’ (or maximising social welfare), ‘equality and fairness’ (including equal opportunity or anti-discrimination principles), and ‘interpretability’ of technology (such as how explainable causal relations are) tend to be subject to exceptions and trade-offs. Finding global and municipal equilibria using values-based approaches to quantum governance ideally involves leveraging existing deliberative mechanisms whereby such values are themselves debated among stakeholders whose behaviour is to be subject of such governance. Interestingly, while interpretability and explainability imperatives are usually advocated on the basis of moral principles of autonomy and informed consent of affected stakeholders, there are parallels with the need for controllability and the ability to explain how or why technology functions in a particular way.

¹⁷ In this sense, such governance models tacitly align to some degree with modern critiques of power Foucault and Sheridan (2002) where institutional (and regulatory) power is mediated and indeed substantiated by the self-policing of agents Ayres and Braithwaite (1992) which may remain, albeit, motivated by the threat of state enforcement Stilgoe et al. (2013).

¹⁸ As a result, modern governance models tend to be built frameworks that recognise the importance of risk-management based approaches Sinclair (1997), varying in their degree of quantitative formalism. Under such models (which we explore throughout), risk management and assessment would involve both (i) *hierarchical* and (ii) *delegated* decision-making. Such modern risk-management-based approaches manifest commonly within, for example, administrative law in common law and code-based jurisdictions, where risk assessments and decision-making is based upon chains of delegated authority, enabling lower-impact risk assessment, monitoring, remediation or control by less senior agents or committees, while higher-risk decisions are assessed and managed by superior decision-making apparatuses, such as governance committees, compliance committees, departmental heads or even government cabinets.

¹⁹ Such factors also motivate consideration of how regulatory technology (regtech) itself must be developed in order to fulfil the coordinating, managerial, surveillance and enforcement imperatives of QIT

Table 1 Quantum governance instruments for international, national and private stakeholder contexts

Quantum governance instruments		
Sector	Instruments	
1.	International	<p><i>Public international law:</i></p> <ul style="list-style-type: none"> • Treaties governing use, classification, development and distribution of QIT • Concordats etc. <p><i>Multilateral institutions:</i></p> <ul style="list-style-type: none"> • Institutions managing/governing QIT • Multilateral fora for quantum governance • Resolutions, memoranda, principles
2.	National	<p><i>Legislation/law:</i></p> <ul style="list-style-type: none"> • Legislation covering use of technologies applicable to quantum • Quantum-specific legislation • Common law and jurisprudential principles <p><i>Institutions:</i></p> <ul style="list-style-type: none"> • National quantum coordinating institutions
3.	Private	<p><i>Quantum risk protocols:</i></p> <ul style="list-style-type: none"> • Protocols covering upside and downside risks of quantum computing and related technologies • Adaptation of existing risk protocols and standards for QIT and institutions <p><i>Quantum transformation management programs:</i></p> <ul style="list-style-type: none"> • Frameworks to manage transformational impacts of QIT on different constituencies • Guidelines for balancing opportunities and risks

5 Quantum Governance Stack

Having reviewed the conceptual underpinnings of QIT governance in the context of technology governance overall, we now detail different features of the quantum governance stack. We proceed by focusing on different stakeholder constituencies, such as states, individuals and commercial organisations, considering their objectives, risks, rights, interests duties and obligations with respect to QIT. Such a stakeholder-centric approach argues for the importance of deliberative governance that takes into account other stakeholder interests and obligations. Stakeholder categories are not necessarily exclusive. For example, states are the primary actors in all formally enforceable governance, but we for convenience distinguish between states vis-à-vis international governance instruments and municipal governments. For each stakeholder, a number of their key objectives and risks with respect to QIT are identified, along with primary governance instruments for regulating their activities, their mooted rights and duties. A diagram of the stack is shown in Fig. 2 and a summary of relevant governance features is set out in Table 3. Some key types of instruments are set out in Table 1.

Footnote 19 (continued)

governance. As a number of scholars note Brownsword (2008), regtech is driven primarily by the complexity challenge posed by technology, particularly information-driven technologies Arner et al. (2016); Anagnostopoulos (2018) whose dynamism and alacrity by comparison with slow-moving regulatory responses present additional risks to be managed.

5.1 International Governance

5.1.1 States and Public International Law

Existing international legal frameworks, including treaties, provide a basis for comparison and idealised governance of QIT at the transnational level. In this section, we list a few key international instruments germane to quantum governance. At an international level, states are the primary actors for which the primary governance mechanisms are (i) formal public international law instruments and (ii) multilateral institutions. The extent to which public international law does or should address governance of QIT is an important consideration of international collaboration. Public international law sets out a legal framework for relations among nation states. It is formally regarded as subsisting in four primary sources Crawford and Brownlie (2019), Zimmermann (2019): international treaties and conventions (expressing rules recognised by states), customary law, general principles recognised by states and judicial decisions, which evidence greater or lesser degrees of normative consensus among nation states. Public international law manifests primarily via *states* (and their controlling governments) as the relevant primary stakeholders whose rights, duties and obligations are framed within public international law instruments. Duties are generally imposed on states, but where rights may be expressed in terms of the rights of other stakeholders, such as states, institutions (e.g. international institutions) or sometimes individuals. Public international law or treaties regarding QIT will concern primarily regulation of quantum-related activity among states, though such instruments may in principle also establish or normatively frame rights of others, such as individuals.

As states are the primary agents in governance (both nationally and internationally) and the central actors in the development and implementation of both formal and informal governance instruments, state interests tend to be paramount considerations.²⁰ At a high level, the motivating factors for supranational governance of QIT arise primarily from the following imperatives: (i) geostrategic, namely managing the strategic risks (both upside and downside) of QIT; (ii) developmental and distributional efficiency, namely that quantum innovation (as with any other) benefits from greater cross-national and cross-disciplinary collaboration; and (iii) maintenance of agreed fundamental individual rights. Furthermore, the increasing reliance of state security apparatuses upon information security Schmitt (2021) renders modern information communication technologies (ICT) essential to the maintenance of such objectives. The unique features of QIT would potentially impact such core existential ICT functionality of states and therefore core state objectives. Other impacts and risks of mooted QIT, such as how the production, use and distribution of such technologies may impact (adversely or otherwise) the social welfare of its citizens, or meet ethical criteria, while important to state interests, can be classified as indirect interests to

²⁰ Of course states as institutional formations themselves are compositions of multiplicities of stakeholders, from formally recognised citizens or individuals to other institutions. The primary objectives of states of course relate to maintaining their sovereignty, followed by duties to their citizens and other constituencies in terms of security, social welfare and so on. In the modern era, information architecture is a core component of facilitating all, if not all, state objectives.

states in themselves, being relevant to the interests of state constituencies. States share development objectives, namely their interests in terms of national security, their economic and other core interests stand to benefit from access to and use of QIT.

Formal state instruments for quantum governance would follow the typical jurisprudential demarcation between (a) public international law instruments as between states (treaties, customary international law etc.) and (b) municipal governance instruments via legislative and executive capacities (addressed below). States already have sophisticated means of addressing novel technological developments.²¹ A key element (as discussed) is the deliberative policy process behind the development and implementation of quantum governance instruments. We examine two examples below.²²

5.1.2 Case Study: Nuclear Non-Proliferation

The development and implementation of the *1970 Treaty on the Non-Proliferation of Nuclear Weapons* (TNN) Treaty (1970), Popp et al. (2016) provides an example of a formal international technology governance instrument (a treaty) governing the use of a highly sensitive and geostrategic technology (nuclear weapons) which has been relatively successful. While quantum information processing will not directly have the potential for existential risk posed by nuclear weapons, SFTQC-based technologies are expected (if realised) to be a core component of state national security infrastructure. Moreover (as we discuss below), given the existential reliance of modern national security apparatuses on information, it is arguable that maintaining information security (and indeed targeting that of adversaries) may be afforded existential-level security prioritisation. The lessons from the TNN are manifold but for QIT governance, importantly, the TNN represents twofold procedural success: (i) that the TNN was able to be legislatively (via treaty) agreed through protracted deliberative procedures in a highly adversarial setting with limited stakeholder communication and trust; and (ii) perhaps even more remarkably, the fact that the key terms of the TNN, namely the reduction in nuclear weapon stockpiles, together with nuclear weapons' control protocols, were able to be implemented within the adversarial climate of the Cold War. In particular, TNN governance provides a method for verification (auditing) regime for such highly sensitive technologies which could be

²¹ In formal public international law, states as the effective 'legal persons' the subject of such law are discursively construed in a way that affords them rights and imposes upon them obligations. State obligations and duties are often framed in terms of duties towards individuals or their citizens, or other constituencies (such as communities or sectors). This is typically manifest at an international level via various rights-based charters (such as various UN rights' declarations) and municipally via enactment of laws either ratifying such rights or separately establishing them. The potential ethical impact of QIT on individual rights Perrier (2021); Johnson (2018) has led some scholars to argue Kop (2021) for the codification of ethical principles in a treaty format as a means of responding to such risks.

²² As with all governance, states are the primary drivers of the processes by which governance is enacted, principally through legislative and executive means. Furthermore, states also perform an important function in facilitating other stakeholder formation and deliberation, including promoting or funding civil society groups, technical communities and or public funded projects which can contribute to the development of quantum governance. For example, as touched on below, the NQIA includes as part of its remit the development of certain technical standards to govern the use of QIT, in effect contributing to the governance ecosystem as a result. We discuss such deliberative processes via governments below.

adapted for QIT auditing (for example, how to verify a state's quantum infrastructure is not being used in proscribed ways).

