At the Intersection between Quantum Communication Networks and Standardisation

Report authors: Nathan K Langford and Simon J Devitt
ABOUT STANDARDS AUSTRALIA

Standards Australia is an independent, non-government, not for profit organisation. We are the nation’s peak non-government standards development organisation.

The work of Standards Australia and our staff, stakeholders, members and contributors enhances the nation’s economic efficiency, international competitiveness and contributes to a safe and sustainable environment for all Australians.

Standards Australia’s vision is to be a global leader in trusted solutions that improve life – today and tomorrow.
Authors

Nathan Langford
A/Prof. Nathan Langford is a lecturer in physics at UTS, a former ARC Future Fellow, and Director of the newly formed Advanced Prototype Packaging Facility (UTS/USYD). He leads the Millikelvin Quantum Science laboratory and the new Hardware Team in the UTS Centre for Quantum Software and Information. Nathan has over 20 years’ experience in advanced experimental quantum science research, working at top labs in Australia, Europe and the US. His CirQuS (Circuit Quantum Science) research group focuses on performance characterisation and optimisation in circuit-QED based Digital Quantum Simulations, as well as Quantum Chaos, Quantum Control and quantum device benchmarking techniques including quantum tomography. He is an active member of the Sydney Quantum Academy, having served on its Technical Advisory Committee for the 4 years since it was established, and through his recent infrastructure development activities, Nathan is also engaging widely with local NSW quantum and advanced manufacturing industry. Since 2022, Nathan has been a member of the ISO/IEC JTC 1 Working Group 14 on Quantum Information Technology. He is playing an influential role in both WG 14’s international standards development work, and the strategic development of Standards Australia’s national quantum standardisation activities.

Simon Devitt
A/Prof. Simon Devitt is Research Director at the Centre for Quantum Software & Information at UTS. His research focuses on Quantum Error Correction and Fault-tolerance, the design of large-scale quantum computing and communications systems and the compilation and resource optimisation of quantum algorithms. Simon is the co-founder and managing director of h-bar quantum consultants and Co-founder of a new quantum start-up, Eigensystems Pty Ltd. Having spent over a decade overseas working in the quantum computing programs of the UK and Japan, Simon has worked with numerous corporations, startups and VC firms on their expansion into the quantum technology space and advised multiple government agencies on multimillion-dollar R&D initiatives.

Acknowledgements

Standards Australia would like to acknowledge the support of the Australian Department of Industry, Science and Resources in the development of this white paper.

The authors would like to acknowledge Peter Rohde for reading and providing feedback on this report.
Contents

Authors ........................................................................................................................................ 3
Executive Summary .................................................................................................................. 5
1. Quantum Communications ................................................................................................... 8
2. From Cryptography to Quantum Communications .............................................................. 9
3. Distribution Hurdles for Quantum Communications .......................................................... 11
   3.1 The Quantum Fibre Network ........................................................................................ 11
   3.2 The Quantum Satellite ................................................................................................ 12
   3.3 Application-specific Challenges .................................................................................... 15
4. The quantum communication application stack ............................................................... 16
5. The quantum communications end game ............................................................................ 17
   5.1 A Future Entanglement-based Economy ...................................................................... 17
   5.2 The Geopolitics Of Entanglement ............................................................................... 19
   5.3 The Technology End Game .......................................................................................... 19
6. The role of standards in quantum communication ............................................................. 26
   6.1 Standardisation Case Studies ....................................................................................... 27
   6.2 An overview of current standardisation activities in quantum communications .......... 31
   6.3 Needs and opportunities for standardisation in quantum communications at different scales ................................................................................................................................. 34
   6.4 Needs and opportunities for standardisation in quantum communications across different spheres of engagement .................................................................................................................. 39
Bibliography .......................................................................................................................... 43
Executive Summary

The Next Generation of Human Communications: Communications systems are at the foundation of all human social, economic and technological development. Ever since the dawn of civilisation, our need and ability to communicate over vast distances has evolved and become more and more sophisticated. Today, humanity has constructed the largest piece of infrastructure ever: the global telecommunications system. Built using a variety of technologies from satellites to deep-sea fibre-optic systems to WiFi, Bluetooth and other radio-, microwave- and optical-frequency communications systems, the global telecommunications grid is extensive in coverage, unparalleled in connectedness and ubiquitous in application. As we move towards the middle of the 21st century, we are on the cusp of the next major revision to this system: incorporating quantum communications technology.

