Quantum Science and Technology

OPEN ACCESS

RECEIVED
13 April 2023

REVISED
28 February 2024

ACCEPTED FOR PUBLICATION
25 March 2024

PUBLISHED
22 April 2024

PAPER

Ten principles for responsible quantum innovation

Mauritz Kop[1,*], **Mateo Aboy**[2,1], **Eline De Jong**[3,1], **Urs Gasser**[4,1], **Timo Minssen**[5], **I Glenn Cohen**[6], **Mark Brongersma**[7,1], **Teresa Quintel**[8], **Luciano Floridi**[9] **and Raymond Laflamme**[10]

[1] Stanford Center for Responsible Quantum Technology, Stanford Law School, Stanford University, Stanford, CA, United States of America
[2] Faculty of Law, University of Cambridge, Cambridge, United Kingdom
[3] Institute for Logic, Language and Computation at the University of Amsterdam, Amsterdam, The Netherlands
[4] TUM School of Social Sciences and Technology at the Technical University of Munich, Munich, Germany
[5] CeBIL, Faculty of Law, University of Copenhagen, Copenhagen, Denmark
[6] Harvard Law School, Harvard University, Cambridge, MA, United States of America
[7] Material Science and Engineering, Stanford University, Stanford, CA, United States of America
[8] European Centre on Privacy and Cybersecurity (ECPC), Maastricht University, Maastricht, The Netherlands
[9] Digital Ethics Center, Yale University, New Haven, CT, United States of America
[10] Institute for Quantum Computing, University of Waterloo, Waterloo, Canada
[*] Author to whom any correspondence should be addressed.

E-mail: mkop@stanford.edu

Keywords: responsible quantum technology, quantum safeguarding, engaging & advancing, quantum-AI ethics & governance, responsible quantum innovation, quantum R&D, responsible research and innovation (RRI)

Abstract

This paper proposes a set of guiding principles for responsible quantum innovation. The principles are organized into three functional categories: *safeguarding, engaging*, and *advancing* (SEA), and are linked to central values in responsible research and innovation (RRI). Utilizing a global equity normative framework and literature-based methodology, we connect the quantum-SEA categories to promise and perils specific to quantum technology (QT). The paper operationalizes the responsible QT framework by proposing ten actionable principles to help address the risks, challenges, and opportunities associated with the entire suite of second-generation QTs, which includes the quantum computing, sensing, simulation, and networking domains. Each quantum domain has different technology readiness levels, risks, and affordances, with sensing and simulation arguably being closest to market entrance. Our proposal aims to catalyze a much-needed interdisciplinary effort within the quantum community to establish a foundation of quantum-specific and quantum-tailored principles for responsible quantum innovation. The overarching objective of this interdisciplinary effort is to steer the development and use of QT in a direction not only consistent with a values-based society but also a direction that contributes to addressing some of society's most pressing needs and goals.

1. Introduction

As we stand on the cusp of the second quantum revolution, we face unprecedented opportunities and challenges in the field of quantum technology (QT) [1]. A recent empirical landscape study showed an exponential increase in the number of patents directed to QT inventions, illustrating the sheer pace and breadth of quantum innovation [2]. With the potential to revolutionize computation, cybersecurity, communication and sensing, QT and its anticipated future uses are poised to redefine the way we understand and interact with the world. Yet, with such power shifts fueled by technological advancements comes the responsibility to innovate thoughtfully and conscientiously. But what does it mean to develop and use QT responsibly? How do we ensure that this transformative technology benefits society, minimizes risks, and remains ethical?

As is the case with large artificial intelligence (AI) models with emergent capabilities such as generative adversarial networks, the rapid development and deployment of QT demands a proactive, holistic and

principle-based approach to ensure that that quantum innovation is managed responsibly in order to ensure that its potential is realized in a manner that is beneficial to society [3, 4].

QT is not new. However, the rise of second-generation (2G) QTs has the potential to revolutionize many fields. The suite of 2G QT consists of various quantum domains, branches, or application areas, including not limited to quantum computing and cryptography, sensing and metrology, simulation, and networking and communication. Each maturing quantum domain has different technology readiness levels (TRLs), risks, and affordances, with sensing and simulation arguably being closest to market entrance. By directly harnessing unique [5, 6] quantum mechanical properties such as superposition, entanglement, and tunneling (box 1), the suite of 2G QT opens up a myriad of applications that will likely impact society at large [7–11]. Given QT's inherent ability to solve complex problems that classical technologies struggle with, the recent progress of QT promises a new era of scientific advancements and industrial applications [12–15]. This includes QT/AI hybrids [16] where the quantum computer (QC) is used as an accelerator to solve computationally intractable problems for classical computers and AI, such as simulation [17] of quantum chemistry to accelerate novel drug development. That said, alongside these beneficial uses, there are material risks that differ in scope and magnitude across the various quantum domains. For instance, quantum computing also has the potential to break the RSA encryption systems that we currently use to the ensure privacy across internet communications [18, 19]. Thus, alongside the vast potential for innovation, there are significant ethical, social, and QT governance implications that must be addressed to ensure responsible growth and adoption [20–22].

Elsewhere [23] it was argued that the great potential of QT calls for a responsible approach to innovation [24–28]. Building on existing literature on responsible research and innovation (RRI) [29–33] the study by Kop *et al* [23] analyzed the risk posed by quantum computing to information security as an illustrative example of the challenges ahead and introduced a responsible QT (RQT) framework that incorporates ethical, legal, social, and policy implications (ELSPI) into the quantum research and development (R&D) process, while responding to the key RRI dimensions of anticipation, inclusion, reflexivity, and responsiveness (AIRR) [34]. The authors argued that quantum innovation should be guided by a methodological framework for RQT, aimed at jointly (1) *safeguarding* against risks by proactively addressing them, (2) *engaging* stakeholders in the innovation process, and (3) *advancing* QT; and called for operationalizing the RQT framework by establishing a set of principles to guide future quantum innovation.

In this paper, building upon the international conversation on RRI in quantum computing that has been evolving since 2015 [24–36], we seek to operationalize the RQT framework [23] by proposing ten guiding principles to help navigate the complex terrain of QT development and application. In order to operationalize the three guidelines of safeguarding, engaging, and advancing (SEA) society, we identified (potential) issues along these lines based on current literature. Furthermore, we connected these issues and their discussion to the dimensions of RRI as articulated by the European Commission [29, 36, 37], which are grounded in the AIRR framework for RRI developed by Stilgoe *et al* [35]. Central in this account of RRI are the process dimensions of anticipation & reflectivity, diversity & inclusion, openness & transparency, and responsiveness & adaptivity to change. By connecting identified issues with these dimensions of RRI, we aim to consociate the proposed principles with the European Commission's current approach to RRI, and with the RRI-literature.