5.1.3 Case Study: EU AI Governance

Other institutions, such as the European Union (EU), also represent an important institutional anchor for QIT as it has done for other technology-related governance, such as data protection and, more recently, artificial intelligence. The EU is itself a treaty-based institution (or rather set of institutions) and so fundamentally anchored in sources of public international law (*Treaty on European Union*, *Treaty on the Functioning of the European Union* and related protocols). Of particular note from a quantum stakeholder perspective is the *Charter of Fundamental Human Rights of the European Union*, which encodes in an instrument binding upon member states certain moral/normative individual rights and freedoms, in effect setting constraints and criteria for other legislation that must be met in order to protect such rights.²³

In terms of a model for quantum governance, the EU's recent moves to propose legislative regulation of artificial intelligence provide an example of not only the type of substantive regulatory approach that may have application to QIT, but also an example deliberative approaches relevant to quantum governance. The European Union's proposed *Artificial Intelligence Act* proposal (2021), Kop (2021) provides a risk-driven model of governance for AI, with stated objectives of integration and consistency of AI with existing EU governance, facilitating AI innovation, maintenance of safety standards, preservation of fundamental rights and development of a single cohesive single market for AI (coordination). The regulation was developed via a consultative/deliberative process seeking input from AI stakeholders across academia, industry, government and civil society. The bill proposes rules for harmonising the use of AI systems, prohibiting certain uses, and heightened requirements for higher-risk AI activities, together with obligations. Surveillance, monitoring and enforcement are also provided for. One feature is a simplified risk assessment or 'pyramid of criticality', with less regulation applying to lower risk uses.²⁴ Such a

²³ While the EU is a multilateral institution, we incorporate it into the more formal end of governance precisely because of the more formal legal status (and public international law status) among nations of its legislative instruments as distinct from other multilateral institutions, such as the United Nations, whose equivalent 'legislative' function (resolutions) lacks the formal qualities of enforceability characteristic of formal public international instruments.

²⁴ *Unacceptable risk* includes cognitive manipulation on the basis of harming fundamental rights or disadvantaged groups; *high-risk* includes use cases that can endanger life or health, that can adversely affect opportunities or fundamental rights; such high-risk deployments of AI require greater typical risk assessments, greater oversight and monitoring along with a registration regime. Transparency obligations to ensure users are made aware of automated system usage and, for example, particular uses (e.g. automated emotion recognition). Other ethical requirements designed to address perceived ethical or moral harms include requirements for fair and representative data. The proposal also frames AI within 'product safety governance' involving risk-based self-assessment and self-certification, presumably owing to the unacceptable burden of direct regulatory oversight. In effect, the EU's approach to such technology governance synthesises (a) fundamental rights-approaches to governance, namely a purposive approach that imposes obligations (depending on risk profile) upon producers and distributors of AI while granting rights to individuals and others to enforce such fundamental rights; and (b) a product safety approach to QIT focused on risk management, mitigation and control.

model could in principle be extended to incorporate the use of QIT. Of course the challenge for such governance when it comes to quantum, as with any product-safety or even fundamental-rights based approach lies in the extent to which ‘hard’ or ‘soft’ governance approaches are adopted. The multiple objectives of quantum governance must facilitate the development of QIT, while managing various categories of risk. It must do so in a way consistent with preservation of fundamental (even constitutional) rights. This means that there is inevitably a debate around the optimal strategy for regulation, enforcement and oversight. In the main, the general precautionist approach for quantum governance would similarly see critical and high-risk uses of QIT (e.g. related to decryption in ways that could harm or transgress fundamental rights) attracting greater degrees of oversight, auditing and restrictions, including *sui generis* regulatory regimes dedicated to specific quantum activities. Lower-risk uses would be more pragmatically require less *sui generis* regulation and rely more on general governance principles.

From one perspective, there is an argument that high-risk usage of QIT may not require any *sui generis* regime and that rather what should be focused upon is whether the outcome of the use of technology is acceptable or whether its use for an outcome should be proscribed (see Moses (2017) for example arguments). One could in principle simply treat QIT devices, such as scalable fault-tolerant quantum computers, as ‘black boxes’ and proscribe their use for particular cases, such as decryption or certain simulations. However, one of the problems of such a generalist approach is that at some point, by subsidiary legislation or some other instrument, the exact permissible uses of technology tend to need to be specified. It is not enough to simply proceed by appeal to values or teleological aims or take a purposive approach. Regulation of most technology tends to involve specification of proscribed use cases. This is in part because law and regulation require that obligations be ascertainable, identifiable and decidable. And to the extent specificity is required or desirable, then this gives rise to specific governance legislation (for example, governing how chemicals may be used, nuclear materials may be prepared, used or transferred and so on). So there is a plausible argument that the necessity of regulatory specificity is what gives rise to *sui generis* regimes in many cases. Thus in the case of higher-risk and sensitive QIT technologies, specific governance instruments (such as legislation, regulation, treaties or other forms) may be needed to prescribe the use of such technology. In a geopolitical context, this might cover specific prohibitions on running certain classes of algorithms on quantum computers (or requiring that their design, if possible, prevent this), or it may require alert mechanisms (again, if feasible) for when actors (be they states or private) use QIT for particular cases correlated with proscribed activities. Thus, it is conceivable that there is or will be a necessary rationale for *sui generis* governance of QIT.

5.1.4 Multilateral International Institutions

Public international law also involves concepts of non-formalised regulatory approaches Guzman and Meyer (2010) which motivate state actors and multilateral institutions towards achieving regulatory objectives. Multilateral institutions are characterised as institutions comprising state actors, while international institutions

(of which there are enormous number Union of International Associations (2021)) can be composed more broadly of non-state actors as well. Multilateral institutions play important roles in interstate coordination and establishing normative contexts for state practice Schermers and Blokker (2021), especially regarding technology (cases in point being the IAEA). In turn, as occurs via state legislative ratification of public international law instruments (such as treaties), such multilateral instruments influence the governance of other stakeholders, such as private institutions. The primary global multilateral institution for coalescing state governance is the United Nations (UN). UN resolutions, while usually not regarded as sources of international law, do form important secondary and normative sources motivating state behaviour which in turn can influence the development of customary international law covering QIT. UN multilateral institutions and agencies also have important normative effects, especially regarding technology and indeed may often be precursors to any QIT treaty development. Thus, the development of quantum governance principles (involving a duties-based focus on states and others) under UN auspices is an important feature of the idealised governance stack that leverages existing institutional frameworks. A recent example is the UN's *Impact of rapid technological change on the achievement of the Sustainable Development Goals and targets* United Nations (2019) which provides a high-level example of synthesising technology governance concepts with established UN imperatives.

International institutions also represent important stakeholders in quantum governance. Such institutions can usefully be partitioned into state and non-state institutions, established according to different levels of governance formality. Global and international technology governance has largely proceeded through institutional practices and the development of agencies charged with coordinating governance, standards, development and auditing or enforcement practices. Such institutions include those under the auspices of treaties and the United Nations, such as the International Atomic Energy Agency. While there do not yet exist any supranational or international institutions dedicated to the multilateral coordination and governance of QIT, the particular features of QIT would naturally presage the establishment of a dedicated inter-state multilateral institution (or expansion of remits of existing agencies) to perform such coordinating functions. This is especially the case for the quantum communications pillars of QIT, where proposals for a quantum internet or networked/distributed quantum computers Kimble (2008), Lloyd et al. (2004), Wehner et al. (2018), Rohde (2021) require regulatory consistency across borders. As with the development of classical information and communications systems, standardisation and consistency of technological protocols is an important feature of the development and scaling of QIT.²⁵

²⁵ From an idealised governance perspective, the development of such protocols would be most likely (and indeed ideally) to follow the typical nexus of protocols developed by stakeholders most closely involved in the technology development themselves (such as research institutions, private sector firms) together with industry bodies and trade associations. In turn, more formalised standardisation instruments could be developed. For example, any quantum internet across multiple states would require consistent governance and technology protocols in order to function.

5.1.5 Case Study: Cybersecurity Governance

The primary risk generally acknowledged regarding quantum computing is the cybersecurity risk Fedorov et al. (2018), namely the risk of enabling decryption of sensitive datasets. A less discussed but also important feature is the deliberate use of QIT to decrypt or decode classically encrypted information, such as in conflict, national security or law enforcement scenarios (it must be remembered that it is not always or categorically the case that decryption of encrypted data is necessarily ethically or morally unjustified).

When estimating how governance of quantum cybersecurity risks would be managed, it is instructive to compare existing governance responses to classical cybersecurity threats. There is no comprehensive treaty governing the use of cybertechnologies or managing cybersecurity risks for state actors Schmitt (2021). In response to the emergence of cybersecurity threats, a number of analyses of the relation of international law and cybersecurity were developed, such as various editions of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* Schmitt (2017) (via NATO states) which initially focused on the legitimacy of offensive use of cybertechnologies, while the second edition covers also peace-time cybertechnological use. A UN United Nations (2013) report provided that international law and the UN Charter applied to the governance of information and communications technology, particularly principles regarding state sovereignty, human rights and admonishing the use of hostile cyberattacks by non-state actors. While the extent to which maintenance of state sovereignty is prioritised over other normative aims remains debatable at international law, the prevailing sentiment within soft international jurisprudence (as manifest in the second *Tallinn Manual*) promotes the principle that states must not conduct cyber-operations that violate the sovereignty of another state, though precisely what activities constitute violation of sovereignty remain vague Egan (2017) and even debated Wright (2018). The types of harms envisaged by such jurisprudence include permanent loss of cyber-infrastructure or intrusion into confidential state information, or even mere interference with digital infrastructure. Generic principles of state sovereignty may also permit the offensive use of QIT, for example on the grounds of necessity or in self-defence. Another principle applicable to any formal international quantum governance is the so-called *due diligence* principle requiring states to prohibit the use of their territory or infrastructure by others in a way that adversely affects other states, itself a principle grounded in protection of state sovereignty Corfu Channel (1949). As noted by scholars Schmitt (2021), the hortatory (normative) nature of such obligations is testament to the difficulties in prescribing or proscribing exact cybersecurity use cases for QIT in an international law context. Such questions concern state rights and duties or obligations towards other states. Nevertheless there are a plethora of international instruments embodying relationships between states and other stakeholders, such as citizens or persons. On cybersecurity grounds alone, there is little current justification for anticipatory regulation of QIT via international treaties specifically tied to QIT. However, such ICT international instruments remain lacking, thus to the extent

modern ICT international law instruments were to be developed, classification of QIT within their remit would make sense.²⁶