One of the three pillars of second-generation quantum technology, along with quantum computing and quantum sensing, quantum communication promises a plethora of new capabilities and applications. Growing out of visionary questions on the information coding and security limits offered by quantum physics, quantum communication was emerging before people even considered the prospect of quantum computing, with research starting in the late 1960s and early 1970s (Wiesner, 1983) (Holevo, 1973), 10–15 years before Feynman famously pointed out that the best machine for simulating nature should be quantum.

Quantum communication systems are a marvel of engineering, with faithful transmission of quantum information often requiring the transfer of individual particles of light—photons—through a world bathed by trillions upon trillions upon trillions of photons. Today, nascent commercial quantum communications systems aim to realise the potential for cryptographic security guaranteed by the laws of quantum mechanics, to provide a technological alternative to the public-key encryption protocols, used so ubiquitously across the global telecommunications grid, that are now vulnerable to the threat posed by future quantum computing systems. Quantum protocols, including the actual teleportation of quantum information, have now been demonstrated through fibre optics systems, between two islands off the coast of Africa, and up to satellite platforms orbiting at over 20,000km per hour. Complex quantum communication grids are now being built in several nations, including a multi-node quantum communications network in the Netherlands, facilitated by small, diamond-based quantum repeaters and an extensive quantum key distribution network in China consisting of fibre, satellite and even drone technology.

The Telecommunications Grid of the Future: While this new technology is currently focused on the security that quantum mechanics can provide, the broader goal for quantum communication is far more interesting. The classical internet, with its profound interconnectedness provided by almost light-speed communication between individuals and our computational systems, has resulted in arguably the largest societal, economic and technological change in the history of our species. What will happen when we can augment the system with quantum capabilities included? The concept of a full quantum internet, that connects together a vast array of quantum computing systems and quantum-enabled sensors, would represent a paradigm shift in how humans process information and communicate with each other. The road ahead, from the rudimentary systems we can build today, to a fully formed and functional quantum internet is a long one, with many scientific and technological hurdles to solve: ultimately, the infrastructure must realise to build a quantum internet is likely to prove more difficult than building full, scalable quantum computing systems.

What is this report about? We commence this report with an introduction into the development of quantum communications networks, before discussing key challenges facing state-of-the-art quantum networks built using classically originated technologies of fibre and satellite networking. We then argue why the most profound impacts for quantum communications lie in moving beyond quantum cryptography to full quantum-powered entanglement-distribution-connected networks of quantum computers and quantum sensors. Such networks would
create a fundamentally new paradigm for international and cooperative relations built on the uniquely quantum, exponentially scaling computational power of connected quantum computers (Rohde, The quantum internet: The second quantum revolution, 2021). To explore the challenges that lie ahead, we consider a range of potential quantum communications end-game scenarios, from quantum-resilient encryption systems (built on classical technologies) and QKD, to a full-scale quantum internet driving an economy powered by shared entanglement resources. We discuss how requirements and applications will vary across the different end-game scenarios, and argue that the path to fully quantum-powered quantum communications is unavoidably tied to the trajectory of quantum computing development. Our analysis suggests that profound impact could already be realisable at scales involving modest numbers of connected quantum computers.

To discuss the role that standardisation processes can play in the development of quantum communications networks, we explore the needs and opportunities for standardisation across different technology scales and across five different spheres of stakeholder engagement for the quantum communications community (Langford & Devitt, 2023):

**Key needs and opportunities for standardisation in quantum communications**

1. **Engaging within the community**
   - Different hardware modalities for quantum communications networks make standardisation difficult, but arguably even more necessary, especially for ensuring the interface compatibility which is so crucial to networking environments.
   - Standardisation will improve communication and compatibility between different technology platforms and layers.
   - *Post-quantum cryptography* will require detailed standardisation to allow the major transition away from existing quantum-hackable cryptography to proceed smoothly.
   - Information-theoretic security offered by *QKD* networks could be classified across tiers according to architecture and protocol robustness, and vulnerability mitigation. Standardisation of hardware modalities may be required for large-scale networks.
   - Networking relying on any “quantum-safe” cryptography will require detailed protocol standardisation to certify genuine benefit and compliance to best practice.
   - Entanglement-distribution-based networks inherit standardisation requirements from both *QKD* networks and data-centre/HPC-cluster scale quantum computers, while facing additional new requirements to achieve more extensive interfacing.
   - While the benefits of a fully quantum-enabled *entanglement-based economy* would be wide and profound, the technical challenge would be at least equally so, and most standardisation activities would currently be meaninglessly speculative.
   - As with quantum computing, focussed initiatives by governments, broad industry consortia or key players are proving most agile at starting to develop standards.

