f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Societal implications of quantum technologies through a technocriticism of quantum key distribution

by Sarah Young, Catherine Brooks, and Jason Pridmore

Abstract

Advancement in quantum networking is becoming increasingly more sophisticated, with some arguing that a working quantum network may be reached by 2030. Just how these networks can and will come to be is still a work in progress, including how communications within those networks will be secured. While debates about the development of quantum networking often focus on technical specifications, less is written about their social impacts and the myriad of ways individuals can engage in conversations about quantum technologies, especially in non-technical ways. Spaces for legal, humanist or behavioral scholars to weigh in on the impacts of this emerging capability do exist, and using the example of criticism of the quantum protocol quantum key distribution (QKD), this paper illustrates five entry points for non-technical experts to help technical, practical, and scholarly communities prepare for the anticipated quantum revolution. Selecting QKD as an area of critique was chosen due to its established position as an application of quantum properties that reaches beyond theoretical applications.

Contents

Introduction to quantum networks

Globally, governments and corporations are investing heavily in a quantum future. These investments are often tied to developments in quantum computing which has afforded engineers new opportunities to come closer to accomplishing a quantum network. Such a network can be conceived as a kind of 'new Internet' with scholars pointing to emerging opportunities and ethical questions tied to quantum communications (Kiesow Cortez, *et al.*, 2023).

A major impetus for development of quantum networks is the enhancement of data security and the protection of information. Technologies capitalizing on quantum mechanics offer the promise of radically changing the security of digital communication practices by shifting security from easily hacked algorithms on classical computers towards safer encryption with quantum mechanics. These enhanced forms of security would make a quantum network, broadly potentially safer and less hackable compared to today's encryption capabilities. This is particularly necessary as increased reliance on quantum computing around the globe poses higher risks to more classical forms of encryption protecting our data today.

One security product invested in globally is quantum key distribution (QKD). QKD is a method of exchanging encryption keys along networks to ensure that only authorized parties get access to the information being communicated. QKD is often touted to be revolutionary in computing, and as Van Meter (2014) commented several years ago, QKD has been called "the most important, commercial application of quantum communication technology" [1].

Although modifications to software and hardware are needed, QKD can address the security challenges of an upcoming quantum network by securing communications that become more vulnerable to more classical forms of security once quantum computers are more commonplace. Current protocols often rely on difficult to solve computations, but these computations can be calculated significantly quicker on efficient quantum computers. In other words, quantum computing can solve contemporary encryption protections such as an RSA key (*i.e.,* today's cryptography system used to secure Internet-transmitted information) at a much faster rate.

QKD is one of the earliest commercial security applications taking advantage of quantum mechanics, with QKD devices emerging as early as 2009 [2]. Scholars have pointed to the many companies and governments that have recently spent millions of dollars to create more refined and more robust versions of the technologies [3].

Despite heavy investment, not everyone wholeheartedly recommends the use of QKD. In fact, in the past few years, several government agencies in the United States, United Kingdom, France, and Germany have all issued position statements that caution the use of QKD as a widespread form of communications security, at least for the present time, focusing particularly on potential technological issues (see National Security Agency/Central Security Service [NSA/CSS], 2020; National Cyber Security Centre [NCSC], 2020; Agence Nationale de la Sécurité des Systèmes d'Information [ANSSI], 2020; and Bundesamt für Sicherheit in der Informationstechnik [BSI], 2021).

What is particularly interesting about a deeper dive into the rhetoric of these four documents, however, is that while the reports more overtly focus on more technological concerns such as when the NSA organizes the reasons not to adopt QKD under the heading "Technical limitations" (NSA/CSS, 2020), in a more subtle way, the reports also raise issues about QKD along some of the more social lines. These spaces are key to draw attention to because as critical technology studies argue, conversations emerging around quantum technologies are in fact not just technical, but they are also of social importance. Research groups in large quantum technology projects illustrate this, such as Thrust 4 of the National Science Foundation-supported Center for Quantum Networks (n.d.) in the United States and the Centre for Quantum and Society through the Quantum

]

Delta NL in the Netherlands (Centre for Quantum and Society, 2023). While social critique with quantum networks is not new (*e.g.*, Hoofnagle and Garfinkel, 2022; Roberson, *et al.*, 2021), there is much less appraisal of the social consequences of quantum networks, particularly in terms of securing human communications in prevailing literatures. This technological emphasis leads to our paper's key research questions: How can we bridge the gap between human, social, and technological practices in the development of quantum networks? Also, where can non-technical experts [4] enter conversations about quantum technologies and their security protocols, including QKD and beyond?

Given this context, we analyze the four government agencies' critiques of QKD through a thematic analysis of the documents to see what the agencies list as drawbacks and what their positions on the use of QKD are. This thematic analysis draws from critical technology studies and serves as a 'technocritique' of those positions to see what additional human and social problems can be identified surrounding QKD as well the more visible technical drawbacks identified by the agencies. We conclude that while most of the rhetoric and criticism about QKD is organized around their technical development, there are at least five human and social conversations that need participation as a network is developed. These spaces are key to keeping track of the technology to avoid repeating blind spots or potential pitfalls in technological development that affected other technologies such as was the case of standardization, transparency, or governance with the classical Internet (Leiba, 2008; Weber, 2008; DeNardis, 2014) or more recently in advances of artificial intelligence (Fenwick, *et al.*, 2017).

In making this case, and in consideration of our research questions above, we synthesize key concepts that exist at the intersection of quantum networking, social science, and humanities. To do this, we proceed in three parts:

1. We provide a basic technical background of quantum networks and QKD to define what is being critiqued by the four agencies.
2. We offer a thematic analysis which serves as a technocritical account of the documents to raise the visibility of spaces of entry points between quantum science and humanities and social science-based scholars.
3. We note how our conclusions contribute to conversations about quantum technologies in general.

From classical networks to quantum key distribution (QKD)

To provide a technical background of quantum networks and QKD as reviewed by the four agencies, we focus on the evolution and transition from a classical Internet infrastructure towards a quantum network. This brief technical description indicates the shifts taking place in this historic period of networking history and demonstrates how technical communication of quantum principles is possible and can bring new and varied audiences into conversations about emerging quantum developments. Researchers across disciplines and locations have been collaborating for years to develop workable quantum networks, but more recently, scholars point to a kind of 'quantum Internet timeline' suggesting people will have quantum networking in full capability by the year 2030 (Clark, *et al.*, 2021; Vermaas, *et al.*, 2019). Quantum networks, as opposed to classical networks, rely on the principles of quantum mechanics to change the way information is sent and received. It is argued that these networks will likely impact our world in unpredictable ways, following a similar trajectory of new developments in information communication technologies (ICTs), or technologies that support the communication of information, over the past centuries (see Mosco, 2004).