In the short term, a greater motivator for governance will likely be the desire to foster the innovation and development of QIT. International cooperation and coordination is a hallmark and integral part of the development of quantum science and economic activity globally. A primary institutional forum for governance instruments promoting technology development are bilateral and multilateral trade agreements Inoguchi and Le (2020), Cottier (1996). As such multilateral institutions driving formal (and informal) trade negotiations, such as the World Trade Organisation, could play an important role in both facilitating deliberative procedures among states for consistency of quantum governance (and its commercialisation). It could also foster the types of trade and economic conditions (such as reducing tariffs) that can positively benefit collaboration on quantum. For the realisation of infrastructure such as any quantum internet Kimble (2008), Rohde (2021), international networking of QIT systems would itself on technical and governance grounds necessitate the development of protocols governing the establishment, maintenance and use of such infrastructure.²⁷

5.2 National Governance

5.2.1 Governments

Quantum governance at the national level is understood from a stakeholder perspective as comprising formal (governmental) and informal (non-governmental) instruments. The primary stakeholders within states are constituted governments, whose instruments of governance can be categorised as (i) *legislative*, via law-making institutions such as parliaments, and (ii) *executive*, being instrumentalities of state that execute legislation and legislatively authorised policy. The executive function of government also encompasses the use of procurement as a policy instrument to

²⁶ For example, offlining of critical information technology infrastructure of a state could be regarded as a *casus belli* at international law Smith (2018). Nevertheless, there are some moves afoot to coalesce a coordinated approach to managing such cybersecurity risks by governments. The ability of non-state actors, such as individuals or collectives, to affect state rights, e.g. via hostile acts, interference with information technology infrastructure or kinetic attacks then raises important questions about (i) when such non-state actors may for example legitimately act in an offensive manner against state interests; and (ii) how other stakeholders can or should respond to intervene. For example, should quantum infrastructure of a private provider be utilised for a cyberattack, on what grounds would a state be within its rights to react. Such questions are not quantum-specific, but they illustrate the ways in which the governance of QIT must consider how the use of such technologies would fall within or be captured by existing, broader, public international jurisprudence.

²⁷ One could envisage, for example, something akin to prescribed and proscribed use cases for shared quantum internet infrastructure embedded into the technical architecture of such a quantum internet. Geostrategic issues of quantum internet in a game-theoretic context, for example, are explored in Rohde (2021): one interesting feature of such strategic quantum calculus is that in principle, networking quantum computers among states can amplify the available benefits beyond linearly; thus, there is motivation at once to share quantum resources, yet motivations also to limit access of adversaries to networking capabilities.

guide the development of technology. In reality, the delegated nature of governance means that even executive instruments will exercise decision-making capacity, including policy, resource allocation all the way to delegated regulatory functions, subject to municipal administrative laws. Thus far, at the national level, the majority of QIT governance initiatives have been largely confined to policy-related instruments, such as (i) national strategies, agendas or plans on quantum Made in China (2015) or (ii) policy papers Brennen et al. (2021) published by governments or their administrative departments etc. Globally only a select number of nations have national quantum strategies Countries (2021), often embedded within existing national science initiatives. Of note are programs from global leaders in quantum such as China, which has prioritised QIT as part of its most recent national strategic plan Made in China (2015), Garisto (2021). Indeed, governments play a leading role in the development of technology via direct investments, policy formation, procurement policies and public/private partnerships. Their governance architectures must be tailored to balance competing objectives of QIT development and management of its risks.

As with all direct forms of governance, governments as representative of state power represent the priority stakeholder for quantum governance regimes at national, international and policy levels.²⁸ Governments in addition form the primary investors in QIT, directly via research programmes (such as those funded by national defence agencies) and indirectly, via funding of academic institutions where most theory and early engineering of quantum systems has emerged. Governments (and states) are generally regarded as owing normative and implicit constitutional duties towards their collective citizenry.²⁹

5.2.2 Public Institutions

Public institutions in our formulation cover national instrumentalities which are established by specific public legislation but usually are afforded a degree of autonomy that distinguishes them from the direct administrative wings of governments,

²⁸ The scope and extent to which governmental obligations give rise to specific rights of other stakeholders, such as individuals, collectives or other associations, is itself a contextual matter which differs across polities. Nevertheless, in most modern democratic nations, the development of jurisprudence has led by design and evolution (through, for example, the evolution of common law or civil law principles) to general acceptance that governments do owe duties towards their citizens. These are usually encoded constitutionally or in administrative law-style legislation or regulation which provide for canonical principles and rights, such as the right to natural justice, the right to be heard (e.g. *habeas corpus*) and other rights. Other jurisdictions also impose human-rights style frameworks as overlays which in many ways resembles risk assessment approaches: proposed legislation is compared against a set of fundamental or important or enumerated rights.

²⁹ Ethically, the types of roles and responsibilities of government are largely all-encompassing; so too are the objectives of government as the instrument par excellence by which conflicting interests and views on production, distribution and behaviour are resolved. The objectives of governments with respect to quantum governance comprise overall development objectives together with the broader imperatives of states regarding sovereignty, security, economic and welfare interests of their citizens. Constitutionally instantiated governments are themselves subject to constitutional rules and laws together with legislation passed that binds or restricts their behaviour as sovereign entities within their jurisdiction. Thus, governance of governments itself proceeds on the same basis as discussed.

such as departments, or those which, while not constituted by separate legislation, are publicly funded.³⁰ Public institutions exhibit their own features as stakeholders. While established according to legislation and/or delegated executive authority, they are endowed with their own sets of institutional interests, shaped by the purposes for which they were established, the economic and political contexts in which they operate and by the participants (such as employees or agents) who carry out their functions. Public institutions can thus develop interests parallel to but separate from governments. Similarly, depending on their form, they may be separate legal persons with liabilities and obligations. Furthermore, they usually must balance often competing interests of other stakeholders, such as consumers, private sector companies and government itself when managing governance. These features of public institutions are relevant to how they would contribute to QIT governance (via policy development, administrative oversight or procurement) and internally, via internal policies or risk management.

Public institutions are core to technology governance globally, as exemplified by such organisations as the National Institute of Standards and Technology in the USA and the Commonwealth Scientific and Industrial Research Organisation (**CSIRO**), an Australian government agency responsible for scientific research. Public institutions, particularly science-related institutions as NIST and the CSIRO perform important roles in coalescing research and industry stakeholders via deliberative means. They also tend to form the core institutions upon which governments, via their own governance processes, rely upon for advice and guidance in order to develop legislative or policy responses. Thus, public institutions, particularly in the technology governance space, are likely to have in some ways an outsized influence on the overall shape of technology governance generally given their capacity to synthesise technical domain expertise with governance requirements. Public institution duties depend on the objective of the institution in question: for umbrella science organisations most likely to drive QIT governance recommendations, it will be developmental and standardisation imperatives, for consumer-facing institutions, the rights which must be assessed in quantum governance will include consumer-based rights (e.g. explainability, rights to correct, product safety). One of the challenges for public institutions involved in QIT governance will be balancing various stakeholder interests. For example, any QIT-focused public institution charged with developing, administering or enforcing public policy will likely face trade-offs that other institutions involved in similar activities face. An analogy would include, for example, institutions governing food and drug administration in the USA (the FDA) which must balance a range of stakeholder interests, including those of consumers, government and large pharmaceutical industrials when setting rules for the development or release of new medicines.

³⁰ While existing by virtue of legislative and executive prerogatives, public institutions relevant to quantum governance can usefully be classified as separate (though not mutually exclusive) stakeholders.

5.2.3 Case Studies: National Quantum Governance

QIT primarily emerged out of two institutions, academia and government. Within government (which often funds academic institutions), it has primarily been defence and strategic-related instrumentalities, such as the USA's Defense Advanced Research Projects Agency (DARPA) and others which have driven funding in the quantum sector both within the USA and also in other nations, such as Australia and Europe through strategic partnerships and direct funding of research programmes. Other nations, such as China, have positioned quantum as top national strategic priorities, such as Made in China (2015) China's recent development plans. In the USA, legislation seeking to motivate and accelerate the development of QIT has been advanced, such as the *National Quantum Initiative Act* (2018) United States (2018), Raymer and Monroe (2019) (NQIA). The NQIA has as one of its stated purposes the promotion of international standards for quantum information science and technology security, including fostering quantum innovation and national security objectives (sec. 3). The NQIA also establishes a National Quantum Coordination Office to coordinate acceleration of investment in the quantum sector, together with a National Quantum Initiative Advisory Committee to advise on, among other things, prospects for international standard development regarding QIT.

The primary legislative instruments managing the geostrategic risks (and opportunities) of QIT tend to be national security-related. As discussed above, the challenge of governing quantum relates in part to its dual-use. Governance models for dual-use technologies already exist in legislative, regulatory and other forms (such as for nuclear, biotechnology and cybersecurity-related technologies Ienca and Vayena (2018), Harris et al. (2016)) and these can be used as a basis for commensurate QIT dual-use regulation. Many jurisdictions also utilise export controls, such as foreign investment export controls, to regulate dual-use risks. An example explicitly covering is *Guidance Note 8 - National Security* issued by the Australian Government's Foreign Investment Review Board (FIRB) Foreign investment (2021), a regulator overseeing foreign investment and joint foreign economic activities in Australia. The note provides proposed legislative reforms to governance of, among other things, QIT deemed significant or with potential for military use. The scope of the coverage is extremely broad, covering 'quantum computing, quantum sensing quantum encryption and quantum communications and technologies'. Effectively the rules mandate FIRB approval for foreign persons (including governments) who may obtain a broad scope of interests in critical technologies when such technologies may be used for defence or intelligence purposes of another country. While securing sensitive technologies and accounting for the realities of geostrategic risk and foreign policy applies to the use of all and any technology in a sovereign nation, the proposed rules have been criticised by other quantum stakeholders such as those in academia and the private sector as potentially stifling innovation in QIT Davidson (2021). This is in essence due to the increased regulatory burden and potential interference with international collaborations. The proposal and responses to it demonstrate the importance of stakeholder engagement in quantum governance in order to take account of the multiplicity of objectives and stakeholder interests, not simply those of one sector (such as defence).