2. **Engaging with suppliers**
   - Quantum communication technologies demand key aspects of performance from supporting technologies far surpassing what they were originally developed for.
   - Developing *Requirements Specifications* for supporting equipment will provide near-term benefits from formal standards development for scaling up quantum networks.
   - If *QKD* networks are to be deployed at scale, this offers new economic opportunities for enabling technology manufacturers willing to engage with new requirements.

3. **Engaging with end users**
   - Establishing rigorous implementation and quality assurance standards will provide important increased confidence for early adopters of *PQC* and *QKD-only networks*. 

---

*At the Intersection between Quantum Communication Networks and Standardisation*  
Research Report, April 2023
• New algorithms and use cases for quantum computing and distributed quantum information processing could strongly influence its reach across sectors, and the technology scales it could be usefully deployed at.
• Developing them requires highly interdisciplinary collaboration with end users.
• Significant innovation is required to understand how fully distributed entanglement networks can facilitate new applications for end-user sectors.
• New standards for negotiating network access will change how end users connect individual quantum computers into a larger network to access exponentially improved computational power for distributed and blind quantum computing.

4. **Educating a quantum workforce**

• Innovation is still required, to identify if standardisation can play a substantive role in helping to grow the broader quantum workforce pipeline.
• Detailed PQC implementation Specifications can help quantum algorithms experts target their efforts at developing new quantum attacks on new PQC protocols.
• The best opportunity for standardisation is to establish Terminology and Requirements standards to help train expert technicians and engineers in supporting areas, especially those required for PQC and QKD-only networks.

5. **Engaging with the wider community**

• In the rapidly developing industry, we are seeing the emergence of so-called “quantum” providers who are not delivering genuine quantum benefits, which risks damaging public and investor confidence.
• Developing robust, objective, widely adopted (and developed), comprehensive and accessible Quality Assurance standards to enable due diligence and regulatory oversight will be crucial to maintain end-user, investor and government confidence.
• Good terminology and informative standards could facilitate better communication with external stakeholders, to help build confidence and public licence.

We also consider what we can learn from existing and forthcoming standardisation activities, e.g., in relation to how to maximise agility and pace of standards development while maintaining quality control. As with quantum computing, we see again that the most agile standards development is currently being driven by national and regional standards bodies, with leading roles being played ETSI (Europe) and NIST (US). **We also argue that it will not be possible to realise full quantum-powered quantum communications networks without quantum technology standards being closely and strategically coordinated, e.g., by a dedicated international quantum standardisation organisation.** We believe that current efforts towards establishing a single unified home for quantum technology applications, including both quantum communication and quantum computing, and ideally also second-generation quantum sensing technologies, will deliver significant benefits for quantum standardisation and quantum technologies overall, and also for the role of quantum technologies in the wider community.
1. Quantum Communications

Reliable, fast, long-distance communication has always been a driver of technological and economic progress. Whether couriers on foot or horseback, carrier pigeons, smoke signals, semaphores or electronic and optical signals, humanity has continually refined technology to make long distance communications easier, faster, cheaper and more reliable. We now live in a world where near-light-speed, global communications is universally available and, for a significant fraction of the population, accessible with a device that lives in our pockets.

Quantum Communication has emerged as one of the main pillars of second-generation quantum technology, along with Quantum Computing and Quantum Sensing. Communication systems that actively exploit the behaviour of quantum mechanics were arguably the first to identify and demonstrate practical applications for this second generation of quantum technologies.