Utilizing a global equity normative framework and literature-based methodology, we link the quantum-SEA categories to the opportunities and challenges specific to QT and provide actionable recommendations for their adoption, actively steering the field into a direction congruent with values-based societies [38]. This work builds on and complements the previous analyses on RQT by Kop *et al* [23, 39, 40] and the World Economic Forum principles for QC [41] to identify the ethical, legal, social, and policy issues of QT along the SEA-categories.

Analytically, the principles are aimed at ensuring that ethical, legal, cultural, socio-economic, and philosophical dimensions [42] are identified and discussed while QTs are still shapeable [43]. From a normative perspective, the objective is to capture and promote beneficial opportunities expected from quantum innovation while managing potential downsides by putting into place technical, organizational, and policy guardrails appropriate to the risk. At present, many of QT's ramifications seem hypothetical, and indeed many societal implications remain unknown. It is precisely this moment, when the state of technology is still in flux, that we have a unique opportunity and responsibility to shape its maturity toward desirable societal outcomes [44]. The ten principles we propose in this article should be considered as a starting point for such an interdisciplinary effort (figure 1). As our knowledge about quantum-ELSPI develops over the coming years, we will be able to further specify, replace, or add principles in order to provide practical guidance.

Box 1: Superposition, entanglement and tunneling

Superposition, entanglement, and tunneling are three central principles in quantum physics [45]. They refer to the phenomena of particles existing in multiple states at the same time (*superposition*), particles having stronger correlations than is permitted by classical physics (*entanglement*), and the ability of particles to cross energy barriers (*tunneling*). 2G QTs are based on *directly harnessing* such quantum phenomena for practical applications such as quantum sensing, quantum computing and quantum communications [1]. This makes QTs fundamentally different from those based on classical physics, and could imply a 'quantum advantage' over our existing technologies.

Category	Topic	Aim	RRI-value	Principle
Safeguarding	Information security	Addressing security threats	Anticipation & Reflection	1. *Make information security an integral part of QT*
	Dual use	Addressing risks of dual use	Anticipation & Reflection	2. *Proactively anticipate the malicious use of quantum applications*
	Quantum race	Addressing a winner-takes-all dynamic	Anticipation & Reflection	3. *Seek international collaboration based on shared values*
Engaging	Quantum gap	Engaging states	Openness & Transparency	4. *Consider our planet as the sociotechnical environment in which QT should function*
	IP	Engaging institutions	Openness & Transparency	5. *Incentivise innovation while being as open as possible and as closed as necessary*
	Inclusion	Engaging people	Diversity & Inclusion	6. *Pursue diverse R&D communities in terms of disciplines and people*
Advancing	Societal relevance	Advancing society	Responsiveness & Adaptation to change	7. *Link quantum R&D explicitly to desirable societal goals*
	Complementary innovation	Advancing technology	Responsiveness & Adaptation to change	8. *Actively stimulate sustainable, cross-disciplinary innovation*
	Responsibility	Advancing our understanding of responsible QT	Responsiveness & Adaptation to change	9. *Create an ecosystem to learn about the possible uses and consequences of QT applications*
	Education and Dialogue	Advancing our collective thinking and education about QT and its impact	Responsiveness & Adaptation to change	10. *Facilitate dialogues with stakeholders to better envision the future of QT*

Figure 1. Ten principles for responsible quantum innovation.

2. Safeguarding principles

The safeguarding category of principles supports proactive risk management and responds primarily to the RRI dimension of *anticipation & reflection*. In particular, the safeguarding principles tackle proactive risk management, delving into information security, dual-use, and the quantum race. By stressing the importance of risk-based quantum impact assessments (QIAs), anticipating malicious use, and fostering international collaboration based on shared values, these principles help build a solid foundation for RQT innovation.

2.1. Information security: make information security an integral part of QT

Principle 1 embraces information security as an integral part of QT. This perspective is considered the starting point for addressing information security risks including threats to data privacy [11]. Quantum algorithms have the potential to break current cryptography protocols [2, 46], hence threatening the information security of existing information technologies [47]. This would destabilize society—as it could expose extensive swaths of information currently regarded as private and confidential—ranging from sensitive personal data to financial sector and national security information assets [47–49]. According to the latest Quantum Threat Timeline Report, the majority of experts' estimate of the likelihood of a QC capable of breaking RSA-2048 in 24 h is 15–20 years [50]. There are ongoing research efforts to develop novel quantum algorithms for integer factorization designed to optimize the required quantum resources (i.e. qubit-saving quantum algorithms) [50–52].

Moreover, the potential quantum cybersecurity threat not only depends on the timeframe of sufficiently strong QCs, but also on the time needed to migrate from regular encryption to quantum-safe, or post quantum cryptography [53, 54]. Innovators share the responsibility for the inherent impact of their creations. Thus, research on and development of quantum computing should be accompanied by risk-based QIAs focused on information security risks and implementing controls to mitigate such risks. This includes the implementation of state-of-the-art information security management systems such as ISO27001 to protect information assets from a particular QT R&D program. Notably, this requires the implementation of quantum-safe information security controls that can ensure our information systems and communications are resistant to attacks by cryptographically relevant QCs [47]. At a minimum, QC should not advance more rapidly than the availability of quantum-resistant cryptographic algorithms. Such algorithms must be safe and secure against cryptanalytic attacks by QC that employ quantum algorithms breaking common public key cryptographic systems in use today [46]. This calls for researching and investing in post-quantum cryptography initiatives, as well as post-quantum information security programs. The National Institute of Standards and Technology (NIST) competition for post-quantum cryptography standards demonstrates such much needed applied responsible quantum computing research efforts [54]. Furthermore, the possibility of implementing a strategy 'store now, decrypt later' should provide incentives to start replacing our existing cryptosystems for critical information assets with post-quantum cryptographic systems that are resistant to attacks by quantum algorithms as early as possible [23].