5.3 Commercial Private Sector

Commercial private sector actors are increasingly important in the QIT ecosystem globally. By private sector, we primarily focus on corporations, including ‘quantum startups’, such as PsiQuantum, Xanadu and Rigetti but also established companies such as Google, IBM, Amazon and Honeywell who are undertaking considerable investment, research and development in the quantum sector. The quantum governance stack approach for such stakeholders involves once more accounting for the overall objectives of such stakeholders, such as maximising profit, growing a business, building scalable or useful products, along with the rights and interests of such stakeholders and those affected by their actions.

5.3.1 Corporations

The governance of corporations, businesses and companies is mandated by municipal business law, such as corporations’ law statutes and regulations. Corporations, for example, are accorded their own distinct legal personhood but must act through the delegated authority of agents (such as officers, contractors or employees) who are bound by typical duties such as the duty to act in the best interests of the company, or other fiduciary-style duties.³¹ Company governance is also manifest via company policies that set out practices, routines and procedures. Such policies in turn usually encode or specify how risk is managed within the organisation Calder (2019). Thus, the governance of QIT-related activities of corporations would occur (a) externally, via the imposition of regulation and (b) internally, via the formulation of internal policies must take into account such fundamental business objectives. Most companies involved in the quantum sector have business objectives aligning with the development of (i) quantum hardware, (ii) quantum software or (iii) infrastructure related to QIT, such as that related to quantum sensing or communication. Thus, their objectives and interests align broadly with the development objectives common across other quantum stakeholders. Companies are also necessarily interested in security.

It is also worth considering the interests of the agents or employees of such companies as distinct quantum stakeholders, though this does of course overlap with individual stakeholders below. For example, a typical quantum hardware or software company will employ experts in relevant disciplines (such as quantum computational science, quantum engineering) but the question from a governance perspective then becomes what are the rights, obligations and duties (and to whom are these owed) of such individual agents within such a company. Does the average quantum algorithm

³¹ In some jurisdictions, companies are obligated to have regard to broader social welfare as well. Thus, such a duties-based nexus, with obligations of the company owed to certain stakeholders (including those at general law, e.g. the duty of care owed by legal persons) and the obligations of agents characterises the governance architecture within which quantum governance at the company level must be situated. What counts as the best interests of a company vary considerably, but by and large ensuring a company is profitable and not insolvent (bankrupt) and treats third parties (such as creditors) fairly are common principles across various jurisdictions.

designer need to modify their work practice in order to comply with quantum governance imperatives or facilitate their outcome? The development imperative of QIT (hardware or software) is integral to the set of tasks and procedures of such agents. But to what extent, for example, should a quantum algorithm designer or engineer working on a particular quantum device owe a duty to consider, for example, the impact of their design choices against normative criteria? From an idealised quantum governance stack perspective, the answer is to be found in existing firm-level risk management protocols. These set out their risk policies and include relevant intra-institutional delegation of responsibilities for management, oversight and control of risks (such as to compliance functions or officers). Moreover, specific policy frameworks that instil auditing, checks and review against governance outcomes both (a) in technical product design/development stages and (b) when products are being approved for release, can be leveraged or adapted to handle quantum-specific risks. An abstraction of firm risk management for quantum is set out in Fig. 3.³² In conjunction with risk-management procedures, impact assessments are also another important tool for identifying the effect of QIT on certain values in ways that may not be captured by formal or quantitative risk assessments.

5.3.2 Startups

QIT has also recently become a focus for a surge in startup communities globally Finke (2015). Startup and fledgling private-sector enterprises have traditionally been a central element of the development and dissemination of technological advances Bloch (2007). The reason it is useful to distinguish between ‘startups’ and ‘established’ companies is mainly due to the fact that startup going concerns tend to operate with limited resources and higher-pressure timelines, which limits their business objectives (e.g. startup objectives differ from more mature businesses) and also the practical availability or utility of complex internal policy architecture.

5.3.3 Case Study: AI Ethics’ Toolkits

One example (among many) of the implementation of governance in a related information technology field by a large-scale company is Google’s Responsible AI Toolkit Google (2022), a set of software protocols connected to its machine learning

³² A speculative example might be that if a product, say access to a cloud-based quantum computing as a service (QCAS) is offered, it must be done in a way that users of such QCAS cannot utilise the platform to, for example, conduct cyberattacks or unlawful or unethical decryption of classical data. This might in turn require either monitoring (or some type of systematic or sample-based auditing) of uses, or even technical setups which (if feasible), would limit the types of algorithms that could be deployed on such QCAS. Whether such built-in risk management is possible for such a toy example is left as an open question, but we use this as an example of where an agent, say a quantum algorithm designer may need to incorporate quantum governance constraints into the very design of their product (manifesting ethical design principles in some sense van den Hoven (2017)). Best-practice governance in the quantum sector for corporations and other business associations involves adapting well-established risk management/governance in ways that identify (a) the potential impact of their quantum sector activities on themselves and other stakeholders (i.e. the risk assessment); and (b) implementing, where appropriate, mitigation, control or monitoring measures as responses to such risks.

offerings. Google's proposals provide guidance for developers in order to help them become cognisant of particular biases, unfair practices or what are deemed to be socially or morally harmful behaviours of algorithms (such as algorithmic architectures that transgress prohibitions on classification using protected attributes of race, gender or class).³³ Google's approach emphasises best practices for designing AI systems along with imperatives of fairness, interpretability, privacy and security. One particular element of such approaches is the focus on what is sometimes termed 'human-centred design' Giacomini (2014) where technology design is based around a set of objectives regarding user experience of the technology. The toolkit is of interest in that it is not simply the user experience of using their platform for technical reasons, but what might be termed the 'user governance experience', the experience a user has of how a system manifests governance, preserves their rights or objectives, which is emphasised. The approach provides an example for user-interaction with quantum systems both from a developer and consumer perspective.

5.4 Academia

Academic institutions, while falling within categories of either public or private institutions, are categorised as separate quantum stakeholders because of their centrality to the development of quantum science (and technology) and because they tend to have their own governance architectures within which quantum governance must sit. Academic institutions have as their primary objectives research output, pedagogical objectives (e.g. teaching and tuition) and also ancillary objectives covering institutes, initiatives or projects involving such institutions. As with most technology, academia has been the primary driver of the early-stage foundational research into quantum information processing and represents the primary institutional sector within which the overwhelming majority of both theoretical and applied research is undertaken. Governance instruments for academia generally consist of its institutional policies and guidelines, such as research policies and also its ability to dictate the terms and conditions of funding or grants for projects. Practically speaking, quantum governance by academia would consist of adopting typical risk-management frameworks that assess (i) the impact of QIT on (ii) the rights of various stakeholders affected by the prospective QIT, together with (iii) a risk-weighting and assessment of significance (remote, unlikely or speculative risks should not ideally constrain research). Universities already have well-established procedures regarding ethical impact of technology research into which such QIT-related assessments could easily fit.

³³ Such governance stems from broader emerging literature and practice on 'fair machine learning' Dwork et al. (2012); Chouldechova and Roth (2018); Caton and Haas (2020) and a manifestation of design-ethics in information technology that seeks to at once socialise the policy reasons for such fairness constraints on algorithmic technology and also then provide technical guidance regarding its implementation. This type of model is also offered by other major providers of cloud computational services and in principle provides a model for how soft governance via key commercial and institutional stakeholders can be pragmatically effected in a way complementary to the work practices of the technical communities who are normatively being obliged with duties to ensure fairness criteria are met.

Academic institutions are also pivotal and leading institutions for the development of principles and guidelines regarding the governance of technology. In addition to academic work on governance, such institutions tend to play an outsized role via the participation of academics in formal governance procedures (such as committees or treaty development) and soft-governance measures, such as principles development. A case in point is the evolution of AI ethics principles, from the Asilomar AI Principles (ostensibly developed tangentially in connection with academic conferences on AI) to the EU ethics guidelines for trustworthy AI.

5.5 Individuals

Individuals are included as stakeholders in governance analysis as ultimately all governance concerns individuals, relates to their rights and obligations and is (despite nascent moves towards automating some regulatory functions) implemented by individuals. In a quantum context, we enrich the distinctions set out in Quantum (2022) to distinguish among (i) *users/consumers* of QIT, (ii) *producers* of QIT and (iii) those impacted by QIT who are not direct consumers or producers of the technology. The types of rights, duties and obligations of individuals with respect to QIT will depend on context, including whether formal or informal governance is at issue (e.g. legislatively enshrined rights versus normative moral claims lacking legal enforceability). As consumers, individual rights are focused on matters such as product safety and informed consent. Moreover, the bedrock requirement of informed consent — or at least the opportunity to be informed if an individual wishes (as in reality most individuals do not delve into the workings of technology they use) — is an important consideration. This in practice means ensuring citizens have rights to be informed about some of the basics of how QIT works, its implications and how QIT may affect their rights. Individuals involved in the production of QIT have objectives describable in terms of overall development interests, together with personal interests (such as career, economic). They also have objectives definable in terms of the organisations of which they are part (e.g. academia, business, government). More pertinently for governance are questions of what types of *duties* individual agents within quantum sectors might owe and to whom.