Quantum communications developed initially out of two key motivations: the search for increased information density, and the search for increased information security; and these form two key conceptual foundations for the field today. The first is epitomised by Holevo’s seminal paper in 1973 (Holevo, 1973) that demonstrated that it was impossible to extract more than N-bits of classical information from N-qubits of quantum information. This result was the first in what is now an entire subfield of quantum information that is sometimes referred to as quantum communications theory or quantum resource theory (Chitambar & Gour, 2019; Wilde, 2013). Essentially, this field of quantum communications research examines theoretical limits that quantum mechanics place on the transmission of information, extending many of the results of researchers like Shannon and Von Neumann who formulated the equivalent framework for classical communications channels.

The second direction arose out of the world of cryptography. Quantum bit commitment (Lo & Chau, 1997), Quantum money (Wiesner, 1983), Quantum Key Distribution (QKD) (Bennett & Brassard, 1984) and random number generation (Pironio, et al., 2010) were a series of protocols that demonstrated how quantum mechanics allowed for certain cryptographic tasks that are not possible using classical communications theory.

While researchers initially came to quantum communications theory from two somewhat distinct directions, in the subsequent 45 years we have built a much more comprehensive framework of quantum communications theory and how it relates to practical protocols such as QKD and distributed quantum computing. The invention of practical techniques to transmit quantum information across the globe has led to multiple technology demonstrators by multiple nations of metropolitan-scale quantum communication networks (Sasaki, 2011) (Peev, 2009) (Elliott, 2004) (Tessinari, 2019) for QKD, intercity networks (DelftQKD21, n.d.) and even global-scale communications enabled by quantum-equipped satellite platforms (Yin, 2017) (Chen, 2021) (Liao, 2018).

We have now reached the stage where serious discussion and design surrounding a future quantum internet is occurring (Rohde, The quantum internet: The second quantum revolution, 2021) (Wehner, Elkouss, & Hanson, 2018). A quantum internet will sit alongside the classical internet and will ideally support a range of protocols from QKD and other quantum secure cryptographic applications all the way through to entanglement-assisted distributed quantum sensing and fully fault-tolerant distributed quantum computing. Ultimately, quantum communication faces the same challenge that faces quantum computing: the classical technology that it attempts to improve upon is already extremely advanced and immensely powerful. Realising its potential cannot simply be a question of doing the same job a bit faster. Like quantum computing, its greatest promise lies in the possibility of realising tasks that are fundamentally out of reach of classical technologies: such as guaranteed security and networked quantum algorithms.
2. From Cryptography to Quantum Communications

Cryptographic protocols were one of the most important applications that initially motivated research into quantum communications during the 1970's and early 1980's. As often happens for paradigm changing research, the small group of researchers who founded this new field initially found it extremely difficult to gain traction in the wider community. As Gilles Brassard noted, when Stephen Weisner first submitted his paper describing the basic ideas of quantum money and conjugate coding to IEEE Transactions on Information Theory, it was rejected as it was "deemed incomprehensible by the editors and referees because it was written in the technical language of physicists" (Brassard, 2005). While the work was completed in the late 1960s, the paper would remain unpublished until 1983 (Wiesner, 1983).

The concept of conjugate coding from Weisner came from the understanding that in quantum mechanics, a valid quantum mechanical state could encode two simultaneous messages, either of which could be read by a receiver, but not simultaneously. Weisner realised that this property of quantum mechanical particles could be used as a cryptographic tool that was grounded in the basic physical rules governing our universe.

The second application that Weisner proposed in his original paper is now known as quantum money and is based on the same basic principle of conjugate encoding. In this example, he proposed that a banknote could be printed containing a long chain of qubits within the banknote itself that could be initialised into certain quantum states and then measured later without destroying the qubits in the banknote. Weisner did not believe his theoretical innovation was going to be a practical solution for solving the counterfeiting problem in real currency, but what he discovered was that quantum mechanics allowed for the preparation of shared randomness between two parties, facilitated by the probabilistic nature of quantum mechanics itself (Wiesner, 1983).

Cryptography loves randomness, its underpinning aim being the encryption and transmission of messages that appear random to anyone not "authorised" to read it. The randomness that is generated by cryptographic protocols is essential to how they work.