The current Internet is based on digital computing with a binary coding system comprised of a series of 1s and 0s that convey information and communication from one place to another. A quantum network is similar in that communication can move from one end of a network to another, with quantum processors existing at each end. However, this communication is conveyed through quantum bits, called qubits. Qubits will be able to be amplified by optical switches and moved over long distances via repeaters that help re-send qubits to their intended destination. Qubits are distinct from classical bits in that they can entangle, or in simple terms, connect to each other so that anything done to one will affect the other. Entanglement happens when two qubits become interdependent with one another. Because they entangle, they are disrupted when disturbed. The security implications tied to the entanglement of bits — and the ability to recognize when interference or disruption occurs is profound. Put differently, information is much tougher to 'hack' when moved as qubits compared to that moved via classical bits because of the ways that qubits can reveal with certainty that they have been hacked. Although this represents a simplified version of the developments here, work on these processes is also in an on-going state of refinement, with scientists and engineers working different techniques to try to bring the theoretical possibilities to realistic implementation.

Although QKD is not the only path towards security, because quantum technologies will change the way information is transmitted and protected, a particular form of securing information currently being researched is QKD. QKD has been described as an encryption solution that can utilize principles of quantum mechanics to distribute random keys to two parties. In its most basic form, Van Meter (2014) indicates that "QKD systems generate shared, secret random numbers between two distant parties: nothing more, nothing less" [5]. Further, its function is security, and anchoring the method, the goal of the whole QKD process is "to detect the presence or absence of an eavesdropper" [6].

A true random number is a key component to QKD and is what QKD protocols are said to rely on, especially entanglement-based protocols (Xavier, *et al.*, 2009). A strength of the protocol is in this supposed true form of randomness, as these numbers are random because they are not produced through algorithms and instead produced through more natural processes of light (ID Quantique, 2020). This randomness makes these processes unlike contemporary systems of encryption which are more predictable and use only pseudo-random numbers that are algorithmically generated [7]. Thus, with their origin based on photons as "an ideal quantum case," these numbers are "truly non-deterministic, without any correlations in terms of repeated patterns [sic] occurrences" [8].

However, the generation of truly random numbers is not the full extent of QKD. Quantum mechanics offers additional affordances. The second stage of QKD involves distributing key numbers. As Ham (2020) notes, QKD's "security relies on how to distribute the keys rather than how to generate them" [9]. Although there are a variety of protocols for the transmission of quantum bits (Li, Li, *et al.*, 2018), two popular protocols are the BB84 protocol and the Ekert protocol (Fürnkranz, 2020).

The BB84 protocol developed by Charles H. Bennett and Gilles Brassard (2014) in 1984 is based on the transmission of polarized photons along, for instance, a fiber optic cable. According to one private company working on development of a quantum network, in a protocol like this, QKD "works by transmitting an encoded key in the form of quantum bits (qubits) between endpoints over a fiber optic cable. Qubits are typically polarized photons, which can travel easily along fiber-optic cables" (Quantum Xchange, 2020). Further, "each photon has a random quantum state, and collectively all the photons create a bit stream of ones and zeros" (Quantum Xchange, 2021). The BB84 is a Heisenberg–based protocol (Haitjema, 2007), which means, according to Cobourne (2011), that protection from an eavesdropper comes from the principle that "measuring a quantum state changes it" and that anyone listening in "will introduce errors into the information transfer along a quantum channel which should always be detected by the protocol" [10]. Thus, "any attempt to intercept the quantum key destroys the qubit's delicate quantum state and the information it holds, alerting the endpoints that an intrusion occurred," and further, "the detectability of the intrusions is what ensures the security of the transmission" (Quantum Xchange, 2020).

On the other hand, the Ekert protocol (or E91) by Artur Ekert from 1991 is an entanglement-based protocol (Haitjema, 2007). This allows photon pairs to be split and received, meaning that "information only springs into existence when the entangled quanta are measured" where "the eavesdropper's only potential ploy is to attempt to inject extra quanta into the protocol" [11]. However, even a minimum amount of movement would be impossible to go unnoticed, so an eavesdropper would be detected [12]. Authors use stand-in friends "Alice" and "Bob" to illustrate the process. As Li, Li, *et al.* (2018) summarized, "Compared with the BB84 protocol which Alice sends quantum particles to Bob, the E91 protocol uses an [Einstein-Podolsky-Rosen] EPR pair during the communication, which divides the EPR pair and sends one particle to Alice and Bob separately" [13]. A protocol like this is less developed and more complex than those which use fiber-optic cables, partly as it requires entanglement to be maintained. Entanglement using this protocol will also reduce some of the quality issues relative to the use of cables, such as losing photons along fibers [14].

Methods

Alongside the complexities outlined earlier, QKD has several limitations. While the process is often touted by industry and supported by governmental research funds, there are many that are weary of the technology particularly for large scale operations. Four high-profile documents indicate a position that is resistant to QKD. These are described in documents issued by security agencies in the United States (NSA/CSS, 2020), United Kingdom (NCSC, 2020), France (ANSSI, 2020), and Germany (BSI, 2021) and can be seen as influential position papers based on the prominence of these agencies [15]. Their comprehensive analysis of QKD, as well as the documents' similar structure, can be seen as a small corpus of QKD position texts. As such, this enabled a more cohesive analysis to be completed in relation to key agencies' responses to QKD.

As part of this research, we engage in a thematic analysis of these four position statements to identify the technical and social challenges the agencies indicated in the documents. According to Braun and Clarke (2006), a thematic analysis approach starts by becoming familiar with a document to identify relevant themes. Themes are "something important about the data in relation to the research question," and due to repetition of its parts, a theme "represents some level of patterned response or meaning within the data set" [16]. Thus, the process is based on coding passages that, over time, begin to develop patterns that become the primary themes in the data set. The process involves multiple reviews of the documentation to refine the codes identified in the data, or in this case, the documents as artifacts.

In addition to identifying the technical themes that become more visible most overtly through the document's organization, we also noted human and social factors. Thus, we consider this thematic analysis as a critical reading of the documents, or a way to accomplish what could be considered a technocritism of the documents. We position technocriticsm as a kind of analytic focus meant to critically interrogate the social meanings and implications tied to the emergence of technological developments, even if the technical elements remained in the forefront of the documents themselves. Certainly, scholars (*e.g.*, Weston and Bain, 2010) have defended technological trends in the face of technocritics, and technocritque has been positioned within broader political discussions around capitalism and innovation resistance (*e.g.*, Fourmentraux, 2021). But we know that history matters as people take up new technological developments as well (Arapostathis and Pearson, 2019). We also know that technological developments "are reworking the sociospatial dimensions of our lives" [17].

A technocriticsm is especially useful for those outside of disciplines focused on the technical aspects of quantum engineering because tools like QKD are very much embedded in society and involve people sending information and communicating across a different kind of network. Not only does one engage with the technical, but one grapples with how a particular technology effects and affects the people, places, and societies that the technology enters, be it with a positive or negative impact. This position is situated in critical studies of technology which "argues that technologies are not separate from society but are adapted to their social and political environment," and thus there will always be both technical and social elements intertwined in any technology [18]. With this desire to grapple with technical realities while coming to this research as non-technical scholars, we engaged the thematic analytical process and reached a set of findings presented next.