2.2. Dual use: proactively anticipate the malicious use of quantum applications

Principle 2 deals with the proactive anticipation of the malicious use of quantum applications. It aims to prevent the harmful use of QT. Most applications of QT may be used for diverse civilian and military ends ('dual use') [41, 55, 56]. QT innovations could be used to serve society through applications that are relevant to today's grand challenges of providing a prosperous, safe, sustainable [57], and connected world—which could well include military secondary usage and deterrence by governments—but when used by malicious parties it can pose a serious material threat. This dual use character is not unique to QT and has been raised with technologies as diverse as gene editing, biometrics, and nuclear energy. However, as with the closely related case of nuclear power, the stakes with QT are exceptionally high [58], and the suite of QT are expected to transform modern warfare [59]. QTs are categorically different from the technological improvements that we have seen since WWII because of the nature of the advantages that 'quantum dominance' could entail. Imagine being able to crack RSA-2048-bit encryption in 10 s by implementing Shor's algorithm in a fault-tolerant QC [46]. The quantum pioneers could achieve an advantage that is orders of magnitude superior to their classical counterparts resulting in vastly superior computation (optimization, search, and cryptography), communication, and measurement [23]. Consequently, both innovators and regulators [23, 60–62] need to anticipate potentially malicious use of QT by (1) utilizing both technology forecasting [63] and horizon scanning techniques [64] anticipating novel dual use quantum use cases [12, 22] and identify novel use cases that are currently out of sight, in unison with (2) implementing appropriate safeguards at the initial stages of the TRL [2]. Such assessments should be conducted by governments and at the organizational level and linked to certification by independent notified bodies in connection with market introduction. For example, by conducting a dual-use risk assessment examining how a particular QT R&D program or innovation could be used for terrorist or criminal ends, potential risks could be anticipated. Just like any product or service on the market, civil use QT can cause harm too, which could be addressed, in part, by creating or applying product certification, market authorization, liability and insurance schemes. These combined procedures would offer the opportunity to implement appropriate safeguards—such as unilateral and multilateral import/export controls, QT access and capability controls or requiring technological 'kill switches'—to mitigate specific inherent risks for a particular QT application throughout its lifecycle so that residual risks are acceptable [48]. The safeguarding measures above, however, come with their own trade-offs and risks, such as kill switches potentially being misused by governments and private

actors. Similarly, trade, import and export controls can distort fragile supply chains, create critical mineral and rare earth scarcity, or result in unintended counterproductive effects of policy interventions such as promoting innovation investment of the export-controlled nations.

2.3. Quantum race: seek international collaboration based on shared values

Principle 3 seeks international collaboration based on shared values. Given larger geopolitical and winner-takes-all dynamics, investments in QT R&D could take the shape of a global arms race [65–68] where companies and countries with incompatible ideologies or fundamental values compete, and where intellectual property rights (IPRs), trade & state secrets, and antitrust enforcement policies are becoming important assets in national and regional strategies. A quantum arms race can be thought of as rivalry between companies to gain a competitive edge (e.g. developing novel qubit modalities and qubit-saving algorithms) and rivalry between states about national and economic security, (e.g. by forming strategic tech alliances with dominant quantum defense capabilities) [65–67]. Such competition between systemic rivals can be a driver of innovation. That said, this race for national success could also thwart progress if it stymies the opportunity to join forces, especially among partners with mutually aligned values [48, 69], resulting in high costs of lost opportunity. For example, the potential ineligibility of UK scientists from EU's flagship quantum R&D programs after Brexit [68] could exacerbate risks of duplication or not exploiting synergies adequately [70]. The prospect that the forerunner in the field will make crucial decisions about the design and use of QT bears a high risk; similar risks have been identified in the context of other strategically significant technologies like AI [71]. Analogs to nuclear fission, there is also a risk that if QT dominance enters a geopolitical race dynamic, the incentives will skew away from ethically-appropriate one step at a time development; it is easy for countries to imagine that as bad as it would be to fail to build in safeguards aimed at ELSPI [72], it would be far worse to lose the dominance race. Fear of losing the race can de-incentivize building regulatory guardrails, as these are often associated with a chilling effect on innovation (principle 8) [73]. In economic, political, and ethical terms, preventing a winner-takes-all dynamic requires forming broad partnerships and joint efforts toward establishing widely endorsed values-based interoperability standards and protocols for quantum computing, sensing, and networking. This directly taps into the dual nature of most QT (principle 2). To avoid a quantum arms race characterized by large public investments in weaponry and defense [56, 59] states and research institutions should seek international partnerships based on shared values (such as liberal-democracy, human rights, and the rule of law), to accelerate quantum R&D and to actively shape its direction. Capital should flow to QT for social development goals (SDGs) (principle 7). As illustrated by the vision underlying the International Thermonuclear Experimental Reactor project for nuclear fusion [74], seeking international collaboration is particularly relevant during the early phases of QT development. In line with this aim, fundamental quantum research (TRLs 1–3) and pre-competitive (TRLs 4–7) core/base layer QT should be as openly accessible as possible [75, 76]. Ideally, knowledge sharing should be incentivized without ignoring crucial security and resilience risks (see principle 5).

3. Engaging principles

The engaging principles aim to create an inclusive environment for quantum R&D. From bridging the quantum gap to managing intellectual property and cultivating an inclusive R&D environment, these principles ensure that QT benefits reach far and wide. This category of the principles aims to create an inclusive environment for quantum R&D, at the level of countries, organizations, and individuals and responds to the RRI values of *openness & transparency* and *diversity & inclusion.*

3.1. Quantum gap: consider our planet as the sociotechnical environment in which QT should function

Principle 4 advocates considering our planet as the sociotechnical environment in which QT functions. It points to our global interconnectedness and aims to promote equitable and fair access to QT (quantum for all). As quantum R&D is highly complex, infrastructure dependent, and expensive, there is a risk that the technology, without proactive interventions, may remain accessible only to an elite, creating a gap between the 'haves' and 'have-nots.' This 'quantum-divide' is not only morally problematic but also suboptimal from an innovation and sustainability point of view. Actively bridging the quantum divide could contribute to achieving desirable goals, such as leveraging the power of QT in enhancing drug discovery [25]. It could also enable helping address (ecological) sustainability challenges ranging from water management, hyper precision weather forecasting, and lowering the carbon footprint of classical computing and data processing, to development of advanced solar cell concepts, clean fuels, and a variety of chemistries that provide us with fertilizers and food [77]. It could facilitate creating the required technical infrastructure more effectively and on a larger scale. What's more, competition law principles and enforcement actions [78]—in concert with respecting IPRs and allied rights including trade secrets, state secrets, and fair-trade conditions—should

contribute to fair and equitable access to QT and solve market failures (see principle 5) [2]. A permanent forum for transdisciplinary dialogue between Majority World countries and the Global North should be established, being mindful that current epicenters of quantum R&D are in a few restricted environments [79]. It should be a shared R&D objective to develop quantum standards [80], applications, and infrastructure that are inclusive and equitable both within and across nations.