Inspired by the work of Weisner, Charlie Bennet and Giles Brassard introduced the most well-known quantum communications protocol in 1984, solving the problem of generating a shared secret key between two distant parties. Now known as the BB84 Quantum Key Distribution protocol (Bennett & Brassard, 1984), it is currently the most widely implemented quantum communications application, has been demonstrated in a variety of hardware environments and is the application of choice for a variety of quantum communication networks running around the world (Stanley, Gui, Unnikrishnan, Hall, & Fatadin, 2022).

The BB84 protocol extends the idea of conjugate coding to allow Alice and Bob to create a shared binary string that can be used as a "key" – a small, random bit string that enables a cryptographic algorithm to effectively encode ciphertext from a larger input string - with security based on fundamental principles of quantum physics, for use in classical, symmetric (or private-key) cryptographic protocols (Kong, Ang, & Seng, 2015). This key exchange problem is a critical vulnerability for classical crypto-systems. If Alice and Bob are physically separated and cannot guarantee the security of a classical communications channel (because if you could, you wouldn't need the key in the first place), how do they establish an initial shared binary string that they could use as a key for more data-intensive, encrypted, communications? If the communications channel used to share a key is vulnerable to interception by an eavesdropper (Eve), then any key-encoded message is no more secure that an attempt to send the message directly between Alice and Bob without any encryption.

Quantum Key Distribution protocols were arguably the first ideas in the development of second-generation quantum technologies that generated significant interest outside the academic community. New protocols for cryptography and cryptanalysis naturally elicit plenty of interest from government and intelligence agencies, who are always looking for the most secure means.
to encrypt information and also the most sophisticated techniques to attack other people’s cryptography. Interest in quantum communication, and its promise of security underpinned by physical laws rather than assumed mathematical complexity, slowly increased throughout the 1980s and early 1990s. This included new quantum protocols to build cryptographic primitives (Crepeau, 1992), and the development of key exchange based on entanglement (Ekert, 1991), the fundamental aspect of quantum mechanics that underpins all second-generation quantum technologies, or more specifically Bell’s theorem (Bell, 1964), one of the most important foundational results in quantum information theory.

The Ekert 91 protocol was first described in 1991 by Artur Ekert (Ekert, 1991), and he demonstrated that Bell’s theorem, a fundamental test of quantum theory developed in the 1960s, could be used to build a cryptographic protocol based on the entanglement generated between two parties. Even though Bell’s theorem and its initial experimental tests were well established before the 1990s (Freedman & Clauser, 1972) (Aspect, Dalibard, & Roger, 1982), it wasn’t until 2015 that tests rigorous enough to close testing loopholes (that is, implement the theorem’s conditions sufficiently strictly) could be performed (Henson, 2015) and it was only in 2022 the Nobel prize was finally awarded to recognise this fundamental theorem that underpins the security of the Ekert 91 quantum key distribution protocol.

During the 1990s and early 2000s, there were multiple projects administered by the US Department of Defence aimed at building the application stack and the hardware associated with rudimentary quantum communication networks (QuIST, 2001) (QCC-Timeline, n.d.). Interest in the technology was significantly increased when Shor found an efficient algorithm for breaking public key (asymmetric) cryptographic protocols based on factoring large numbers (Shor, 1997).

Test networks were built in numerous locations around the world, including Boston (Elliott, 2004), Vienna (Peev, 2009), Tokyo (Sasaki, 2011) and the UK (Tessinari, 2019), based on the transmission of single particles of light (photons) to carry the quantum information necessary to create cryptographic keys. These networks were not large, in terms of their number of “nodes” or geographic extent, but they were effective proof-of-principle demonstrations of quantum-enabled key exchange networks.

QKD systems do face a number of important technical limitations. Despite the obvious important of cryptography for national security and intelligence agencies, US and UK security organisations have both released statements against the current adoption of QKD for national security applications (NSA, n.d.) (NCSC, 2020). The main fundamental limitation is that QKD does not provide a full cryptographic solution: It does provide in principle security for establishing a secret shared key between two end users. It does not provide a means to authenticate the user at the other end, leaving it vulnerable to attack by an intermediate party who establishes secret keys with two end users who think they are communicating with each other. No known quantum solution exists for digital authentication. QKD can, however, be combined with extremely strong classical digital signatures to provide authentication. For example, there is a general consensus that hash-based digital signatures (NIST ITL, 2022) are almost certainly not vulnerable to quantum computing attack, because they are highly unstructured (Rohde, Information security in the quantum era (review; manuscript in preparation), 2023; Rohde, The quantum internet: The second quantum revolution, 2021). QKD systems are also likely to be more vulnerable to denial-of-service attacks (NSA, n.d.).
3. Distribution Hurdles for Quantum Communications

Quantum information has one difference from classical information that is responsible for both the security offered by appropriately distributed quantum information, and the most fundamental challenge for constructing a large-scale quantum communication network: the no-cloning theorem (Dieks, 1982) (Wooters & Zurek, 1982).