Thematic analysis of policy documents

After multiple readings of the four documents and refinement of the coding process, it became clear that through our technocriticism, we found both 1) technical *and* 2) human/social reasons why the agencies did not support the widespread adoption, despite that the organization of the documents often put the technical reasons in the forefront such as when the U.S. groups all their recommendations under the heading, "Technical limitations."

We found that the passages focused on technical reasons emphasized the technical nature of QKD and the more engineering-related drawbacks to utilizing QKD as a method for security. On the other hand, the passages themed human and social reasons were those that focused on the social context that the technology circulates in. It is of note that while the documents often framed the reservations along technical lines rather than social critique, the social concerns were often subtly present within more technically oriented discussions often made visible through the organization of the headings of the documents. It is important to also note too though, that these undercurrents of social concern were ever-present within the same discourses, providing support for assertions from critical theories of technology which argue that the technical and the social are always intertwined.

QKD critiques — Highlighting technical concerns

The passages that focused most specifically on the technology-related shortcomings of the QKD process were divided into two subthemes described as "partial solutions" and "better alternatives." The majority of the documents were focused on technical concerns, primarily related to the shortcomings QKD represented.

The first sub-category of technological reasons was "partial solutions," and this theme highlights that QKD only offers partial solutions to complex security problems which can create other challenges. For instance, the French document noted that QKD only offers a partial solution to security because, while it can perform some functions well, it also cannot perform all necessary security functions such as being able to protect data at rest in storage [19]. In another example, the U.S. document noted that QKD can generate keys for confidentiality, but also that "QKD does not provide a means to authenticate the QKD transmission source" (NSA/CSS, 2020). Thus, QKD requires trusted nodes, and there can be authentication issues, along with other problems with key agreements, increased risk of denial-of-service issues or man in the middle attacks. The German document states that in general for QKD, the process does not alone meet expectations for encryption, resistance to attacks, or authentication [20]. Finally, the U.K. document remarked that "QKD protocols do not provide authentication," thus, "they are vulnerable to physical man-in-the-middle attacks" (NCSC, 2020), arguing that the protocols provide some protections, but have partial vulnerably.

We also identified a second subtheme of "better alternatives." Passages in this category all argued that QKD was not the best solution overall for security, even with the prospects of more computationally powerful quantum computers, because there were superior solutions for those looking to secure communications. The passages we coded for this category focused on post-quantum cryptography (again, also called quantum-resistant cryptography) and argued that post-quantum cryptography is a better choice for security. For instance, NSA/CSS (2020) argued for post-quantum cryptography because this approach is cheaper and less risky. The U.K.'s NCSC (2020) argued post-quantum cryptography is better because it can fit into classical computers and does not require special hardware. France's ASSI (2020), argued security would be better left to processes like post-quantum cryptography that do not require trusted nodes [21], and would be served by technology that provides more long-term data protection in modern systems [22]. Worth noting is that Germany's document from the Federal Office for Information Security articulated a more centrist argument between post-quantum cryptography and QKD and argued for the complimentary use of the technologies, but this was also because at times, post-quantum cryptography was superior to QKD such as in key agreement. For instance, the document suggested that only *if* [emphasis added by authors] QKD continues to be developed and refined and becomes operational, then it may "provide a complement to post-quantum schemes for key agreement" [23], emphasizing that QKD, when it is further developed, is not to be used by itself but does offer a compliment security option.

QKD critiques — Entry points for social science

We identified and labeled the second thematic category "social impacts" for passages that focused on people. While the passages in this theme could mention technological issues, they also reflected focus on themes that could be categorized as having human or social implications. In other words, these were related to people and their cultures or societies and their relationships to each other, their tools, or their environments. Humanities and social sciences are intertwined because the humanities focus on the human and their social and cultural environment, and the social sciences focus on both "the society and the embedded individuals, institutions and structures" that make it up [24]. Again, while these passages were not the primary focus of the concluding remarks of the documents and even though the documents primarily focused on technical reasons, we identified five

categories under the social impacts theme: economic dimension, linguistics, risk management, public policy, and communication. These categories are useful to note because they show entry points into the conversations beyond more technical lines for differing types of scholars and practitioners.

Economics

First, across documents, the texts mentioned costs associated with QKD technologies that would hinder implementation. We coded the passages that spoke about costs and economies in this subtheme. For instance, the French document noted several technological issues that related to costs when they commented that the number of specialized technologies needed for QKD would, "make its largescale deployment extremely complex and costly" [25]. Adding to this, the German document noted that post-quantum algorithms "are more cost-effective" [26], suggesting there were other more efficient ways to spend funds. Further, the U.S. document stated, "**Quantum key distribution increases infrastructure costs**" [bolding in original] (NSA/CSS, 2020). Finally, while the U.K. document did not expressly mention the word costs, the agency also invoked the need for additional infrastructure and argued that "the specialised hardware requirements of QKD" was a major reason not to recommend the technology (NCSC, 2020) which could imply higher costs for systems.

While some may argue economics is driven by exact calculations and mathematical (un)certainty, economics is a social science because its truths are relative to theory and submerged in social context (Beker, 2022). What amount of money and where it is spent is rooted in ideology, such as beliefs in efficiency, market corrections, or the role of government in managing market forces [27]. Thus, the costs and economics of quantum are a social issue and a space where social scientists like economists, political scientists, historians, and the like are poised to enter because where funds are allocated and money is spent is important, particularly where finances are limited, and the decision to distribute money to one area results in less funding distribution to another. The distribution of resources is important globally, too, with some regions like China and the European Union topping announced quantum spending with US$15 billion and US$7.2 billion respectively, while other countries are not even on the charts for spending for current applications or for research and development [28]. This difference in investments across geographic and political boundaries raises questions about a country's abilities to get and retain access to human, intellectual, and technological resources [29], and potentially sets up a future "quantum divide" (Hidary and Sarkar, 2023).

Linguistics

Second, there were linguistic elements identified in the documents. By linguistics, we refer to both the semantics of language in use and the social use of language, or how words get taken up by certain communicators. For some, linguistics can be conceived as an interdisciplinary social field because they not only focus on the symbols and rules that make up a language spoken by people, but linguistics also looks at the context in which the language circulates (Foucault, 2023). Even with the view of linguistics as a discipline, a variety of analytic tools can be applied.

Linguistic analysis can contribute to quantum conversations by drawing attention to the words used in a particular situation, drawing special attention to how different stakeholders use language or embrace certain discourses around quantum issues and developments. In these documents that were the foci for this research, the agencies critiqued language used by some stakeholders in the quantum field. In an ongoing way, a mismatch existed among those talking about what quantum technologies are theoretically supposed to do versus those talking about (*i.e.*, those who know about) how the technology is actually implemented. Passages coded in this category reflected this contrast across stakeholders' words used to describe contemporary quantum developments. Identifying this contrast makes visible the differences in descriptions of how the technology works and also, a gap between theory and practice.