3.2. Intellectual property: incentivize innovation while being as open as possible and as closed as necessary

Principle 5 should aim to incentivize quantum innovation and achieving appropriate degrees of openness in quantum R&D. RRI benefits from sharing insights and approaches [37]. This is especially the case in QT, as only a relatively small number of key players could influence and decide the direction of quantum innovation. The patent system is currently encouraging public disclosure in the field of QT, despite trade secrets potentially being a more commercially viable intellectual property (IP) option at this stage [2]. This preference for trade secrets can be attributed to the early-stage nature of many QTs, the market structure, and emergent business models. Large-cap incumbents with leading market positions tend to benefit from and may favor proposals that weaken patent rights, while new QT entrants are more likely to benefit from stronger patent rights to not only protect their inventions but also attract investment [2]. Notably, in addition to promoting public disclosure, an important aspect of the patent system is the concept of 'secrecy orders.' In certain instances, particularly when dealing with inventions with direct applications to defense and national security, the United States (US) patent system allows for inventions to be classified and subject to secrecy orders. This means that the disclosure of these inventions would be restricted as their publication or dissemination could be detrimental to national security. While this practice is necessary in some cases, it also highlights the need for a careful balance between promoting innovation through public disclosure and protecting sensitive information. For instance, secrecy orders could undermine international collaboration (principle 3). Given the findings of the aforementioned patent landscape study, we recommend that public policy considerations for responsible quantum innovation should take into account the results of evidence-based (empirical) results of IP studies when designing, assessing, and proposing legal and regulatory reforms related to QTs [78]. Additionally, we suggest that further research is needed to clarify the role of IPRs and push incentives in different sectors and technologies, such as quantum sensing & metrology, simulation, computation, imaging, novel materials & devices, and communications & networking, to better inform responsible innovation strategies in the quantum domain. The role of secrecy orders in the patent system should be carefully considered to strike a balance between promoting innovation and protecting sensitive information.

While IP continues to play an important role for incentivizing quantum innovation, beyond the noisy intermediate-scale quantum era, it may be necessary to balance it with other legal regimes, such as competition law [78]. It is essential to tailor existing IP policy—including debates about its reform—to QT and consider it in the context of national and regional security strategies [81]. Funders should promote quantum-open innovation [76, 82] and democratize access to QTs [39, 83] at the base layer while enabling innovators to obtain sufficient levels of IP protection for their inventions to attract the necessary investment [2]. Two decades ago, a similar proposal of opening fundamental technology while allowing IPRs for narrower downstream applications of that technology was made for nanotechnology [84]. This could be accomplished by providing cloud-based access to quantum computing infrastructure, allocating educational resources to learning quantum skills and programming (see principle 9), implementing progressive standard essential patent policies [85] for technologies embedded in QT interoperability standards, and by building and deploying quantum algorithms using open-source software development kits. That said, an important aspect of this effort is also implementing best practices for safeguarding IP including preventing IP theft (see principle 1) via QC CPA [86, 87], NSPM-33 [88] and ITAR [89], as well as addressing associated geostrategic and national security concerns (see principles 2 & 3) [47, 55, 56, 90]. This may require geographic-based restricted access to cloud-based QT and R&D, and targeted export controls that restrict access to key QT enabling technologies while minimizing disruption to fragile supply chains (see principle 3) [47]. Among the tools to consider are the use of secrecy orders as part of the patenting process, export controls, and trade secrets.

3.3. Inclusion: pursue diverse R&D communities in terms of disciplines and people

Principle 6 calls for an inclusive and participatory R&D environment, which includes a diverse R&D community in terms of disciplines and people. Anticipating and addressing considerations about quantum-ELSPI from a broad range of perspectives at an early stage is vital. Later in the development lifecycle, changes to design or use are much harder to implement. Engaging a group of people that is diverse in cultural and professional backgrounds during the R&D phase can prevent potentially irreversible harm and contributes to building a richer quantum workforce that capitalizes on talent in order to cultivate an

inclusive view of the risks and values at play [43]. Building a competitive and inclusive quantum workforce in the US and Europe requires establishing progressive science, technology, and math (STEM) immigration laws. Empirical evidence confirms the positive effect of R&D team diversity on innovative performance [91, 92]. Thus, we recommend including different voices and perspectives during the R&D phase by (i) diversifying communities and teams in terms of discipline, experience, gender, nationality and ethnicity, (ii) implementing participatory public and private feedback mechanisms regarding the functioning of an application in practice, and (iii) closing STEM-related skills—and participation gaps in education sectors most important for QT.

4. Advancing principles

The advancing principles advocate for further QT innovation. Additionally, these principles provide a vision for QT's role in society, interpreting the RRI values of responsiveness and adaptiveness proactively. By underlining QT's societal relevance, complementary innovation, responsibility, and the importance of education and dialogue, these principles inspire a vision of a quantum future worth striving for. This category of principles is aimed at envisioning the role of QT in society, thereby interpreting the RRI values of *Responsiveness & Adaptive to Change* proactively, centering the social environment in which QT will be embedded.

4.1. Societal relevance: link quantum R&D explicitly to desirable societal goals

Principle 7 encourages explicitly directing quantum R&D toward desirable societal goals such as the UN SDG [93]. It aims at unlocking the potential that QT offers for the benefit of humanity and our planet [25, 94]. That said, it recognizes that further R&D and investment is needed to advance 'base-layer' [75] QTs including quantum sensing [9], quantum computing [45], and quantum communications [10]. These enabling fundamental building blocks require significant further private and publicly funded investment and development in order to unlock their potential across application domains [66]. The considerable promises of QT come with the responsibility to apply them wisely. At a minimum, quantum applications must refrain from consolidating or exacerbating existing problems, such as inequality. Beyond a 'do no harm' ethical baseline [27], we advocate that innovations that explicitly link QT innovation to society's grand challenges of providing a safe, sustainable, and prosperous world should be incentivized[11]. This includes, for instance, providing cloud-based QT to lower the cost of advanced computer access for the world's poorest countries. As the overall objective of public and private funding policy, a mission-driven approach can be adopted to encourage R&D programs [95] that focus on pressing societal goals [93] and prioritize them, either as a matter of design choices or envisioned uses. Such socially conscious funding schemes could include tailored programs as part of national science foundations.

4.2. Complementary innovation: actively stimulate sustainable, cross-disciplinary innovation

Principle 8 seeks to stimulate sustainable, cross-disciplinary innovation resulting in positive externalities, spillover effects [96], and a virtuous cycle of progress comparable to that of the semiconductor industry[12]. QT are part of a larger sociotechnical ecosystem, as it *relies on* other technologies and research fields that QT, in its turn, can *enable or enhance*. Innovation should thus not only be envisioned in terms of applications for QT narrowly defined, but also in gestalt of hybridization with other technologies, such as machine learning [16] and biotechnology [2]. This involves investing in aligned quantum-AI (QAI) as exemplified by the Quantum Artificial Intelligence Lab at NASA's Ames Research Center [97]. NASA Quantum AI Laboratory is aimed at improving the agency's ability to address challenging optimization and machine learning problems arising in aeronautics, space exploration missions, and Earth and space sciences. In an era of high paced exponential innovation however, QAI alignment efforts may benefit from steadier, incremental development as less powerful systems are easier to align. To fully explore and take advantage of QT's potential, we recommend creating interdisciplinary research groups (see principle 6), organizational R&D interfaces, and innovation agendas for QT that refer to potential cross-disciplinary applications and use cases [98].

4.3. Responsibility: create an ecosystem to learn about the possible uses and consequences of QT applications

Principle 9 advances the creation of an ecosystem that fosters continuous learning about the possible uses and consequences of QT applications across contexts. The development and adoption of RQT over time requires

[11] For a catalog of nine principles relating to quantum computing, *see* [41]. For ten broader principles and a list of ten risks pertaining to the entire suite of QT, *see* [39].