Individual objectives coincide with their interests and duties which are in turn normatively and formally constituted. The instruments of individual governance are of course those to which other legal persons are subject within a state, such as legislation, regulation and common law (for example). Much governance is directed fundamentally at preservation of individual rights, albeit non-uniformly internationally and within states. These are typically encoded in charters, legislation or constitutionally which have, from a technology governance perspective, the effect of (where applicable) imposing constraints or additional requirements upon technology development or use. Examples include autonomy-based rights (the right to be informed, principles of consent of the governed etc., accountability/explainability) and the right to be free from harm. QIT need not reinvent the wheel on this score. Numerous institutional practices exist for identifying and responding to technology impacts on individual/fundamental rights. However, there is also legitimate debate

Table 2 Some speculative impacts of QIT on individual rights

Individual rights and QIT	
QIT activity	Rights and impact
Decryption of confidential data	Right to privacy (via data access and distribution) Right to personal security (if released data compromises individual safety)
Unethical use of quantum algorithms	Right to equality before the law (if antidiscrimination rules are contravened)
Offensive use of quantum algorithms	Right to life, liberty and personal security (e.g. use of quantum algorithms to design chemical or biological weapons)
Inaccessibility to quantum computation	Right to adequate standard of living (if inequality of access to QIT exacerbates standard of living disparities)

as to whether traditional governance instruments remain fit for purpose in preserving fundamental rights in the face of rapidly emerging technologies, including any that may emerge from QIT in the future.

Where QIT stakeholders can add value is in parsing the estimated or likely risk and impact of QIT (which may be direct or indirect where QIT is merely part of a broader product or operation) and, in particular, pushing back against potential unjustified hyperbole about downside risks of QIT. Thus for stakeholders involved in QIT governance, it is paramount that the deliberative governance processes involved factor in the impact of their activities upon core individual rights overall.³⁴ Such a rights-based assurance or superstructure approach is common globally and is reflected in such seminal instruments as UN charters on individual (human) rights, multilateral declarations and treaties covering rights, as well as individual rights under customary, common and code-based law. Understanding the impact upon individual rights is imperative for other quantum stakeholders when considering their involvement in QIT and designing their own governance instruments. We set out a (non-exhaustive) table of some select rights (as set out in various UN charters)³⁵ and speculative ways in which they may be impacted by QIT in Table 2.

5.6 Civil Society

Civil society groups are an important stakeholder in most societies, and include groups such as trade unions, political parties, charities or privately constituted associations which receive public or other funding. Civil society institutions tend to have

³⁴ Individuals may involve themselves in governance processes across different levels of the governance stack. For example, direct participation in (democratic) governance (e.g. via activity in politics or civil society groups) is an important way for individuals to manifest their interests and protect their rights. While ‘quantum specific’ rights’ organisations are unlikely, it is foreseeable that rights groups, such as the Algorithmic Justice League (a civil society group focusing protecting individual rights in an AI context) may also engage in advocacy around perceived risks to individual rights from QIT.

³⁵ Such as the *Universal Declaration of Human Rights*, *International Covenant on Civil and Political Rights 1966 (ICCPR)*, *International Covenant on Economic, Social and Cultural Rights 1966 (ICESCR)*.

objectives covering social change, securing some conception of justice or improve outcomes for their constituencies (which may be the population as a whole), advocacy functions, charitable or welfare objectives. Civil society groups play important roles within communities regarding (a) the development and deliberation of governance; and (b) the socialising and acceptance of governance, including through outreach. Such groups play (and historically have played) an important role in how technology is governed within societies.³⁶ Another key civil society stakeholder are media participants and journalists, whom play an important role in setting agendas, highlighting risks and drawing attention to issues requiring governance responses.

Civil society group objectives are defined in the main by the constituencies they represent and ideologies they advocate. One of the overall risks to consider from quantum governance is the role that misinformation, hype or ignorance may play on how public responses to QIT plays out over time. Importantly, not all civil society groups are engaged in idealised rational debate nor are such constituencies necessarily responsive to empirical evidence, e.g. about QIT or its impacts. As is abundantly evident, most recently with culture war debates over vaccines or climate science, conspiracy theories and misinformation about the impact of technologies can have significant impacts on public responses and more formally on how governance stakeholders, such as politicians, respond to technology-related governance. At the more severe end of misinformation spectrum, conspiracy theories can have significant effects on governance such as adherence to best practice by constituencies suspicious of technology. By contrast, civil society groups also fulfil an important role in countering such misinformation and ignorance in ways that foster environments conducive to rational governance, such as academies of science or other institutions.³⁷ Moreover, ensuring open and transparent accessibility for journalistic reporting on QIT will be a crucial element of civil society contributions to governance.

5.6.1 Case Study: Ethical AI Frameworks

An example of civil society input is in the realm of ethical AI. The last half-decade has seen a surge in awareness of ethical issues and the requirement of governance of information technologies with potential for profound impact, such as artificial intelligence and automated systems. The OECD's AI observatory OECD (2021) notes over

³⁶ The role of such groups in relation to a specialised field such as quantum governance is most likely analogised by reference to the role of such groups in other topical technology governance, such as artificial intelligence, nuclear technology or climate science. An example of such civil society groups in the quantum sector is the Sydney Quantum Academy, a partnership among certain Australian universities whose aim is to foster Australia's quantum economy via coordinating collaboration among industry, academia and government (rather than specifying technical standards typical of technical communities).

³⁷ Civil society is subject to governance, usually through the constitutive rules of the associations, and is also a producer of informal governance instruments such as guidelines, manifestos, principles and frameworks published as part of their contribution to public debate and advocacy. The particular form that a civil society group takes determines its formal legal rights and duties. Associations usually have legal personhood rights and owe duties to their membership or constituencies whose interests must be usually be prioritised. Civil society groups tend to be involved in formal governance via contributions to deliberative governance development, such as via formal institutional enquiries conducted by public institutions or committees.

700 initiatives on AI governance across 60 countries, including (i) national initiatives and strategies, agendas and plans (primarily consisting of national strategies, development plans for AI, proposals for trustworthy AI), (ii) coordination and monitoring bodies, (iii) public consultation processes and (iv) public sector governance. Civil society institutions have been instrumental in raising awareness of AI ethics' issues and driving governmental responses globally (such as prohibitions on facial recognition or emotional profiling). The response to potential AI impact, while different from QIT due to its later technological maturity, provides useful case studies for stakeholders considering how to analyse and anticipate QIT governance.

5.7 Technical Communities

In the context of governance, technical communities comprise those industry groups, institutes and other collective associations whose activities involve research, development of standards and coordination. Examples in the information technology sphere include the multilateral International Organization for Standardization (ISO) and industry association, the Institute of Electrical and Electronics Engineers (IEEE). Technical communities also overlap with other stakeholder groups, such as academia where quantum research groups also form in effect technical communities of practice and expertise. Technical communities thus form institutions with their own collective interests, agendas and, depending on their legal structure, rights and obligations. As such, technical societies are properly considered distinct stakeholder groups despite overlap with other categories articulated above. Technical communities are a critical and fundamental basis of technology governance both in respect of imperatives like standardisation but also in terms of setting out proposals for risk management specific to technology. The primary objective of technical communities is the promotion and development of their technical subdisciplines in a theoretical and applied context. They also play an important role in coordinating the translation of theoretical research into applications and act as conduits for coordination among other stakeholders involved in technology, such as academia and industry.

As communities of practice, technical communities' primary contribution to governance lies in the development of subdisciplines themselves via research output, the development of standards. Voluntary codes of conduct Johnson (2018), Webb (2004) represent another form of behavioural standardisation and self-regulation among technical communities across different technology sectors. Standards represent critical governance instruments due to their effect on research and development, coordination, production and market penetration of technologies Tassey (2000).³⁸

³⁸ They also carry normative force by establishing and setting expectations for stakeholder behaviour which in turn can often become the basis, via more formal governance mechanisms, for regulatory requirements Seidl (2007). Such codes often interplay with the development of standards, though as noted by a number of scholars, they lack the more sophisticated mechanics for oversight, reporting and enforcement characteristics of transparency and accountability requirements of governance Johnson (2018). Moreover, such codes are also rarely developed with the type of comprehensive input from other affected stakeholders, and so such codes, while often facilitating useful anticipatory governance, generally are no substitute for formal governance instruments

As with civil society groups, technical communities play a significant role in contributing to technical information germane to technology governance, especially regarding capabilities and risks of particular impacts. In addition, their crossover with other stakeholder groups, such as industry, means that their soft-governance influence extends through to for example corporate governance or policy and other areas in ways that other civil society groups do not. At a pragmatic level, the development of (a) standards and (b) codes of conduct via deliberative procedures represents probably the most beneficial type of activity that technical communities can participate in at the very early stage of quantum governance.³⁹ Indeed, standardisation can often become intertwined with other stakeholder interests such as those of nation states or private sector actors whom seek to preserve their own interests via the shaping of technical standards. Given the importance of QIT to national security, it is foreseeable that international standardisation procedures will involve such strategic considerations. Examples in other technological domains, such as international standard setting for atomic energy and technology, illustrate how standard setting in an adversarial geopolitical context might be undertaken for QIT.

5.7.1 Case Study: IEEE

Industry associations such as IEEE (discussed above) are also playing an increasing role in the development of standards for quantum information (as they have been instrumentally involved for other technologies such as Wi-Fi) — standards are developed as deliberative initiatives of stakeholders. The IEEE is the world's largest technical professional ICT organisation (active in over 160 countries with nearly half a million members). It has been instrumental in developing standards that shape ICT sectors globally. The structure of the IEEE involves numerous technical societies under the umbrella of technical councils, running hundreds of standardisation and governance programs. Existing standards include protocols for quantum communication (IEE P1913), QIT definitions (IEEE P713) and performance metrics and benchmarking (IEEE P7131). The IEEE is an example of an industry body exemplifying how technical communities can bridge the gap. One analogous early proposal albeit short on detail for management and governance of quantum computing is based upon adapting COBIT (Control Objectives for Information and Related Technology) principles developed by ISACA (Information Systems Audit and Control Association), an information-technology sector industry association Blanco and Piattini (2020).