Emphasizing certain kinds of language gave off a sense of belief, view, or social opinion. For instance, with strategic use of quotes around the word "guaranteed," the U.S. government argues, "Quantum key distribution and Quantum cryptography vendors — and the media — occasionally state bold claims based on theory — *e.g.*, that this technology offers 'guaranteed' security based on the laws of physics" (NSA/CSS, 2020). The document also states that QKD "is highly implementation-dependent rather than assured by laws of physics." Rhetoric such as this not only elevates quantum applications as somehow products of nature instead of mathematics, computers, and algorithms, but it also presents that these applications are more secure and reliable than they actually are, at least in their present abilities for implementation, which is where the documents' critique focused.

While not attributing the claims to any particular actors, the French document expressed skepticism in their opening paragraph through their word choice of "alleged" when they stated, "The defining characteristic of QKD is its alleged superior secrecy guarantee that would justify its use for high security applications" [30], and then they followed up with the clause, "However, deployment constraints specific to QKD hinder large-scale deployments with high practical security" [31]. The second sentence clarified why QKD is only "allegedly" superior. Further, the French document added another example of theory versus reality when it noted: "While theoretically QKD protocols are not vulnerable to mathematical attacks, in practice it is very difficult to implement them perfectly" [32].

The U.K. agency was a bit fuzzier in their use of the language when they argued that "QKD claims to offer a potential mitigation since its security properties are based on the laws of physics rather than the hardness of some underlying mathematical problems," but the document did not follow up with their own counterclaims (NCSC, 2020). However, this passage was next to a section pointing out technological limitations, thereby providing a contrast between claims of security and actual risks presented by the technology.

Finally, the German document mentioned a vague categorization of stakeholders with differing standpoints on QKD and some of its technical capabilities when they noted, "There are certainly voices that consider a lower assurance level EAL 2 to be appropriate. This assessment is not shared by BSI, but EAL4+ is seen as a minimum requirement" [33]. They also noted that QKD "promises 'security based on the laws of physics,'" but ultimately is does not deliver this security [34]. The German document also contributes the statement about the random number component of QKD, "Certainly false are general statements of the type 'QRNGs provide random numbers based on natural laws and are therefore automatically secure'. It cannot be assumed that ideal random number generators exist in the real world" [35].

This linguistic area is particularly important area to cover as quantum technologies emerge because, as noted by the documents, there are various claims by different actors about what quantum can do now and in the future, and while some of these claims might have come to reality or will be possible, other claims about quantum can overstate what can in reality be engineered or equates to "quantum hype" (Smith, 2020). Thus, there is a vibrant quantum imaginary at work in the milieu of quantum technologies, and it is important to analyze the word choice and arguments used surrounding quantum technologies so that the narrative surrounding quantum is based in reality and not the quantum imagination. Put another way, there are stories that can be told about quantum, and there are functional operations understood about quantum — linguists, discourse analysts, and others from cognate disciplines would do well to follow the myriad ways the quantum story gets told in the coming decades.

Risk management

A third category identified within the social impacts theme was risk management. Risk management put simply is an interdisciplinary field that interrogates the likelihood of something negative occurring to humans or places such as their social organizations, their environments, or their institutions. Although often viewed through business and government lenses through prediction, management, and control of pressing dangers, risk management also involves sustainability and stability for the future (Beck, 2004). Thus, studies of risk can involve fairly definitive or imminent events or represent organizational long-term strategies for managing potentially uncertainty (Reamer, 2015).

In the quantum documents, we identified this theme of risk management in several forms. First, there were indications that using QKD could present technological risk, especially for security. For instance, the French document noted that in satellites used for QKD, there would be a "risk of computer intrusion" [36]. The U.S. document noted another security issue when it argued that because the QKD system is so sensitive to detecting eavesdroppers, "denial of service is a significant risk for QKD" (NSA/CSS, 2020). The U.K. also detailed how using QKD technology increased "the risk of man-in-the-middle attacks" (NCSC, 2020). It is worth noting that the German agency did not use the specific word "risk" in their report of QKD like the other documents; however, they emphasized that that certain technical issues made QKD too risky to fully embrace. They noted that "from BSI's point of view, there are still numerous issues to be clarified and limitations to be addressed before QKD can be recommended as a security-critical technology for practical applications" [37]. These issues can be

considered risks, or technical issues that can cause problems, even if the word risk is not used.

It is important to note, too, that risk in the form of security problems was not the only risk addressed, and while using the technology can cause harm, not using QKD could also be risky. For instance, the German document noted that "BSI believes that it is already urgently necessary to take appropriate measures to switch to quantum-safe schemes," and while post-quantum cryptography is more advanced in research and use, and while "there are still numerous issues to be clarified and limitations to be addressed before QKD can be recommended as a security-critical technology for practical applications," QKD should not be abandoned [38]. Instead, "QKD and post-quantum cryptography have the potential to complement each other, especially since they are based on different principles" [39]. Where QKD could be more helpful is "in the context of experiments for restricted use cases where practical limitations are less significant [such as] in hybrid mode as an add-on in conjunction with classical and post-quantum key agreement techniques." Because of these potentials, it is useful to keep investing in the technology despite its drawbacks because the technology has the potential to help minimize future risk. This enthusiasm is reflected by Germany's public-funded spending on quantum computing which was reportedly 41.9 percent of the European Union's announced US$7.2 billion investment in 2021 [40].

The other three documents also reflected this willingness to work with the technologies, too, despite their risk because they have some benefits. For instance, the U.K. noted, "However, we welcome the ongoing research and assurance work currently underway in this [QKD] area ...[and] we support continued research into QRNGs" (NCSC, 2020). Even the U.S. stated they would not recommend the process unless certain limitations were overcome (NSA/CSS, 2020) showing still future possibilities to work with the technology, and France also noted that despite drawbacks to the process, "QKD may find some use in a few niche applications, for instance as a defense-in-depth measure on point-to-point links" [41].

The continued support for quantum processes in general can also be explained through geopolitical posturing and a perceived winner-take all, race to the finish for the development of the technologies. These positions are often narrated through the rhetoric of a China-U.S. quantum arms race, both from a security standpoint and from a monetary one, relative to the potential financial boom for deployable quantum technologies (Schmidt, 2023) and are sustained through efforts to minimize collaboration with supposed competitors (Clarke, 2021). Risk analysts and like-minded experts can continue to weigh the balances, tradeoffs, and stabilities possible in a quantum future.

Public policy

A fourth category identified in the documents is public policy and, like the other social impacts categories, functions as an area in which scholars from the humanities and social sciences can use their expertise to enter the conversation about quantum networks and QKD. The social experience is tightly aligned with public policy because policy involves regulation of and for people and their societies to standardize goods, services, and systems for cultures in contexts (Omobowale, *et al.*, 2023). This standardization legitimizes governments and ensures that the collective group of people managed through the polices experience the agreed upon codes of conduct and standards. This standardization also crosses national boundaries and looks at how nations can globally regulate technologies (Higgins and Larner, 2010).

This theme of standardization was noted in all the documents, specifically outlining that either QKD and its associated technologies and processes would need to be standardized before any widespread use could be adopted, or they argued that if the agency was going to standardize something, it would not be QKD. The German document provided a stronger argument of not standardizing QKD and started out with a general statement of why standardization is needed when they outlined that standardization requires uniformity of the "basic building blocks" involved in a technology like "the protocols used, the authentication methods used, key management, the integration of repeaters and network aspects," and for QKD in particular, "The standardization of QKD protocols with associated security proofs is particularly important in the context of certifications and approvals to be able to assess their security" [42]. However, "Standards, for example on protocols, and certified products are still lacking" [43].