[12] A virtuous cycle, or positive feedback loop, requires ongoing private and public investments, research, development and engineering efforts, advancing QT (including successful commercial QT applications) and attracting talent [112].

feedback loops to track and assess the risks and opportunities of QT at the application level [99]. Given the current state of uncertainty, it is essential to create a learning ecosystem where QT can be applied to gain insights into ethical, legal, societal, and policy aspects and develop a deep understanding of what 'RQT' entails. The goal is to ensure that this learning process occurs as early and responsibly as possible, avoiding any costs of learning being distributed unequally among different members of society, for instance already underserved or vulnerable communities. One method to advance responsible quantum ecosystems while learning about the possible uses and consequences of QT applications, is by implementing expert-based QIAs. QIA can be utilized to influence and shape the innovation process, guide the design of the technology at a very early stage, cultivate a deeper understanding about the dual use character of QT, and connect natural science and engineering inquiries in quantum R&D to social sciences, humanities and policy strategy from day one, before the technology becomes locked-in [100]. Similar flexible soft law instruments such as QT sandboxes, certifications, benchmarks, international standards, best practices, moral guides, physics de-risking instruments, voluntary codes of conduct and life cycle auditing [64] are among the tools to create a responsible quantum learning ecosystem [39].

4.4. Education and dialogue: facilitate dialogues with stakeholders to better envision the future of QT

Principle 10 encourages societal dialogue about the future of QT. It aims to engage society in actively envisioning and shaping that future. Providing accessible QT educational resources and facilitating discussions with stakeholders, enables a collective vision of a quantum future worth wanting. To be empowered to participate in such debates, people must have a basic understanding of QT and its uses. This is challenging, as the basics of QT (i.e. quantum physics are not only highly complex but also counterintuitive) [101, 102]. Our common-sense acquired by daily interaction with the familiar macro level world may be helpful to intuitively understand and use technologies based on classical physics such as cameras or cars, but less so for QT. Nonetheless, we should work on ways to familiarize people with QT and encourage quantum literacy and intuition—which includes teaching and informing policymakers, legislators and the judiciary about principled approaches and responsible use—so that they can join the discussion about its implications. Educational materials should be accessible to broad and diverse audiences, for example, by designing accessible online national QT courses aimed at different levels of engagement from the general audience to the QT workforce (see principle 9), and by initiatives such as the European Competence Framework for Quantum Technologies [103, 104]. In addition to larger societal debates, deliberative democracy models like stakeholder panels, shadow boards, citizen juries, or youth labs could serve as participatory mechanisms during both R&D and implementation phases to reflect on specific applications [83].

5. Balancing safeguarding and advancing principles

Our proposed principles are not designed to be independent of each other. Instead, they are in an interactive relationship and their interplay can be optimized strategically to help create the conditions for sustainable quantum innovation over the long term. Perhaps counterintuitively, their overlap and interconnectedness are a feature and not a bug by broadening the available 'solution' space and levers available to work toward responsible quantum innovation.

The *engagement* principles, for instance, play a crucial role in balancing the *safeguarding* and *advancing* principles by encouraging inclusivity and competition in QT, while promoting awareness of QT issues in society through education and cross-sector dialogue with stakeholders across sectors. The *safeguarding* and *advancing* principles, in turn, are two key components of a fit-for-purpose QT regulatory framework. They are interrelated and should be jointly optimized to promote quantum innovation [105]. For instance, the safeguarding principles help manage the risks of dominant players achieving monopolistic competitive advantage by restricting access to essential quantum infrastructure, while the advancing principles promote access to key quantum infrastructures by encouraging open access to cloud-based QCs, open quantum interoperability standards and protocols, and open-source quantum development tools.

The insight that *safeguarding* can at times be better achieved by *advancing* QT instead of merely seeking to optimize safety alone offers another illustration of the productive dynamics among the principles. In the case of cybersecurity, for instance, advancing quantum computing and quantum cryptography can help accomplish safeguarding objectives by developing new quantum cryptographic protocols that are resistant to quantum attacks. Similarly, by promoting open access to key quantum infrastructures and encouraging the creation of novel hardware, algorithms, and software solutions, one can increase economic growth and competitiveness while also managing the downside risks associated with dominant players achieving monopolistic competitive advantage by restricting access to essential quantum infrastructure [106].

These interactions among principles apply beyond the corporate competitive dynamics. At the global geopolitical level, an *advancing* QT strategy to ensure overall technological leadership in QT is crucial to

achieving the underlying *safeguarding* objectives. This way, a 'Sputnik moment' or 'Soviet missile gap' for quantum can be prevented [107]. Conversely, without *safeguarding* QT advances with appropriate *dual-use* export controls that do not distort interoperability [108], and IP rights, the benefits of such R&D investments and resulting QT innovations could end up accruing to geopolitical adversaries.

6. Conclusion: a path forward

QT roadmaps developed by governments, companies, and consulting firms worldwide anticipate various opportunities, challenges, and risks arising within the next 25 years. Some challenges demand immediate attention, such as establishing practical solutions to protect privacy [109] and ensure information security [110] in light of quantum computing's threat to widely used public key cryptosystems[13]. Other ELSPI of QT may emerge in the longer term, but proactive measures are necessary to guarantee responsible quantum R&D. Previous cycles of technological innovation—including currently AI—teach us that important ELSPI that can emerge in the longer term [72].

The ten quantum SEA-principles proposed in this article aim to promote responsible quantum R&D by embedding shared principles and values into the policies and practices of quantum innovators and stakeholders. These principles are interoperable with shared RRI values [6] while addressing the unique nature of QT. Our interdisciplinary effort seeks to steer the development and use of QT in a direction that aligns with a values-based society and contributes to addressing society's most pressing needs and goals.

The quantum SEA-principles are intended to be complementary to existing frameworks for Responsible 4IR Technology, such as the IEEE Ethically Aligned Design Principles, the Asilomar AI Principles, FAIR Data, the Trustworthy AI paradigm, and the WHO guidance on the ethical use of health AI. Moreover, these principles are designed to apply to technological synergies such as quantum–classical interactions and QAI hybrids. However, since most of QT's ramifications remain unknown, we must approach the implementation of these principles with caution, continuously evaluating and updating them based on our collective experiences.