Classical information can be copied. It is the best method we have for providing error correction redundancy in classical communication and computation. If a communications channel is noisy or lossy, or in any way unreliable, we can simply copy a message hundreds, thousands or millions of times. It is even okay if 99% of the information we want to transmit is lost, because we have copied it so many times that some of it will reach the intended receiver. We can’t do this with quantum-encoded information.

In its simplest form, the no-cloning theorem states that it is impossible in quantum mechanics to exactly copy unknown pieces of quantum information. This is not a technical restriction: it is a fundamental law of nature similar to Einstein’s proof that nothing in space can travel faster than the speed of light. And it creates an obvious problem: How do we protect quantum communication channels against noise if the most effective method we know of in classical communications – transmitting many different copies of the information – is unavailable to us? A critical focus is therefore obviously to find more reliable ways to transmit quantum information – that is, reduce the noise. But this is also extremely difficult when the information is being carried by literally a single particle of light.

3.1 The Quantum Fibre Network

Optical fibre was one of the obvious choices for distributing photons for quantum communications, and fibres are, for classical communications, extremely reliable. However, for the transmission of quantum information, our current technology is very lossy. The best low-loss, single mode, optic fibre that is commercially available is optimised for photons with a wavelength of 1550nm and has a loss rate of approximately 0.14dB/km (Hasegawa, 2018). This means that over approximately 21km, a single photon has a 50% chance of being lost. This is already an astonishing feat of technology: if ocean water were as clear as this fibre, one could see to the very bottom of the Mariana Trench in the Pacific Ocean – a depth of 11km – as easily as you can see the bottom of a (clean) backyard swimming pool. For classical communications, this presents no problem, since signals can be amplified indefinitely en route, and improving fibre losses would only modestly reduce costs by reducing the number of amplifiers required in a given stretch of fibre. But for quantum communication purposes, where the no-cloning theorem prevents straightforward signal amplification, such losses present a profound challenge.

Classical fibre repeaters, which rely on amplification, are compact units that are installed in-line with the fibre cable, usually containing an erbium-doped fibre amplifier powered by a conductor also carried within the cable (Repeaters, n.d.). Long distance fibre optic lines generally have repeaters placed approximately every 100km (around 98% loss). Classical fibre repeaters effectively measure the bitstrings carried by the light and then re-transmit them. But in quantum communication, simple amplification (copying) is prohibited by the no-cloning theorem.

Entanglement again provides the solution, enabling the quantum equivalent of a signal repeater (Ruihong & Ying, 2019), though quantum repeaters do not rely on the same operating principles. Entanglement is usually distributed using simple Bell pairs, which are known states and can therefore be reproduced indefinitely. “Repeat-until-success” strategies allow entanglement to be distributed reliably even in lossy environments. Unknown quantum states (including shared entanglement) can then be communicated by combining shared Bell states with quantum teleportation. This makes entangled Bell states a fundamental resource for quantum communications. Wider implications of this are discussed in Section 5.
Quantum repeaters effectively utilise the concept of redundant encoding to embed a Quantum Error Correction (QEC) code within a large collection of single photons (Fowler, 2010) (Azuma, Tamaki, & Lo, 2015). Essentially, we encode a single qubit of information across many individual photons in a way that allows us to reconstruct the encoded information even if multiple photons used within the encoding are lost during transmission. A quantum repeater processes and effectively “refreshes” this encoding.

This encoding does allow sufficient redundancy to transmit over longer distances, but comes with numerous disadvantages:

1. Quantum mechanics imposes a fundamental limit on the number of photons we can lose. Because of the no-cloning theorem, if we lose more than 50% of the photons used in the encoding, we cannot reconstitute the quantum information at the repeater station. Consequently, quantum repeaters must be placed close enough such that greater than 50% of the photons are successfully transmitted to the repeater station.