Germany also moves into the second emphasis in favor of standardizing another procedure other than QKD, when they added that the belief that "cryptographically relevant quantum computer will be available in the early 2030s" requires new technologies, now, and thus "makes the migration to post-quantum cryptography, the standardisation of which is already well advanced in the NIST process, a clear priority from BSI's point of view" [44]. The French document also noted that post-quantum algorithms are more favorable over QKD and are already slated to be the preferred security standard. The document stated that not only can QKD "hinder large-scale deployments with high practical security," but threats on existing cryptography with universal quantum computers "are taken into account by upcoming standardized 'post-quantum' algorithms" rather than QKD [45]. The U.S. government also supports the standardization of post-quantum algorithms. They stated, "The National Institute of Standards and Technology (NIST) is presently conducting a rigorous selection process to identify quantum-resistant (or post-quantum) algorithms for standardization" and that due to too many other limitations, the agency does not support the current standardization of QKD for the protection of communication in national security systems (NSA/CSS, 2020). The U.K. also notes that "Work towards standardising quantum-safe cryptographic algorithms is underway in international standards bodies such as NIST" and therefore sees more promise in quantum-safe cryptography rather than QKD.

These pushes towards standardization are matters of public policy and are particularly important for quantum technology like QKD because quantum research is so costly. If policies on what technology are used are directed towards other technologies, the incentive to pursue those technologies are greater than the technology that is demoted to a lesser status. Public policy and other legal experts will be helpful in engaging these conversations moving forward given their potential for awareness of the many uses of QKD and related technologies nationally and internationally.

Communication

Fifth and finally, communication emerged as an additional social category to consider. Communication experts are needed to continue raising questions about the new information-sharing potential tied to quantum technologies like QKD and also the myriad issues faced when trying to communicate about quantum communications. Each document discussed the publication or discussion of research by other groups and illustrates the importance of communicating about quantum research to gain understanding and find impact with various audiences. We termed this theme "communication," and passages coded into this area were grouped due to their language discussing knowledge sharing and technical or science communication in particular.

The authors identified the communication theme in at least two ways. First, they documents spoke on the work of others and illustrate that other communications are useful to make informed decisions. For example, the U.S. government document argued, "Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper," and while the document goes on to express skepticism about these claims, the fact that the agency acknowledged the statements supports that they are reading the work of others. The French document also noted use of the work of others when they noted, "The threat of quantum computers has been considered by the cryptographic community for many years" and because of that, quantum-safe algorithms are already available today [46]. The document further explained that it was these techniques that are already being standardized and their ease of installation that makes QKD not as attractive to adopt. Overwhelming, though, it also shows how various technological communities can work together to protect people.

Second, the documents also show a space for social scientists through communication when they call for more research. The German document concluded at the end of its document, "Further research in quantum communication is welcome, also because there may be promising applications outside cryptography" [47]. The U.K. document also calls for more communication of research when they stated, "More research is needed to understand how QKD protocols can be implemented and integrated into these complex systems of classical components" and that "we welcome the ongoing research and assurance work currently underway in this area." This presents an imperative for others to share that information, and the fact that this call is in a public Web site also turns the call for more research to the public, also indicating a willingness to hear what others come up with, even, in theory, non-official actors.

In all four of these documents, there are clear themes of either considering the communication output of others or calls for additional research and collaboration. Whether it be published quantum codes in open access resources or journalists sharing technical information in a public-friendly way, communication is important to allow social development of technologies or getting young people interested in quantum which promise to be more influential in their lives. While the bulk of technical work might be conducted by those doing more scientific research, there is also space to translate these developments from highly technical reports into texts for those

less specialized in the quantum through technical and scientific communication.

Discussion

Overall, the results of this study help solidify the argument of this piece: while much criticism about QKD centers around their technical issues, imbedded in the criticism are also entry points for non-technical social scientists, humanities scholars, and the public in these conversations. Beyond quantum communications, these same conversations are relevant to quantum technologies beyond QKD. Quantum technologies will impact our futures, especially with the quantum computer's potential to disrupt classical security measures, and a wide range of stakeholders representing a variety of interests need to be present as early as they can to minimize potential harms. Matters of economics, linguistics, risk, public policy, and communication are not only important for QKD, but they also apply to other quantum technologies as well because the adoption of technologies is always a social matter.

The results found in this study are important for two reasons. First, the results illustrate five concrete ways non-technical experts can enter the conversation to bring their expertise, and second, the study also impresses the importance of conducting a technocritique of complex topics like quantum, especially technologies that are touted to have revolutionary potential to impact humans and their social world. The spaces we identified spur on larger questions of where to spend funds and even the possibly disproportionate abilities for countries to invest in the first place [48]. The results also question the language used to sell a quantum product as well as highlight the diverging motivations to develop a quantum product. These motivations can range from commercial application to government or military use. The results also bring to the forefront a more wicked, societal question of what presents a bigger risk — investing or not investing in an emerging technology, and they draw attention to the need for standardization to establish policy and law. Finally, the conclusions encourage a bigger picture assessment of the communication of the research, development, and applications of quantum technologies such as the illustrative example of QKD.

Second, the study also impresses the importance of conducting a technocritique of complex topics like quantum. Beyond the organization of the documents around technical hurdles, a more latent technocriticsm was also able to magnify the social dimensions of the technical problems. This is especially useful for emerging and potentially disruptive or revolutionary technologies. Further, it is also useful as a focus to not only be employed by humanists and social scientists, but it is also useful for more technical scholars and scientists like those working in the field of quantum. An articulation of lens designed to draw attention to social critique is useful for those that typically spend their time in a lab trying to develop working technologies instead of grappling with social critique or critical theories of technology. However, as research into the technical life cycle has shown, social critique needs to occur at the onset of technological development and not tacked on at the end of the process or questions just for ethicists (Klitou, 2014; van Belkom, 2020).

Conclusion

Returning to the driving questions of this article, how can we bridge the gap between human, social, and technological practices in the development of quantum networks? Also, where can non-technical experts enter conversations about quantum technologies and their security protocols, from QKD and beyond? We have ultimately concluded that while QKDs and their associated network structures are technical in nature, and while conversations about these technologies often seemingly focus on the technical base of the applications, running concurrently with these technological conversations are also social conversations seen more easily with technocritique that asks where the social meets the technical. There are many other ways to enter the conversation about quantum security like QKD and even quantum technologies in general. There is a strong need for scholars of all kinds to address the present and future human and social impacts of new technologies like QKD and the broader vision for quantum communications.

Certainly, quantum technologies are coming, and adapted forms of security will be needed in the very near future. Whether this looks like postquantum cryptography, QKD, a mixture of both, or something else, it is important to engage these conversations. Fully interrogating user-focused issues relative to all-emerging technical tools is of paramount importance before monies are allocated, processes are standardized, and risks are realized.