Looking into the future, responsible quantum innovation principles apperceived by ELSPI considerations can inform debates on how to regulate QT. This complex and challenging task should be taken on before the technology becomes locked-in and entrenched [44, 111]. Crucially, such a regulatory framework must take into account the unique and counter-intuitive properties of applied quantum phenomena, their dual-use nature, and the need to balance open innovation, fair competition [2, 78], value appropriation, and risk management [39]. As with other domains such as genomics [13], it is essential that quantum-ELSPI work be funded alongside and ideally integrated into opportunities for research funding in QT. In the long run, we anticipate the emergence of a legal and infrastructural ecosystem that includes both horizontal and industry-specific frameworks, such as a Quantum Governance Act or Global Quantum Treaty. Although self-regulation is not enough within the context of QT given its expected power ramifications, soft law instruments based on existing quantum use cases could supplement robust legal frameworks. In a risk-based regulatory environment, standardization, certification, performance benchmarking, verification, quantum quality management systems (QMS), and life cycle auditing will play a crucial role in promoting sustainable innovation while putting targeted controls and guardrails in place [23].

Further development and operationalization of the guiding principles proposed in this article will require engagement and collaboration among multidisciplinary teams of diverse quantum stakeholders across academia, industry, government, and international organizations. Given the uncertainty surrounding QT's consequences and societal impact, it is essential for researchers, innovators, and regulators to design methods for contextualizing and implementing agreed-upon principles for responsible quantum innovation and document their application at the level of use cases. The worthy objective of such an ambitious effort is to safeguard, engage, and advance humanity in the quantum age through responsible quantum innovation.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

[13] This is now required by President Biden's Two Executive Orders Advancing QT [47] and the Quantum Computing Cybersecurity Preparedness Act [86].

Acknowledgments

Mateo Aboy's, Timo Minssen's, and I Glenn Cohen's research for this paper was supported, in part, by a Novo Nordisk Foundation Grant for a scientifically independent International Collaborative Bioscience Innovation & Law Programme (Inter-CeBIL Programme—Grant No. NNF23SA0087056).

The authors thank Mark Lemley for helpful comments on an earlier version of this article.

ORCID iDs

Mauritz Kop https://orcid.org/0000-0002-2166-1962
Mateo Aboy https://orcid.org/0000-0002-5168-4321

References

[1] Dowling J and Milburn G 2003 Quantum technology: the second quantum revolution *Phil. Trans. R. Soc.* A 361 1655–74
[2] Aboy M, Minssen T and Kop M 2022 Mapping the patent landscape of QT: patenting trends, innovation and policy implications *Int. Rev. Intell. Prop. Competition Law* **53** 853–82
[3] Singla S 2023 Responsible generative AI: empowering innovation and ensuring ethical accountability *InsiderFinance Wire* (available at: https://wire.insiderfinance.io/responsible-generative-ai-empowering-innovation-and-ensuring-ethical-accountability-f795581d6cc9)
[4] Baxter K and Schlesinger Y 2023 Managing the risks of generative AI *Harvard Business Review* (available at: https://hbr.org/2023/06/managing-the-risks-of-generative-ai)
[5] Downing C A and Vidiella-Barranco A 2023 Parametrically driving a quantum oscillator into exceptionality *Sci. Rep.* **13** 11004
[6] Martin V *et al* 2021 Quantum technologies in the telecommunications industry *EPJ Quantum Technol.* **8** 19
[7] Preskill J 2021 Quantum computing 40 years later (arXiv:2106.10522)
[8] Coenen C, Grinbaum A, Grunwald A, Milburn C and Vermaas P 2022 Quantum technologies and society: towards a different spin *NanoEthics* **16** 1–6
[9] Stray B *et al* 2022 Quantum sensing for gravity cartography *Nature* **602** 590–4
[10] Wehner S, Elkouss D and Hanson R 2018 Quantum internet: a vision for the road ahead *Science* **362** eaam9288
[11] Mattsson J, Smeets B and Thormarker E 2021 Quantum technology and its impact on security in mobile networks *Ericsson Technol. Rev.* **2021** 2–12
[12] Singh J and Bhangu K S 2023 Contemporary quantum computing use cases: taxonomy, review and challenges *Arch. Comput. Methods Eng.* **30** 615–38
[13] Sarkar A 2022 Applications of quantum computation and algorithmic information: for causal modeling in genomics and reinforcement learning (Delft University of Technology) (available at: https://repository.tudelft.nl/islandora/object/uuid:0952c9e9-115c-4672-9381-2b302d1b9576)
[14] Bayerstadler A *et al* 2021 Industry quantum computing applications *EPJ Quantum Technol. Heidelberg* **8** 25
[15] Bentley C 2022 Quantum computing for transport optimization (arXiv:2206.07313)
[16] Yang X, Chen X, Li J, Peng X and Laflamme R 2021 Hybrid quantum-classical approach to enhanced quantum metrology *Sci. Rep.* **11** 672
[17] O'Malley O *et al* 2016 Scalable quantum simulation of molecular energies *Phys. Rev.* X **6** 031007
[18] Wimmer M and Moraes T 2022 Quantum computing, digital constitutionalism, and the right to encryption: perspectives from Brazil *DISO* **1** 12
[19] De Wolf R 2017 The potential impact of quantum computers on society *Ethics Inf. Technol.* **19** 271–6
[20] Quantum ethics—a call to action by the quantum community (available at: www.youtube.com/watch?v=5qc7gpabEhQ) (February 2021)
[21] Kiesow Cortez E, Yakowitz Bambauer J and Guha S 2023 A quantum policy and ethics roadmap (available at: https://ssrn.com/abstract=4507090)
[22] Perrier E 2021 Ethical quantum computing: a roadmap (arXiv:2102.00759)
[23] Kop M *et al* Towards responsible quantum technology 2023 *Harvard Berkman Klein Center for Internet & Society* (*Research Publication Series 2023–1*) (Harvard University) (available at: https://cyber.harvard.edu/publication/2023/towards-responsible-quantum-technology)
[24] Coenen C and Grunwald A 2017 Responsible research and innovation (RRI) in quantum technology *Ethics Inf. Technol.* **19** 277–94
[25] Ten Holter C, Inglesant P, Srivastava R and Jirotka M 2022 Bridging the quantum divides: a chance to repair classic(al) mistakes? *Quantum Sci. Technol.* **7** 044006
[26] Inglesant P, Ten Holter C, Jirotka M and Williams R 2021 Asleep at the wheel? Responsible innovation in quantum computing *Technol. Anal. Strateg. Manage.* **33** 1364–76
[27] Roberson T 2023 Talking about responsible quantum: awareness is the absolute minimum. That we need to do (arXiv:2112.01378)
[28] Holter C T, Inglesant P and Jirotka M 2021 Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing *Technol. Anal. Strateg. Manage.* **35** 1–13
[29] Owen R, von Schomberg R and Macnaghten P 2021 An unfinished journey? Reflections on a decade of responsible research and innovation *J. Responsible Innov.* **8** 1–17
[30] von Schomberg R 2013 A vision of responsible research and innovation R Owen J Bessant and M Heintz ed *Responsible Innovation (First Edit)* (John Wiley & Sons, Ltd) pp 51–74 (available at: http://onlinelibrary.wiley.com/doi/10.1002/9781118551424.ch3/summary)
[31] Declich G, Berliri M and Alfonsi A 2022 Responsible research and innovation (RRI) and research ethics D O'Mathúna and R Iphofen ed *Ethics, Integrity and Policymaking: The Value of the Case Study* (Springer) (available at: www.ncbi.nlm.nih.gov/books/NBK589347/) (Accessed 3 November 2022) ch 2