2. Quantum repeaters are themselves mini-quantum computers. They require the same cooling infrastructure, vacuum infrastructure, power, and control electronics of a standard quantum computing system. However, in the case of the repeater, all of this must be placed into a device that has high reliability, effectively no need for maintenance and, to achieve global quantum networking, will ultimately need to be deployed in very inhospitable locations such as deserts and at the bottom of the ocean.

3. Quantum repeater networks do not provide high bandwidth end-to-end connections over long distances. Due to the complicated protocols necessary at each repeater station, obtaining a trans-oceanic link – of the order of 5000–10,000km – that can be operated at even MHz or higher is not possible, even in the most optimistic theoretical analyses (Fowler, 2010) (which is already 100,000s times slower than the 100s of gigabits per second which can be achieved in modern fibre-based internet connections).

Despite these drawbacks, several nations have devoted significant investment into a repeater-based quantum communication network. Arguably the most advanced is the Dutch quantum repeater network, designed to connect the cities of Amsterdam, Leiden, the Hague and Delft (DelftQKD21, n.d.). In such a small nation, the complications described above don’t have a significant impact on the deployment and operation of a repeater-based quantum network. This network has achieved some significant milestones in the past 5 years (Pompili, 2021) and is a quantum network designed to also enable more complex applications. This contrasts with previous fibre-based quantum networks that were exclusively used for Quantum Key Distribution (QKD) protocols. These networks do not require as strict performance requirements, as distribution of a classical key does not require reconstruction of the full quantum information after transmission (Diamanti, Lo, Qi, & Yuan, 2016). Photon loss in a QKD network can therefore be largely corrected in sophisticated classical software post-processing and ultimately only effects the rate in which you can build a secret key. A quantum network that can be used to transmit and receive quantum information that can be processed further – in the same way the classical internet operates – is much more difficult to construct.

3.2 The Quantum Satellite

The complications associated with long-distance quantum communication through fibre-optic systems are well known, and while fibre systems have improved over the past 20–30 years, it has not improved enough for it to be an effective backbone for global quantum communications.

Starting in the early 2000s, researchers in Austria began to investigate the viability of long-distance quantum communication through free space. This culminated in a set of seminal experiments performed between the islands of La Palma and Teneriffe in the Canary Islands, off the west coast of Africa (Ursin, 2007) (Schmitt-Manderbach, 2007) (Ma X., 2012).

The researchers used high-quality telescopic receivers and laser-driven photon sources to demonstrate a QKD connection over 144km of free space between the two islands (Ursin, 2007).
This, and related (Villoresi, 2008), work investigated the absorption and scattering properties of the atmosphere, how to align and track the telescopes for sending and receiving the quantum information, and whether individual photons could be accurately tagged so that Alice and Bob could synchronise which photons were carrying which individual pieces of quantum information used to form a cryptographic key.

These initial investigations into the utility of free-space quantum communication made crucial steps to providing answers to the question we were really interested in: would it be feasible to achieve long-distance quantum communication by placing sources of quantum entanglement into space and beaming them to the ground?

From 2007 – when the free-space quantum communication link in the Canary Islands was first demonstrated – to 2016, there were several projects proposed to extend quantum communication into space, the most notable being a European Space Agency proposal to place a photon source onto the International Space Station (Armengol, 2008). These efforts were then eclipsed when researchers in China launched the Micius quantum satellite platform as part of their “Quantum Experiments at Space Scale” project in August 2016 (Lu, 2016). This project was the crown jewel of a rapid expansion into quantum technology R&D undertaken in China between 2010 and 2014, and was to be a core trunk-line technology for a national QKD network developed by China, motivated by the Snowden leaks in 2013 (Devitt S., 2020).

The Micius platform was and is unique in the expansion of quantum communications into space, being the only quantum satellite to achieve (Lu, 2016):

1. Distribution of entangled photon states from the satellite to ground stations.
2. Demonstration of the original BB84 QKD protocol between space and ground.
3. Demonstration of the Ekert91 entanglement-based QKD protocol between two ground stations, mediated by entangled states supplied by the satellite.
4. Teleportation of a quantum state from a ground station to the satellite
5. Teleportation of a quantum state from the satellite to a ground station.
6. Distribution of a secure key between Austria and China, mediated by the Micius satellite and used to provide an encryption key to encode a video conference feed between the Chinese Academy of Sciences and the Austrian Academy of Science.