Rather than being caught off guard by the rapid development of the technology such as what has been reported about generative artificial intelligence in tech companies like Apple or in the educational sector (*e.g.*, Gurman, 2023; McMurtrie and Supiano, 2023), communities outside of the more technical producers of quantum technologies need to be involved in the conversations, even during the phase where technical limitations are still being identified and overcome. Just because there are limitations now does not mean that these limitations will not be fixed in the future. As more applications for quantum technologies are developed and emerge, there will only be even more spaces to engage with these technologies and more considerations of impact, be it broadly technological, social, human, ethical, financial, or political. Broad engagement now from across disciplines and practical domains is urgent as we continue to form future technological tools and systems. Engagement now helps shape what futures will be. Quantum is coming, and we need to be ready to adapt as we begin to adopt its applications.

About the authors

Sarah Young is a postdoctoral researcher in digitalization and AI researching quantum networks, science and technical communication, and surveillance and privacy in the Media and Communication Department at Erasmus University Rotterdam in Rotterdam, Netherlands. She is also a Social Impacts Research Fellow with the Center for Quantum Networks (https://cqn-erc.org/).
ORCID: https://orcid.org/0000-0002-0644-8485
Web: https://www.eur.nl/en/eshcc/people/sarah-young
E-mail: sarah [dot] jackson [dot] young [at] gmail [dot] com

Catherine F. Brooks, Ph.D., is a professor and interim dean of the iSchool (School of Information) at the University of Arizona. With a focus on language use, social interaction, and discourse, her scholarly work focuses on matters of identity and social behavior. Her research spans disciplines of education, communication, and information science, and it most recently focuses on human protections amid technological innovation and change. She was senior personnel as part of the Center for Quantum Networks (https://cqn-erc.org/).
ORCID: https://orcid.org/0000-0002-7735-4558
E-mail: cfbrooks [at] arizona [dot] edu

Jason Pridmore is the Vice Dean of Education for the Erasmus School of History, Culture and Communication and an Associate Professor in the Department of Media and Communication at Erasmus University Rotterdam. Jason is also the lead on several projects with his research team, including SEISMEC, COALESCE, SPATIAL, Ashvin, REINCARNATE, and he co-leads the Inspiring and Anchoring Trust in Science project. Previously, Jason led the TRESCA project, and was the Project Exploitation Manager and Data Security Manager on the BIM-SPEED project. He was the Principle Investigator in the Netherlands on the Mobile Privacy

Project.
ORCID: https://orcid.org/0000-0001-9159-8623
E-mail: pridmore [at] eshcc [dot] eur [dot] nl

Acknowledgements

The work of the Center for Quantum Networks is supported in part under NSF cooperative agreement number 1941583.

Notes

1. Van Meter, 2014, p. 93.

2. Hoofnagle and Garfinkel, 2022, p. 289.

3. *E.g.*, Barker, 2017; Forteza, *et al.*, 2019, p. 45; Ndousse-Fetter, *et al.*, 2019; Oak Ridge National Laboratory, 2019; Qrypt, 2021; Toshiba, 2022.

4. Collier (1996) noted that non-technical experts are those who are not necessarily specialists but are able to understand basic theories and concepts of a topic such as decision-makers in other fields.

5. Van Meter, 2014, p. 94.

6. Van Meter, 2014, p. 93.

7. The statements under review in this paper would argue that the idea of a truly random is more theoretical, and quantum random number generators are still not truly random in their implementation (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2021).

8. Jacak, *et al.*, 2020, p. 2.

9. Ham, 2020, p. 1.

10. Cobourne, 2011, p. 21.

11. *Ibid.*

12. Cobourne, 2011, p. 21.

13. Li, Li, *et al.*, 2018, p. 2.

14. Center for Quantum Networks, 2021, 46:15.

15. As indicated on their Web sites, these agencies are tasked with aspects of digital security of their respective countries. To be more specific, the U.S. agency authoring the article was the National Security Agency/Central Security Service is described as a "combat support agency" that "leads the U.S. Government in cryptology." The author of the U.K. document was the National Cyber Security Centre (NCSC) which is part of the U.K. government functioning as a "bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents" (NCSC, n.d.). The French agency Agence nationale de la sécurité des systèmes d'information (French National Cybersecurity Agency), explains it does not prevent cybercrime, but is focused on deploying "a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring alert and rapid response — particularly on government networks" (ANSSI, 2023). Finally, the German agency Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), takes responsibility for information security "in government, business and society" through protection, investigation, assessment, and anticipation (BSI, n.d.).

16. Braun and Clarke, 2006, p. 82.

17. *E.g.*, Del Casino, *et al.*, 2020, p. 606.

18. Grimes and Feenberg, 2015, p. 121.

19. ANSSI, 2020, p. 2.

20. BSI, 2021, pp. 49–50.

21. NCSC, 2020, p. 4.

22. NCSC, 2020, p. 1.

23. BSI, 2021, p. 53.

24. Omobowale, *et al.*, 2023, p. 32.

25. ANSSI, 2020, p. 4.

26. BSI, 2021, p. 54.

27. Beker, 2022, p. 131.

28. McKinsey & Company, 2021, p. 14.

29. McKinsey & Company, 2021, p. 33.

30. ANSSI, 2020, p. 1.

31. *Ibid.*

32. ANSSI, 2020, p. 3.

33. BSI, 2021, p. 53. To clarify, an Evaluation Assurance Level (EAL) is a technological assurance level where an increasing value corresponds to increasing confidence in the system's implemented security features.

34. BSI, 2020, p. 53.

35. BSI, 2021, p. 52.

36. ANSSI, 2020, p. 4.

37. BSI, 2021, p. 54.

38. *Ibid.*

39. BSI, 2021, p. 54.

40. McKinsey & Company, 2021, p. 14.

41. ANSSI, 2020, p. 1.

42. BSI, 2021, p. 53.

43. BSI, 2021, p. 55.

44. BSI, 2021, p. 53.

45. ANSSI, 2020, p. 1.

46. ANSSI, 2020, p. 4.

47. BSI, 2021, p. 54.

48. For instance, according to the World Economic Forum, as of January 2021, only 17 countries had a national initiative set up for quantum technologies while at least 150 did not have a strategy set up (Hidary and Sarkar, 2022).

References

Agence nationale de la sécurité des systèmes d'information [French National Cybersecurity Agency; ANSSI], 2023. "Forerunners and governance," at https://cyber.gouv.fr/en/about-french-cybersecurity-agency-anssi, accessed 6 March 2024.

Agence nationale de la sécurité des systèmes d'information [ANSSI], 2020. "Should quantum key distribution be used for secure communications?" (26 May), at https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications, accessed 6 March 2024.

S> Arapostathis and P.J.G. Pearson, 2019. "How history matters for the governance of sociotechnical transitions: An introduction to the special issue," *Environmental Innovations and Societal Transitions*, volume 32, pp. 1–6.
doi: https://doi.org/10.1016/j.eist.2019.05.001, accessed 6 March 2024.