[32] Griessler E, Braun R, Wicher M and Yorulmaz M 2023 The drama of responsible research and innovation: the ups and downs of a policy concept *Putting Responsible Research and Innovation into Practice. Library of Ethics and Applied Philosophy* vol 40, ed V Blok (Springer)
[33] UKRI and AREA Framework for responsible research and innovation (available at: www.ukri.org/who-we-are/epsrc/our-policies-and-standards/framework-for-responsible-innovation/) and (www.ukri.org/manage-your-award/good-research-resource-hub/responsible-innovation/)
[34] Pols A, Macnaghten P and Ludwig D 2019 RRI practice internal RRI review—European commission (available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c70b3c34&appId=PPGMS)
[35] Stilgoe J, Owen R and Macnaghten P 2013 Developing a framework for responsible innovation *Res. Policy* **42** 1568
[36] Kumar Thapa R, Iakovleva T and Foss L 2019 Responsible research and innovation: a systematic review of the literature and its applications to regional studies *Eur. Plan. Stud.* **27** 2470–90
[37] RRI tools for the quantum stakeholders (available at: https://rri-tools.eu/research-community) and (https://rri-tools.eu/project-description)
[38] Gasser U and Almeida V 2017 A layered model for AI governance *IEEE Internet Comput.* **21** 58–62
[39] Kop M 2021 Establishing a legal-ethical framework for QT (Yale J.L. & Tech. The Record) (available at: https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology)
[40] Kop M 2020 Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation *2 TTLF Newsletter on Transatlantic Antitrust and IPR Developments Stanford-Vienna Transatlantic Technology Law Forum, Stanford University* (available at: https://law.stanford.edu/publications/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation/)
[41] World Economic Forum 2022 Quantum computing governance principles (available at: www.weforum.org/reports/quantum-computing-governance-principles)
[42] Floridi L 2011 *The Philosophy of Information* (Oxford University Press)
[43] Kop M 2021 Ethics in the quantum age (Physics World) (available at: https://physicsworld.com/a/why-we-need-to-consider-the-ethical-implications-of-quantum-technologies/) (Accessed 31 December)
[44] De Jong E 2022 Own the unknown: an anticipatory approach to prepare society for the quantum age *Digital Society, Quantum-ELSPI TC* vol 1 (Springer Nature) (available at: https://link.springer.com/article/10.1007/s44206-022-00020-4) Topical Collection here: https://link.springer.com/collections/eiebhdhagd
[45] Kaye P, Laflamme R and Mosca M 2007 *An Introduction to Quantum Computing* (Oxford University Press)
[46] Shor P 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Sci. Stat. Comput.* **26** 1484
[47] FACT SHEET: president Biden announces two presidential directives advancing QT (White House) (available at: www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/) (4 May 2021)
[48] Hoofnagle C J and Garfinkel S 2021 *Law and Policy for the Quantum Age* (Cambridge University Press) pp 303–456
[49] Das S 2023 A first order survey of quantum supply dynamics and threat landscapes (arXiv:2308.09772)
[50] 2022 Quantum threat timeline report (GRI) (available at: https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/)
[51] Herman A 2023 Did China break the quantum barrier? (Forbes) (available at: www.forbes.com/sites/arthurherman/2023/01/10/did-china-break-the-quantum-barrier/)
[52] Regev O 2023 An efficient quantum factoring algorithm (arXiv:2308.06572)
[53] Gidney C and Ekerå M 2021 How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits *Quantum* **5** 433
[54] Post Quantum Cryptography 2023 The NIST competition for post-quantum cryptography standards are expected to be released early in 2024 (NIST) (available at: https://csrc.nist.gov/projects/post-quantum-cryptography)
[55] Krelina M 2021 Quantum technology for military applications *EPJ Quantum Technol.* **8** 24
[56] Zhou Q 2021 The subatomic arms race: mutually assured development (Harvard International Review) (available at: https://hir.harvard.edu/the-subatomic-arms-race-mutually-assured-development/)
[57] Meyer L Intergenerational Justice *The Stanford Encyclopedia of Philosophy* Summer 2021 edn, ed E N Zalta (available at: https://plato.stanford.edu/archives/sum2021/entries/justice-intergenerational/)
[58] INTERNATIONAL ATOMIC ENERGY AGENCY 2007 Establishing a code of ethics for nuclear operating organizations *IAEA Nuclear Energy Series No. **NG-T-1.2*** (IAEA)
[59] Giles M 2019 The US and China are in a quantum arms race that will transform warfare (MIT Technology Review) (available at: www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/)
[60] Koops B 2006 Should ICT regulation be technology-neutral? *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* ed B-J Koops (TMC Asser Press)
[61] Johnson W G 2018 Governance tools for the second quantum revolution *Jurimetrics* **59** 487 (available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350830)
[62] Rand L and Rand T 2022 The "Prime Factors" of quantum cryptography regulation *Notre Dame J. Emerg. Tech.* **3** 37
[63] Zhang Y, Porter A, Chiavetta D, Newman N C and Guo Y 2019 Forecasting technical emergence: an introduction *Technol. Forecast. Soc. Change* **146** 626–7
[64] Greely H T 2022 Governing emerging technologies—looking forward with horizon scanning and looking back with technology audits *Glob. Pub. Pol'y Governance* **2** 266–82
[65] Waters R 2017 Quantum computing rivals muster software power in new 'arms race' (Financial Times) (available at: www.ft.com/content/6701d8a8-a4fb-11e7-b797-b61809486fe2)
[66] Rogers M and Minerbi N 2022 The quantum computing arms race is not just about breaking encryption keys (NextGov) (available at: www.nextgov.com/ideas/2022/06/quantum-computing-arms-race-not-just-about-breaking-encryption-keys/368834/)
[67] 2022 FACT SHEET: implementation of the Australia—United Kingdom—United States Partnership (AUKUS) (available at: www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/)
[68] Williams O 2021 "This risks creating an arms race": inside Europe's battle over the future of quantum computing (New Statesman) (available at: www.newstatesman.com/business/2021/04/risks-creating-arms-race-inside-europes-battle-over-future-quantum-computing)