5.7.2 Case Study: Internet Governance

While the focus of this paper leans towards formal governance instruments (given the primacy of sovereign states as the loci of enforcement), an important counterpoint to state-centric governance involving a multitude of civil society and technical community

³⁹ indeed such processes themselves often give rise to important early-stage discussions about the types acceptable costs and benefits of technology, together with alerting stakeholders to issues regarding rights, obligations and interests of others Abbott and Snidal (2000).

groups is illustrated by the evolution of internet governance. As a (perhaps the) primary information technology infrastructure globally, the internet developed as with many technologies under considerable uncertainty. As such, the types of governance responses and norms applicable to it have tended to map the decentralised and collaborative approach. Modern norms of internet governance tend to emphasise the role of a range of non-state actors together with states in deliberating how to regulate facets of the technology. Thus, states, academic institutions, technical organisations and the commercial sector play a role in development of underlying norms as encoded in protocols of varying formality Dany (2013). Examples include the *2005 Tunis Agenda for the Information Society* (which established participatory governance models and venues), various World Summits on the Information Society and other initiatives (the *2014 NETmundial Initiative and Multistakeholder Statement of Sao Paulo*) Fraundorfer (2017) embedding multi-stakeholder approaches Haggart et al. (2021). This preference for multistakeholder and non-state directed protocol governance led to the establishment of bodies such as ICANN and IETF Carr (2015). This meant that state actors were already faced with governance norms embedded not just via principles, but in practice across economies which become difficult to displace via formal instruments. The cost of unwinding such norms together with the functionality of such protocols has been in part responsible, then, for the continuation of the multilateral approach. This is an example of how early-stage technology norms can embed into routines of technological use in ways that render them relatively robust as more and more infrastructure or economic activity becomes dependent upon them. In effect, the governance architectures become ‘sunk costs’ that are difficult to unwind. It is conceivable that QIT could develop in parts similarly. However, it should be noted that, in respect of internet governance, despite such a multilateral provenance, scholars are increasingly questioning whether there has been a resurgence in the role of the state (see Haggart et al. (2021) for a recent review).

6 Conclusion

QIT governance globally represents an important emerging branch of technology governance applicable to what is potentially among the most profound set of technologies ever created. As we have discussed in this article, regulating nascent technology such as QIT requires a delicate anticipatory balancing act in anticipatory framing of uncertain outcomes and risks. For this reason, an awareness of governance methodologies and deliberative processes among stakeholders charged with oversight of QIT and those impacted by QIT is crucial. In this paper, we have aimed to provide an overview of key characteristics features that the governance of QIT should exhibit. These include conceptual understandings of how early-stage and highly uncertain innovative technology is best regulated and the need to treat fostering innovation and QIT development as an explicit goal of governance themselves. QIT is not emerging into a governance vacuum: a variety of well-established responses exist across the governance landscape. As a model of governance, the quantum governance stack introduced in this article aims to provide a basis for systematically thinking about governance from the perspective of stakeholder rights, duties and interests. The governance stack explicitly identifies the hierarchies of hard and soft governance regimes

Table 3 *Quantum governance stack. A matrix illustrating for different quantum stakeholders (rows) types of governance instruments (columns)*

Model governance						
Category	Agents	Objectives/risks	Instruments	Rights/interests	Powers/duties	Example
International	States	Strategic, QC development, national security, coordination (research, quantum networks)	Formal (treaties, conventions, customary law) Informal (concordats, memoranda, joint ventures)	Sovereignty, jurisdiction, restraint	Respect sovereignty, duties to citizens	Quantum Cybersecurity Treaty
International	Multilateral institutions, courts, tribunals	QC development, collaboration, jurisprudence, standardisation	Resolutions, memoranda, principles	International collaboration, influence	Charter/mission-related, facilitate deliberation	International Quantum Agency
National	Governments	Security, economic, social welfare, QD development	Legislative, executive, policy, strategy, expenditure	Access to QC research, QC infrastructure resources	Duties to citizens, organisations, other states	National Quantum Legislation, Quantum Strategic Plans, QIT funding
National	Public institutions	Administration of policy, expenditure, standards	Administrative regulation, general law, policy, codes of conduct	Policy implementation, mission, advisory, charters	Standard development, policy	National Quantum Academy
National	Academia	Research, education, workforce development,	Administrative, grants, policy, statutes	Research, funding, autonomy	Duties to students, researchers, public	Quantum Research Joint-Ventures
Private (groups)	Corporations	Profit, growth, QC development	Policies, risk management, internal compliance	Legal rights, intellectual property	Risk management, benefit shareholders, legal duties, product safety	Quantum Risk Management Frameworks
Private (individuals)	Individuals	Economic, social, employment advancement	National laws, ethical guidelines	Legal rights, human rights (privacy), normative rights	Duties of care to others	Guidance for Responsible QIT
Civil Society	Unions, charities	Advocacy, policy change	Campaigns, guidelines, principles, publication	Legal rights, participation	Duties to members, causes, public	QIT Ethics Associations
Technical communities	Quantum research groups, IEEE etc.	Standardisation, research output, development	Standards, protocols, publications, committees	QIT development, coordination	Duties to members, public	IEEE

involving states, governments, private actors, individuals and civil-society groups together with the types of formal and informal instruments applicable to their regulation. As summarised in Figs. 1, 2 and 3, the quantum governance stack advocated herein provides a systematic series of steps that stakeholders can adopt to help frame their governance response to QIT. A high-level summary of the quantum governance stack structure for reference is set out in Table 3.

Importantly, as with all idealised governance, process is key. QIT governance best practice involves inclusive and deliberative engagement of a variety of stakeholders, from states, to citizens, to civil and public institutions to the commercial sector in a way that enables stakeholder interests to be advanced and compromises reached. Such technology governance must be responsive based on (a) the state of technology at the time; (b) resource and economic requirements for its development; and (c) assessments and estimates of the near-term and future impacts of such technology. In this article, we have set out a prospective taxonomy of stakeholders and governance instruments according to which early QIT governance initiatives might proceed at any level in the quantum governance stack. Quantum governance should not be an exercise in looking through the glass darkly as a ward against the anxiety of uncertainty. Rather, governance must explicitly factor in maintaining and fostering the conditions for the development of QIT itself in both the public and private sectors in order to facilitate the flourishing of the technology and its potential benefits.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Aaronson, S. (2013). *Quantum computing since Democritus*. Quantum Computing Since Democritus: Cambridge University Press.
- Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. *International Organization*, 54(3), 421–456. Cambridge University Press. <https://doi.org/10.1162/002081800551280>
- Aggarwal, C.C., Yu, P.S. (2008). A General Survey of Privacy-Preserving Data Mining Models and Algorithms. *Advances in Database Systems*. In C. C. Aggarwal & P. S. Yu (Eds.), *Privacy-Preserving Data Mining: Models and Algorithms* (pp. 11–52). Springer. https://doi.org/10.1007/978-0-387-70992-5_2
- Allenby, B. (2014). Are new technologies undermining the laws of war? *Bulletin of the Atomic Scientists*, 70, 21–31.
- American Bar Association. (2017). *Handbook on Antitrust in Technology Industries*. ABA Book Publishing.
- Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, 100, 7–25. <https://doi.org/10.1016/j.jeconbus.2018.07.003>

- Arner, D. W., Barberis J., & Buckley, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. & Bus.*, 37, 371.
- Australian Government. (2021). *Foreign investment review board - Guidance notes - National security*. Retrieved February 20, 2022, from <https://firb.gov.au/guidance-notes>
- Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press. <https://doi.org/10.2307/2938772>
- Baldwin, R., Cave, M., & Lodge, M. (2010). Introduction: Regulation—the Field and the Developing Agenda. In R. Baldwin, M. Cave, and M. Lodge E, *The Oxford Handbook of Regulation* (pp. 3 - 16). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199560219.003.0001>
- Ball, P. (September 19, 2021). *Major quantum computing strategy suffers serious setbacks*. Quanta Magazine. Retrieved March 3, 2022, from <https://www.quantamagazine.org/major-quantum-computing-strategy-suffers-serious-setbacks-20210929/>
- Bernstein, S. (2011). Legitimacy in intergovernmental and non-state global governance. *Review of International Political Economy*, 18, 17.
- Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549, 188–194. <https://doi.org/10.1038/nature23461>
- Black, J. (2001). Decentring regulation: Understanding the role of regulation and self-regulation in a “post-regulatory” world. *Current Legal Problems*, 54, 103. <https://doi.org/10.1093/clp/54.1.103>
- Black, J. (2005). *What is regulatory innovation?* In Julia Black, Martin Lodge, and Mark Thatcher, editors. *Regulatory Innovation*: Edward Elgar Publishing.
- Black, J. (2012). Paradoxes and failures: “New Governance” techniques and the financial crisis. *MLR*, 75, 1037. <https://doi.org/10.1111/j.1468-2230.2012.00936.x>
- Black, J. & Baldwin, R. (2010). Really responsive risk-based regulation. *Law and Policy*, 32, 181. <https://doi.org/10.1111/j.1467-9930.2010.00318.x>
- Blanco, M. Á., & Piattini, M. (2020). Adapting COBIT for quantum computing governance. In M. Sheperd, F.B. e Abreu, A. R. da Silva, and R. Pérez-Castillo (Eds.), *Quality of information and communications technology, communications in computer and information science* (pp.274–283). Springer International Publishing. https://doi.org/10.1007/978-3-030-58793-2_22
- Blair, R. D., & Sokol, D. D. (Eds.) (2017). *The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech*. Cambridge University Press. <https://doi.org/10.1017/9781316671313>
- Bloch, C. (2007). Assessing recent developments in innovation measurement: The third edition of the Oslo Manual. *Science and Public Policy*, 34(1), 23–34. <https://doi.org/10.3152/030234207X190487>
- Brennen, G., Devitt, S., Roberson, T., & Rohde, P. (2021). *An Australian strategy for the quantum revolution*. Australian Strategic Policy Institute: Technical report.
- Brownsword, R. (2008). *Rights, Regulation and the Technological Revolution*. Oxford University Press.
- Brownsword, R., Scotford, E., & Yeung, K. (2017). *The Oxford handbook of law, regulation and technology*. Oxford University Press.
- Brownsword, R., & Yeung, K. (Eds.) (2008). *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. Hart Publishing. <https://doi.org/10.1111/j.1468-2230.2010.00814-2.x>
- Calder, A. (2019). *ISO/IEC 38500: A Pocket Guide, Second Edition*. IT Governance Publishing.
- Carr, M. (2015). Power plays in global internet governance. *Millennium*, 43(2), 640–659. <https://doi.org/10.1177/0305829814562655>
- Caton, S., & Haas, C. (2020). Fairness in machine learning: A survey. <http://arxiv.org/abs/2010.04053>. arXiv:2010.04053 [cs, stat].
- Chouldechova, A., & Roth, A. (2018). The frontiers of fairness in machine learning. <http://arxiv.org/abs/1810.08810>. arXiv:1810.08810 [cs, stat].
- Collingridge, D. (1980). *The social control of technology*. Open University Press.
- Conference for the Supervision of the International Trade in Arms and Ammunition and in Implements of War, Geneva (1925). *Protocol for the prohibition of the use in war of asphyxiating, poisonous or other gases, and of bacteriological methods of warfare* (1925). Signed at Geneva, on June 17, 1925.
- Cottier, T. (1996). The impact of new technologies on multilateral trade regulation and governance. *Chicago-Kent Law Review*, 72, 415.
- Crawford, J., & Brownlie, I. (2019). *Brownlie's principles of public international law*. USA: Oxford University Press.
- Christopher, L. (2019). Atkinson. Public policy and instrumentalism. Public policy, and governance. In Ali Farazmand (Ed.), *Global Encyclopedia of Public Administration, Public Policy, and Governance*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-20928-9>