S. Barker, 2017. "Department of Defence to invest $3.26m into quantum key research," *SecurityBrief Australia* (25 July), at https://securitybrief.com.au/story/department-defence-invest-326m-quantum-key-research, accessed 6 March 2024.

U. Beck, 2004. *World risk society*. Cambridge: Polity Press.

V.A. Beker, 2022. *Economics, social science and pluralism: A real-world approach*. London: Routledge.
doi: https://doi.org/10.4324/9781003267393, accessed 6 March 2024.

C.H. Bennett and G. Brassard, 2014. “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, volume 560, part 1, pp. 7–11.
doi: https://doi.org/10.1016/j.tcs.2014.05.025, accessed 6 March 2024.

V. Braun and V. Clarke, 2006. “Using thematic analysis in psychology,” *Qualitative Research in Psychology*, volume 3, number 2, pp. 77–101.
doi: https://doi.org/10.1191/1478088706qp063oa, accessed 6 March 2024.

Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security; BSI], 2021. “Quantum-safe cryptography — Fundamentals, current developments and recommendations,” at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf, accessed 6 March 2024.

Bundesamt für Sicherheit in der Informationstechnik [BSI], n.d. “Our mission statement,” at https://www.bsi.bund.de/EN/Das-BSI/Leitbild/leitbild_node.html, accessed 6 March 2024.

Center for Quantum Networks, 2021. “Overview of quantum information science & technology by Michael Raymer,” *YouTube* (3 May), at https://www.youtube.com/watch?v=Df4We9eeBwM&t=432s, accessed 6 March 2024.

Center for Quantum Networks. n.d. “Thrust 4: Societal impacts of the quantum Internet.” at https://cqn-erc.org/research/thrusts/thrust-4/, accessed 6 March 2024.

Centre for Quantum and Society, 2023. “Center for Quantum and Society,” at https://quantumdelta.nl/centre-for-quantum-and-society, accessed 6 March 2024.

R. Clark, S. Bartlett, M. Bremner, P.K. Lam, and T. Ralph, 2021. “The impact of quantum technologies on secure communications,” *Australian Strategic Policy Institute*, at http://ad-aspi.s3.amazonaws.com/2021-04/Quantum%20technologies.pdf, accessed 6 March 2024.

L. Clarke, 2021. “Geopolitics and protectionism threaten the next era of quantum research,” *Tech Monitor* (27 May), at https://techmonitor.ai/technology/emerging-technology/geopolitics-protectionism-threaten-quantum-computing-research, accessed 6 March 2024.

S. Cobourne, 2011. “Quantum key distribution — Protocols and applications,” Royal Holloway, University of London, Department of Mathematics, Technical Report, RHUL–MA–2011–05 (8 March).

J. Collier, with D.M. Toomey (editors), 1996. *Scientific and technical communication: Theory, practice, and policy*. Thousand Oaks, Calif.: Sage.
doi: https://doi.org/10.4135/9781483327815, accessed 6 March 2024.

V.J. Del Casino, Jr., L. House−Peters, J.W. Crampton, and H. Gerhardt, 2020. “The social life of robots: The politics of algorithms, governance, and sovereignty,” *Antipode*, volume 52, number 3, pp. 605–618.
doi: https://doi.org/10.1111/anti.12616, accessed 6 March 2024.

L. DeNardis, 2014. *The global war for Internet governance*. New Haven, Conn.: Yale University Press.

M. Fenwick, W.A. Kaal, and E.P.M. Vermeulen, 2017. “Regulation tomorrow: What happens when technology is faster than the law?” *American University Business Law Review*, volume 6, number 3, pp. 561–594, and at http://digitalcommons.wcl.american.edu/aublr/vol6/iss3/1, accessed 6 March 2024.

P. Forteza, J.-P., Herteman and I. Kerenidis, 2019. “Quantique: Le Virage Technologique que la France Ne Ratera Pas,” at https://www.entreprises.gouv.fr/fr/etudes-et-statistiques/autres-etudes/quantique-virage-technologique-que-la-france-ne-ratera-pas, accessed 6 March 2024.

M. Foucault, 2023. “Linguistics and social sciences,” *Theory, Culture & Society*, volume 40, numbers 1–2, pp. 259–278.
doi: https://doi.org/10.1177/02632764221091549, accessed 6 March 2024.

J.P. Fourmentraux, 2021. “Hacking into capitalism — Technocriticism of digital innovation,” *Études digitales*, volume 2020, number 9, pp. 261–270, and at https://classiques-garnier.com/etudes-digitales-2020-1-n-9-capitalocene-et-plateformes-hommage-a-bernard-stiegler-hacking-into-capitalism.html, accessed 6 March 2024.

G. Fürnkranz, 2020. *The quantum Internet: Ultrafast and safe from hackers*. Cham, Switzerland: Springer.
doi: https://doi.org/10.1007/978-3-030-42664-4, accessed 6 March 2024.

S.M. Grimes and A. Feenberg, 2015. “Critical theory of technology,” In: S. Price, C. Jewitt, and B. Brown (editors). *Sage handbook of digital technology research*. Los Angeles, Calif.: Sage, pp. 121–129.
doi: https://doi.org/10.4135/9781446282229, accessed 6 March 2024.

M. Gurman, 2023. “Inside Apple’s big plan to bring generative AI to all its devices,” *Bloomberg* (22 October), at https://www.bloomberg.com/news/newsletters/2023-10-22/what-is-apple-doing-in-ai-revamping-siri-search-apple-music-and-other-apps-lo1ffr7p, accessed 6 March 2024.

M. Haitjema, 2007. “A survey of the prominent quantum key distribution protocols” (2 December), at https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/, accessed 6 March 2024.

B.S. Ham, 2020. “Unconditionally secured classical cryptography using quantum superposition and unitary transformation,” *Scientific Reports*, volume 10, article number 11687 (15 July).
doi: https://doi.org/10.1038/s41598-020-68038-7, accessed 6 March 2024.

J. Hidary and A. Sarkar, 2023. “The world is heading for a ‘quantum divide’: Here's why it matters,” *World Economic Forum* (18 January), at https://www.weforum.org/agenda/2023/01/the-world-quantum-divide-why-it-matters-davos2023/, accessed 6 March 2024.

V. Higgins and W. Larner, 2010. “Standards and standardization as a social scientific problem,” In: V. Higgins and W. Larner (editors). *Calculating the social: Standards and the reconfiguration of governing*. London: Palgrave Macmillan, pp. 1–17.
doi: https://doi.org/10.1057/9780230289673_1, accessed 6 March 2024.

C.J. Hoofnagle and S.L. Garfinkel, 2022. *Law and policy for the quantum age*. Cambridge: Cambridge University Press.
doi: https://doi.org/10.1017/9781108883719, accessed 6 March 2024.

ID Quantique, 2020. “True random number generation exploiting quantum physics” (7 December), at https://www.idquantique.com/random-number-generation/overview, accessed 6 March 2024.

J.E. Jacak, W.A. Jacak, W.A. Donderowicz, and L. Jacak, 2020. “Quantum random number generators with entanglement for public randomness testing,” *Scientific Reports*, volume 10, article number 164 (13 January).
doi: https://doi.org/10.1038/s41598-019-56706-2, accessed 6 March 2024.