[69] Der Derian J and Wendt A 2020 'Quantizing international relations': the case for quantum approaches to international theory and security practice *Secur. Dialogue* **51** 399–413
[70] Candelon F, Courtaux M, Nahas G and Bobier J, 2022 The U.S., China, and Europe are ramping up a quantum computing arms race. Here's what they'll need to do to win (Fortune) (available at: https://fortune.com/2022/09/02/quantum-computing-cryptography-companies-arms-race/)
[71] Sheikh H, Prins C and Schrijvers E 2023 *Mission AI, The New System Technology* (Springer) (available at: https://link.springer.com/book/10.1007/978-3-031-21448-6)
[72] Kop M 2023 Quantum-ELSPI: a novel field of research *DISO* **2** 20
[73] Meacham S 2023 A race to extinction: how great power competition is making artificial intelligence existentially dangerous (Harvard International Review) (available at: https://hir.harvard.edu/a-race-to-extinction-how-great-power-competition-is-making-artificial-intelligence-existentially-dangerous/)
[74] International Thermonuclear Experimental Reactor (available at: www.iter.org/)
[75] Yang J, Chesbrough H and Hurmelinna P 2021 How to appropriate value from general-purpose technology by applying open innovation *Calif. Manage. Rev.* **64** 000812562110417
[76] Friesike S, Widenmayer B, Gassmann O and Schildhauer T 2015 Opening science: towards an agenda of open science in academia and industry *J. Technol. Transfer* **40** 581–601
[77] Berger C *et al* 2021 Quantum technologies for climate change: preliminary assessment (arXiv:2107.05362)
[78] Kop M, Aboy M and Minssen T 2022 Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis *J. Intell. Prop. Law Pract.* **17** 613–28
[79] Schneider F, Patel Z, Paulavets K, Buser T, Kado J and Burkhart S 2023 Fostering transdisciplinary research for sustainability in the Global South: pathways to impact for funding programmes *Humanit. Soc. Sci. Commun.* **10** 620
[80] DeNardis L 2022 Quantum internet protocols 10.2139/ssrn.4182865
[81] National security memorandum on promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems (available at: www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/)
[82] EU open innovation policy (available at: www.europarl.europa.eu/factsheets/en/sheet/67/innovation-policy)
[83] Seskir Z *et al* 2023 *Quantum Sci. Technol.* **8** 024005
[84] Lemley M 2005 Patenting nanotechnology *Stan. Law Rev.* **58** 601
[85] Larouche P and Van Overwalle G 2014 Interoperability standards, patents and competition policy *TILEC Discussion Paper No. 2014–050* 10.2139/ssrn.2539964
[86] 2021-2022 H.R.7535—quantum computing cybersecurity preparedness act *117th Congress* (available at: www.congress.gov/bill/117th-congress/house-bill/7535/actions)
[87] Sanzeri S 2023 What the quantum computing cybersecurity preparedness act means for national security (Forbes) (available at: www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/)
[88] 2022 National Science and Technology Council guidance for implementing National Security Presidential Memorandum 33 (NSPM-33) on national security strategy for United States government-supported research and development (Subcommittee on Research Security and Joint Committee on the Research Environment) (available at: www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf)
[89] 2020 International Traffic in Arms Regulations: U.S. munitions list categories I, II, and III (ITAR) (available at: www.federalregister.gov/documents/2020/01/23/2020-00574/international-traffic-in-arms-regulations-us-munitions-list-categories-i-ii-and-iii)
[90] Inglesant P *et al* 2018 Responsible innovation in QT applied to defence and national security *NQIT*
[91] OECD 2017 Making innovation benefit all: policies for inclusive growth (available at: www.oecd.org/innovation/inno/making-innovation-benefit-all.pdf)
[92] Garcia Martinez M, Zouaghi F and Garcia Marco T 2017 Diversity is strategy: the effect of R&D team diversity on innovative performance *R&D Manage.* **47** 311–29
[93] United Nations Sustainable Development Goals (UN SDG) (available at: https://sdgs.un.org/goals)
[94] Roberson T, Leach J and Raman S 2021 Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies *Quantum Sci. Technol.* **6** 25001
[95] Munafò M, Nosek B, Bishop D, Button K S, Chambers C D, Percie du Sert N, Simonsohn U, Wagenmakers E-J, Ware J J and Ioannidis J P A 2017 A manifesto for reproducible science *Nat. Hum. Behav.* **1** 0021
[96] Cassiman B and Veugelers R 2002 R&D cooperation and spillovers: some empirical evidence from Belgium *Am. Econ. Rev.* **92** 1169–84
[97] Neven H 2013 Launching the quantum artificial intelligence lab (Google Research) (available at: https://blog.research.google/2013/05/launching-quantum-artificial.html)
[98] Pansera M, Owen R, Meacham D and Kuh V 2020 Embedding responsible innovation within synthetic biology research and innovation: insights from a UK multi-disciplinary research centre *J. Responsible Innov.* **7** 384–409
[99] Friedman B 2008 Embodying values in technology: theory and practice *Information Technology and Moral Philosophy* vol 3 (Cambridge Publisher: Cambridge University Press) pp 322–53
[100] Kop M 2023 Quantum technology impact assessment *EU AI Alliance, European Commission* (available at: https://futurium.ec.europa.eu/en/european-ai-alliance/best-practices/quantum-technology-impact-assessment)
[101] Vermaas P E 2017 The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable *Ethics Inf. Technol.* **19** 241–6
[102] Turlington M, Sattler L, Pacella D, Gamble J and Toy M 2021 Quantum computing and its impact *Future Networks, Services and Management* ed M Toy (Springer)
[103] Greinert F, Müller R, Bitzenbauer P, Ubben M and Weber K 2023 Future quantum workforce: competences, requirements, and forecasts *Phys. Rev. Phys. Educ. Res.* **19** 010137
[104] European Competence Framework for Quantum Technologies (available at: https://op.europa.eu/en/publication-detail/-/publication/93ecfd3c-2005-11ec-bd8e-01aa75ed71a1/language-en)

[105] UK's approach to regulating AI: establishing a pro-innovation approach to regulating AI an overview of the UK's emerging approach (available at: www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai) (Accessed 18 July 2022)
[106] Bova F, Goldfarb A and Melko R 2023 Quantum economic advantage *Manage. Sci.* **69** 1116–26
[107] Lamberth M 2021 Can America meet its next Sputnik moment? *TechCrunch* (available at: https://techcrunch.com/2021/12/24/can-america-meet-its-next-sputnik-moment/)
[108] Klyman K The U.S. wants to make sure China can't catch up on quantum computing (Foreign Policy) (available at: https://foreignpolicy.com/2023/03/31/us-china-competition-quantum-computing/) (Accessed 31 March 2023)
[109] Fitzsimons J 2017 Private quantum computation: an introduction to blind quantum computing and related protocols *npj Quantum Inf.* **3** 23
[110] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5
[111] Perrier E 2022 The quantum governance stack: models of governance for quantum information technologies *Digit. Soc.* **1** 22
[112] National Academies of Sciences, Engineering, and Medicine 2019 *Quantum Computing: Progress and Prospects* ed M Horowitz and E Grumbling (The National Academies Press) pp 158–9