- Dany, C. (2013). *Global governance and NGO participation: Shaping the information society in the United Nations*. Online access with subscription: Proquest Ebook Central. Routledge.
- Dargan, J. (2021, April 29). *15 countries with national quantum initiatives*. Quantum Insider. Retrieved on March 03, 2021, from <https://thequantuminsider.com/2021/04/29/15-countries-with-national-quantum-initiatives/>
- Davidson, J. (2021, August 16). *Foreign investment limits “strangling” quantum start-ups*. Australian Financial Review. Retrieved August 20, 2021, from <https://www.afr.com/technology/foreign-investment-limits-strangling-quantum-computing-20210813-p58ik5>
- Degen, C. L., Reinhard, F., & Cappellaro, P. (2017). Quantum sensing. *Review of Modern Physics*, 89(3), 035002. <https://doi.org/10.1103/RevModPhys.89.035002>
- Dryzek, J. S. (2012). *Foundations and frontiers of deliberative governance*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199562947.001.0001>
- Dwork, C., Hardt, M., Pitassi, T., Reingold, O., & Zemel, R. (2012). Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12*, pages 214–226. Association for Computing Machinery. <https://doi.org/10.1145/2090236.2090255>
- Dworkin, Gerald. (1988). *The theory and practice of autonomy*. New York: Cambridge University Press.
- Egan, B. J. (2017). International law and stability in cyberspace. *Berkeley Journal of International Law*, 35, 169. <https://doi.org/10.15779/Z38CC0TT2C>
- Einstein, D. (2014). Extension of the transdiagnostic model to focus on intolerance of uncertainty: A review of the literature and implications for treatment. *Clinical Psychology: Science and Practice*, 21, 280.
- European Commission. (2021). *Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. Retrieved May, 10,2022, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. *Nature*, 563, 465–467. <https://doi.org/10.1038/d41586-018-07449-z>
- Feenberg, A. (1999). *Questioning Technology*. Routledge. <https://doi.org/10.4324/9780203022313>
- Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6), 467–488. <https://doi.org/10.1007/BF02650179>
- Finke, D. (2015). *Startup/private companies*. Quantum Computing Report. Retrieved January 10, 2022, from <https://quantumcomputingreport.com/privatestartup/>
- Fisher, E., Jones, J., & Schomberg, R. (Eds.). (2006). *The precautionary principle and public policy decision making: A prospective analysis of the role of the precautionary principle for emerging science and technology*. Edward Elgar Press.
- Forge, J. (2010). A note on the definition of “dual use”. *Science and Engineering Ethics*, 16(1), 111–118. Springer. <https://doi.org/10.1007/s11948-009-9159-9>
- Foucault, M., & Sheridan, A. (2002). *Archaeology of knowledge*. Archaeology of Knowledge: Routledge.
- Frantz, D. (2017, October 4). *Artificial intelligence: Why a global dialogue is critical*. OECD. Retrieved February, 12,2022, from <https://www.oecd-forum.org/posts/21562-artificial-intelligence-why-a-global-dialogue-is-critical>
- Fraundorfer, M. (2017). Brazil’s organization of the NETmundial meeting: Moving forward in global internet governance. *Global Governance*, 23, 503.
- Friedman, B. (2008). Embodying values in technology: Theory and practice. In M. Flanagan, D. Howe & H. Nissenbaum (Eds.) *Information Technology and Moral Philosophy*. (pp. 322–353). Cambridge University Press. <https://doi.org/10.1017/CBO9780511498725.017>
- Friedman, B., Kahn, P. H., Jr, & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang & D. Galletta (Eds.), *Human-computer interaction in management information systems: Foundations* (pp. 348–372). London: M. E. Sharpe.
- Garisto, D. (2021, July 15). *China Is Pulling Ahead in Global Quantum Race, New Studies Suggest*. Scientific American. Retrieved February 10,2022, from <https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/>
- Giacomin, J. (2014). What is human centred design? *The Design Journal*, 17(4), 606–623. <https://doi.org/10.2752/175630614X14056185480186>
- Gibney, E. (2016). Inside Microsoft’s quest for a topological quantum computer. *Nature*. Nature Publishing Group. <https://doi.org/10.1038/nature.2016.20774>
- Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145–195. American Physical Society. <https://doi.org/10.1103/RevModPhys.74.145>

- Global Industry Analysts, Inc. (2021). *Quantum Cryptography - World Market Report*. StrategyR. Retrieved February, 10, 2022, from <https://www.strategyr.com/market-report-quantum-cryptography-forecasts-global-industry-analysts-inc.asp>
- Google. (2022). Responsible AI Toolkit. Retrieved February 10, 2022, from https://www.tensorflow.org/responsible_ai
- Graham, J. (2004, January 15). *The perils of the precautionary principle: Lessons from the American and European experience*. Heritage Foundation. Retrieved February, 15, 2022 from <https://www.heritage.org/government-regulation/report/the-perils-the-precautionary-principle-lessons-the-american-and>
- Gunningham, N., Grabosky, P., & Sinclair, D. (1998). *Smart Regulation: Designing Environmental Policy*. Oxford University Press.
- Gunningham, N., & Rees, J. (1997). Industry self-regulation: An institutional perspective. *Law & Policy*, 19(4), 363–414. <https://doi.org/10.1111/1467-9930.t01-1-00033>
- Guston, D. H. (2014). Understanding ‘anticipatory governance’. *Social Studies of Science*, 44(2), 218–242. Sage. <https://doi.org/10.1177/0306312713508669>
- Guzman, A. T., & Meyer, T. L. (2010). International Soft Law. *Journal of Legal Analysis*, 2(1), 171–225. Oxford University Press. <https://doi.org/10.2139/ssrn.1353444>
- Haggart, B., Tusikov, N., & Scholte, J. A. (2021). *Power and authority in internet governance: return of the state?* Routledge global cooperation series: Routledge.
- Harding, R. & Fisher, E. (Eds.) (1999). *Perspectives on the precautionary principle*. Federation Press. <https://doi.org/10.4414/smw.2018.14688>
- Harris, E. D., Rosner R., Acton J. M., & Lin, H. (2016). *Governance of dual-use technologies: Theory and Practice*. American Academy of Arts and Sciences.
- Hemenway, D. (1980). *Performance vs. design standards*. US Department of Commerce: National Bureau of Standards.
- Holter C. T., Inglesant, P., & Jirotko, M. (2021). Reading the road: Challenges and opportunities on the path to responsible innovation in quantum computing. *Technology Analysis & Strategic Management*, 1–13. <https://doi.org/10.1080/09537325.2021.1988070>
- Hoven M. J., Vermaas P. E., & Poel. (2015). *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*. Springer. <https://doi.org/10.1007/978-94-007-6970-0>
- Hurst, A. (2022, March 2). *NATO successfully tests communication over post-quantum VPN*. Information Age. Retrieved March, 4, 2022, from <https://www.information-age.com/nato-successfully-tests-communication-over-post-quantum-vpn-123498872/>
- Ienca, M., & Vayena, E. (2018). Dual use in the 21st century: Emerging risks and global governance. *Swiss Medical Weekly*, 148, w14688. <https://doi.org/10.4414/smw.2018.14688>
- Inoguchi, T., & Quynh Le, L. T. (2020). Sovereign states’ participation in multilateral treaties. In *The Development of Global Legislative Politics: Rousseau and Locke Writ Global* (pp. 33–71). Springer. https://doi.org/10.1007/978-981-32-9389-2_4
- International Court of Justice. (1949). *Corfu Channel Case (United Kingdom v. Albania); Assessment of Compensation*. 15 XII 4 International Court of Justice (ICJ). *I.C.J. Reports 1949*, p. 244; General List No. 1.
- International Court of Justice. (1996). *Legality of the threat or use of nuclear weapons (Advisory Opinion)*. ICJ Reports 1996, p. 226.
- Johnson, W. G. (2018). Governance tools for the second quantum revolution. *Jurimetrics*, 59, 487.
- Karlsson-Vinkhuyzen, S. I., & Vihma, A. (2009). Comparing the legitimacy and effectiveness of global hard and soft law: An analytical framework. *Regulation & Governance*, 3(4), 400–420. <https://doi.org/10.1111/j.1748-5991.2009.01062.x>
- Kennedy, S. (2015, June 1). *Made in China 2025*. Centre for Strategic & International Studies. Retrieved February, 11, 2022, from <https://www.csis.org/analysis/made-china-2025>
- Kimble, H. J. (2008). The quantum internet. *Nature*, 453, 1023–1030. Nature Publishing Group. <https://doi.org/10.1038/nature07127>
- Kop, M. (2021, March 30). *Establishing a legal-ethical framework for quantum technology*. Yale Journal of Law & Technology. Retrieved June, 30, 2021, from <https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology>
- Kop, M. (2021). *EU Artificial Intelligence Act: The European approach to AI*. Stanford-Vienna Transatlantic Technology Law Forum: Transatlantic Antitrust.
- Kop, M. (2021). Quantum computing and intellectual property law. *Berkeley Technology Law Journal*, 35(3).