E. Kiesow Cortez, J.R. Bambauer, S. Guha, and S. Fleming, 2023. “A quantum policy and ethics roadmap,” *SSRN* (12 September).
doi: https://dx.doi.org/10.2139/ssrn.4507090, accessed 6 March 2024.

D. Klitou, 2014. *Privacy-invading technologies and privacy by design: Safeguarding privacy, liberty and security in the 21st century* The Hague: T.M.C. Asser Press.
doi: https://doi.org/10.1007/978-94-6265-026-8, accessed 6 March 2024.

B. Leiba, 2008. “An introduction to Internet standards,” *IEEE Internet Computing*, volume 12, number 1, pp. 71–74.
doi: https://doi.org/10.1109/MIC.2008.2, accessed 6 March 2024.

J. Li, N. Li, Y. Zhang, S. Wen, W. Du, W. Chen, and W. Ma, 2018. “A survey on quantum cryptography,” *Chinese Journal of Electronics*, volume 27, number 2, pp. 223–228.
doi: https://doi.org/10.1049/cje.2018.01.017, accessed 6 March 2024.

McKinsey & Company, 2021. “Quantum computing: An emerging ecosystem and industry use cases,” at https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf, accessed 6 March 2024.

B. McMurtrie and B. Supiano, 2023. “Caught off guard by AI,” *Chronicle of Higher Education* (13 June), at https://www.chronicle.com/article/caught-off-guard-by-ai, accessed 6 March 2024.

V. Mosco, 2004. *The digital sublime: Myth, power, and cyberspace*. Cambridge, Mass.: MIT Press.

National Cyber Security Centre [NCSC], 2020. “Quantum security technologies” (24 March), at https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, accessed 6 March 2024.

National Cyber Security Centre [NCSC], n.d. “About the NCSC,” at https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, accessed 6 March 2024.

National Security Agency/Central Security Service [NSA/CSS], 2020. “Quantum key distribution (QKD) and quantum cryptography (QC),” at https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/, accessed 6 March 2024.

T. Ndousse-Fetter, N. Peters, W. Grice, P. Kumar, T. Chapuran, S. Guha, S. Hamilton, I. Monga, R. Newell, A. Nomerotski,D. Towsley, and B. Yoo, 2019. “Quantum networks for open science,” *arXiv*:1910.11658 (27 March).
doi: https://doi.org/10.48550/arXiv.1910.11658, accessed 6 March 2024.

Oak Ridge National Laboratory, 2019. “ORNL teams with Los Alamos, EPB to demonstrate next-generation grid security tech” (12 February), at https://www.ornl.gov/news/ornl-teams-los-alamos-epb-demonstrate-next-generation-grid-security-tech, accessed 6 March 2024.

A.O. Omobowale, O. Akanle, and D. Busari, 2023. “Social science foundations of public policy,” In: E.R. Aiyede and B. Muganda (editors). *Public policy and research in Africa*. Cham, Switzerland: Palgrave Macmillan, pp. 29–61.
doi: https://doi.org/10.1007/978-3-030-99724-3_3, accessed 6 March 2024.

Quantum Xchange, 2021. How does quantum key distribution (QKD) work?” (23 April), at https://quantumxc.com/blog/how-does-quantum-key-distribution-work/, accessed 6 March 2024.

Quantum Xchange, 2020. “What are quantum networks and how do they work?” (20 January), at https://quantumxc.com/blog/what-are-quantum-networks-and-how-do-they-work, accessed 6 March 2024.

Qrypt, 2021. “About us” (18 October), at https://www.qrypt.com/about-us/, accessed 6 March 2024.

D. Reamer, 2015. “‘Risk = probability × consequences’: Probability, uncertainty, and the Nuclear Regulatory Commission’s evolving risk communication rhetoric,” *Technical Communication Quarterly*, volume 24, number 4, pp. 349–373.
doi: https://doi.org/10.1080/10572252.2015.1079334, accessed 6 March 2024.

T. Roberson, J. Leach, and S. Raman, 2021. “Talking about public good for the second quantum revolution: Analysing quantum technology narratives in the context of national strategies,” *Quantum Science and Technology*, volume 6, number 2, 025001.
doi: https://doi.org/10.1088/2058-9565/abc5ab, accessed 6 March 2024.

E. Schmidt, 2023. “Innovation power: Why technology will define the future of geopolitics” *Foreign Affairs*, volume 102, number 2, pp. 38–52, and at https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics, accessed 6 March 2024.

F.L. Smith, 2020. “Quantum technology hype and national security,” *Security Dialogue*, volume 51, number 5, pp. 499–516.
doi: https://doi.org/10.1177/0967010620904922, accessed 6 March 2024.

Toshiba, 2022. “Toshiba, Chicago Quantum Exchange partner to activate quantum network between University of Chicago, Argonne National Laboratory” (19 April), at https://news.toshiba.com/press-releases/press-release-details/2022/Toshiba-Chicago-Quantum-Exchange-Partner-to-Activate-Quantum-Network-between-University-of-Chicago-Argonne-National-Laboratory/default.aspx, accessed 6 March 2024.

R. van Belkom, 2020.“AI no longer has a plug,” *Stichting Toekomstbeeld der Techniek* (30 June), at https://stt.nl/nl/toekomstverkenningen/de-toekomst-van-ai/ai-no-longer-has-a-plug, accessed 6 March 2024.

R. Van Meter, 2014. *Quantum networking*. Hoboken, N.J.: Wiley.

doi: https://dx.doi.org/10.1002/9781118648919, accessed 6 March 2024.

P. Vermaas, D. Nas, L. Vandersypen, and D. Elkouss Coronas, 2019. “Quantum Internet: The Internet’s next big step,” *Delft University of Technology*, at https://research.tudelft.nl/en/publications/quantum-internet-the-internets-next-big-step, accessed 6 March 2024.

R.H. Weber, 2008. “Transparency and the governance of the Internet,” *Computer Law & Security Review*, volume 24, number 4, pp≥ 342–348.
doi: https://doi.org/10.1016/j.clsr.2008.05.003, accessed 6 March 2024.

M.E. Weston and A. Bain, 2010. “The end of techno-critique: The naked truth about 1:1 laptop initiatives and educational change,” *Journal of Technology, Learning, and Assessment*, volume 9, number 6, n6.

G.B. Xavier, T. Ferreira da Silva, G. Vilela de Faria, G.P. Temporao, and J.P. von der Weid, 2009. “Practical random number generation protocol for entanglement-based quantum key distribution,” *Quantum Information and Computation*, volume 9, numbers 7-8, pp. 683–692.
doi: https://doi.org/10.26421/QIC9.7-8-10, accessed 6 March 2024.

Editorial history

Received 8 February 2024; revised 5 March 2024; accepted 6 March 2024.

Societal implications of quantum technologies through a technocriticism of quantum key distribution
by Sarah Young, Catherine Brooks, and Jason Pridmore.
First Monday, volume 29, number 3 (March 2024).
doi: https://dx.doi.org/10.5210/fm.v29i3.13571