- Koops, B. (2006). *Should ICT regulation be technology-neutral?* In Bert-Jaap Koops, editor. Starting points for ICT regulation: Deconstructing prevalent policy one-liners. TMC Asser Press.
- Lessig, L. (2000). *Code and other laws of cyberspace*. New York: Basic Books.
- Lloyd, S., Shapiro J. H., Wong F. N. C., Kumar, P., Shahriar, S. M., & Yuen, H. P. (2004). Infrastructure for the quantum internet. *ACM SIGCOMM Computer Communication Review*, 34(5), 9–20. <https://doi.org/10.1145/1039111.1039118>
- Maas, M. M. (2019). International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order. *Melbourne Journal of International Law*, 20(1), 29–57. <https://doi.org/10.3316/informit.20190903016408>
- Mandel, G. N. (2009). Regulating Emerging Technologies. *Law, Innovation and Technology*, 1(1), 75–92. <https://doi.org/10.1080/17579961.2009.11428365>
- Marchant, G., Allenby, B., & Herkert, J. (2011). *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem*. Netherlands: Springer.
- Moses, L. B. (2017). Regulating in the Face of Sociotechnical Change. In R. Brownsword, E. Scotford & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology* (pp. 573–596). <https://doi.org/10.1093/oxfordhb/9780199680832.013.49>
- Nielsen, M. A., & Chuang, I. L. (2011). *Quantum computation and quantum information: 10th Anniversary Edition*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511976667>
- OECD. (2021). *The OECD Artificial Intelligence Policy Observatory*. OECD. Retrieved February, 14, 2021, from <https://oecd.ai/>
- Paddock, L. (2010). An integrated approach to nanotechnology governance. *UCLA Journal of Environmental Law and Policy*, 28, 251.
- Perrier, E. (2021). Ethical Quantum Computing: A Roadmap. arXiv:2102.00759 [quant-ph] <https://arxiv.org/abs/2102.00759>
- Perrier, E. (2021). Quantum Fair Machine Learning. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 843–853. Association for Computing Machinery. <https://doi.org/10.1145/3461702.3462611>
- Popp, R., Horowitz, L., & Wenger, A. (2016). *Negotiating the Nuclear Non-Proliferation Treaty: Origins of the nuclear order*. Taylor & Francis. <https://doi.org/10.4324/9781315536576>
- Preskill, J. (2021). Quantum computing 40 years later. arXiv preprint <http://arxiv.org/abs/2106.10522>. arXiv:2106.10522.
- Prosser, T. (2010). *The Regulatory Enterprise: Government, Regulation, and Legitimacy*. Oxford University Press.
- Purdy, G. (2010). ISO 31000: 2009—Setting a new standard for risk management. *Risk Analysis: An International Journal*, 30(6), 881–886. <https://doi.org/10.1111/j.1539-6924.2010.01442.x>
- Rawls, J. (1993). *Political liberalism*. New York: Columbia University Press.
- Rawls, J. (1999). *A theory of justice*. Oxford University Press.
- Rayfuse, R. (2017). Public International Law and the Regulation of Emerging Technologies. In R. Brownsword, E. Scotford & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology* (pp. 500–521). <https://doi.org/10.1093/oxfordhb/9780199680832.013.22>
- Raymer, M. G., & Monroe, C. (2019). The US National Quantum Initiative. *Quantum Science and Technology*, 4(2), 020504. IOP Publishing. <https://doi.org/10.1088/2058-9565/ab0441>
- Raz, J. (1986). *The morality of freedom*. Oxford: Clarendon.
- Richardson, H. (2003). *Democratic autonomy: Public reasoning about the ends of policy*. Oxford: Oxford University Press.
- Rohde, P. P. (2021). *The Quantum Internet: The Second Quantum Revolution*. Cambridge University Press.. <https://doi.org/10.1017/9781108868815>
- Rosen, H. S., & Gayer, T. (2010). *Public finance*. McGraw-Hill/Higher Education: McGraw-Hill series. in economics.
- Rothstein, H., Huber, M., & Gaskell, G. (2006). A theory of risk colonization: The spiralling regulatory logics of societal and institutional risk. *Economy and Society*, 35, 91.
- Schermers, H. G., & Blokker, N. M. (2021). *International Institutional Law* (4th ed.). BRILL.
- Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- Schmitt, M. N. (2021). Cybersecurity and International Law. In R. Geiss & N. Melzer (Eds.), *The Oxford Handbook of the International Law of Global Security* (pp. 661–678). <https://doi.org/10.1093/law/9780198827276.003.0037>

- Seidl, D. (2007). Standard Setting and Following in Corporate Governance: An Observation-Theoretical Study of the Effectiveness of Governance Codes. *Organization*, 14(5), 705–727. <https://doi.org/10.1177/135050840708031>
- Sinclair, D. (1997). Self-Regulation Versus Command and Control? Beyond False Dichotomies. *Law & Policy*, 19(4), 529–559. <https://doi.org/10.1111/1467-9930.00037>
- Smith, P. T. (2018). Cyberattacks as Casus Belli: A Sovereignty-Based Account. *Journal of Applied Philosophy*, 35(2), 222–241. <https://doi.org/10.1111/japp.12169>
- Solis, G. (2010). *The Law of Armed Conflict: International Humanitarian Law in War*. Cambridge University Press. <https://doi.org/10.1017/CBO9781316471760>
- Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy*, 42(9), 1568. <https://doi.org/10.1016/j.respol.2013.05.008>
- Tassey, G. (2000). Standardization in technology-based markets. *Research Policy*, 29, 587–602. [https://doi.org/10.1016/S0048-7333\(99\)00091-8](https://doi.org/10.1016/S0048-7333(99)00091-8)
- Union of International Associations. (2021). *Yearbook of International Organizations 2021-2022, Volumes IA & IB*. BRILL.
- United States (2018). *National Quantum Initiative Act*. Public Law 115-368.
- United Nations. (1969). Vienna Convention on the Law of Treaties. *UNTS* 1155, 331.
- United Nations. (1970). Treaty on the Non-Proliferation of Nuclear Weapons. *UNTS*, 729, 161.
- United Nations. (1972). Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction. *UNTS*, 1015:163, 1972.
- United Nations. (1980). Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. *UNTS*, 1342, 137.
- United Nations. (1993). Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons. *UNTS*, 1974, 317.
- United Nations. (1996). Conference of the States Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects: Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and other Devices (Protocol II) as Amended, and Protocol on Blinding Laser Weapons (Protocol IV). *International Legal Materials*, 35(5), 1206–1218. <https://doi.org/10.1017/S0020782900024438>
- United Nations. (2013). *Human Development Report 2013-The Rise of the South: Human Progress in a Diverse World*. United Nations Development Programme.
- United Nations. (2019). *The Impact of Rapid Technological Change on the Sustainable Development Goals and Targets*. *Technical Report A/RES/73/17*. United Nations General Assembly.
- Van den Hoven, J. (2017). The Design Turn in Applied Ethics. In J. Van den Hoven, S. Miller, & T. Pogge (Eds.), *Designing in Ethics* (pp. 11-31). Cambridge University Press. <https://doi.org/10.1017/9780511844317.002>
- Van Grembergen, W. (2004). *Strategies for Information Technology Governance*. Idea Group Publishing.
- Webb, K. R., & Carleton Research Unit for Innovation, Science and Environment (2004). *Voluntary Codes: Private Governance, the Public Interest and Innovation*. Carleton Research Unit for Innovation, Science and Environment, Carleton University.
- Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362 (6412). <https://doi.org/10.1126/science.aam928>
- Winickoff, D. E., & Pfothenauer, S. M. (2018). Technology Governance and the Innovation Process. In *OECD Science, Technology and Innovation Outlook 2018: Adapting to Technological and Societal Disruption* (pp. 221–240). OECD Publishing Paris. https://doi.org/10.1787/sti_in_outlook-2018-15-en
- World Economic Forum. (2020, December 2). *Global Technology Governance Report 2021*. World Economic Forum. Retrieved February, 8, 2022, from <https://www.weforum.org/reports/global-technology-governance-report-2021/>
- World Economic Forum. (2022, January 19). *Quantum Computing Governance Principles - Insight Report*. Retrieved January, 20, 2022, from <https://www.weforum.org/reports/quantum-computing-governance-principles/>
- Wright QC, J. (2018). *Cyber and International Law in the 21st Century*. Chatham House.
- Zimmermann, A. (2019). *Christian J Tams, Karin Oellers-Frahm, and Christian Tomuschat*. The statute of the International Court of Justice: A commentary. Oxford University Press.

Authors and Affiliations

Elija Perrier^{1,2,3,4} 

- ¹ Centre for Quantum Software and Information, University of Technology, Sydney, 11 Broadway, Sydney 2000, NSW, Australia
- ² Humanising Machine Intelligence Programme, The Australian National University, Canberra 2601, ACT, Australia
- ³ Project Q (Carnegie Corporation of New York), University of Sydney, Camperdown, Sydney 2006, NSW, Australia
- ⁴ Quantum Meta-Ethics Project (Australian Department of Foreign Affairs and Trade), University of Sydney, Camperdown, Sydney 2006, NSW, Australia