The Micius platform was a tour de force and undoubtedly a huge advance in the development of quantum communications technology in space, and many nations have now built R&D programs to develop and deploy quantum-enabled communications platforms. However, as with quantum repeater systems, the fact that we must faithfully transmit single particles of light to transmit the quantum information creates significant technological hurdles for leveraging space technology to enable global quantum communications. As with fibre systems, photon loss is major hurdle, this time caused by the interaction between the earth’s atmosphere and the photons as they travel to the ground.
The Micius platform has provided extensive data on the effective photon loss rates that we can expect from a quantum satellite system, and theoretical work on a quantum version of a low-earth to medium-earth orbit satellite constellation has estimated the loss rates for quantum communication between city pairs (Khatri, 2021):

<table>
<thead>
<tr>
<th>Comms link</th>
<th>Distance</th>
<th>Loss rate</th>
<th>Satellite altitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toronto – New York:</td>
<td>551km</td>
<td>99.69%</td>
<td>500km</td>
</tr>
<tr>
<td>Sydney – Auckland</td>
<td>2156km</td>
<td>99.997%</td>
<td>500km</td>
</tr>
<tr>
<td>New York – London</td>
<td>5569km</td>
<td>99.9999%</td>
<td>3000km*</td>
</tr>
</tbody>
</table>

*Satellite altitude from New-York to London is elevated to 3000km for better line of sight.

These loss rates are obviously extreme and unfortunately, since they are caused by random, constantly fluctuating interactions between the atmosphere and the photon stream, there are few options available to reduce the loss rate. Therefore, while satellites have a better ability to reach global distances, they ultimately suffer from the same issues that plague fibre-based communication networks. They may also be harder to solve, since space-based platforms may be even harder to access than deep-sea quantum repeater stations.

The Micius platform weighed approximately 630kg and the reported cost to launch this system into low earth orbit was over $100M USD (Micius, n.d.) (Lu, 2022), even for a comparatively simple entangled photon emission device and telescope transmission system. Introducing sufficient redundancy into the quantum payload to provide high-rate, low-loss satellite-to-ground transmission of quantum entanglement will be a much greater technological challenge, as it would require literally deploying small-scale quantum computing systems into space.

---

These initial testbed systems provide us with extensive data on the advantages and limitations of our current approaches, which in many ways have simply taken the technology used for our classical communications infrastructure and attempted to “port” it across to the quantum regime. As we will discuss later in this report, this may not be the way we ultimately achieve the goal of a quantum internet.

### 3.3 Application-specific Challenges

Quantum Key Distribution was the first application identified in the communications space, and largely remains the only protocol utilising nascent fibre and free-space quantum communications systems. The idea of a QKD network is often conflated with a more general purpose “quantum internet” (Rohde, The quantum internet: The second quantum revolution, 2021), with both terms often used synonymously. However, the communication link, network constraints and performance required are all significantly different for the two deployment scales.

QKD networks are designed for a very specific task: to generate a random, shared classical bit-string between two classical network users. This shared bit-string ultimately becomes the key that is used in strong symmetric encryption protocols to secure a classical communications channel. In this context, a QKD network can delegate the “heavy lifting” of correcting errors in the quantum distribution network to the classical bit-string processing used to create the final key. Specifically:

- Photon loss in a QKD network does not result in a loss of information, instead it will decrease the rate in which secret bits are created.
- Error correction in QKD systems occurs after the photons are received and converted back to classical information. Hence, error-correction redundancy does not have to be built into the photons that are transmitted. This allows QKD systems to work even when quantum state fidelities are extremely low (provided bipartite fidelities are above a minimum threshold of 50%) (Wooters & Zurek, 1982).
- QKD is not a high data-rate protocol. A strong key for a symmetric cypher can be as little as 256-bits long (AES, n.d.). While AES does not offer unconditional security, it makes limited assumptions and is already considered quantum resilient. Hence the quantum platform does not have to provide high bandwidth before it becomes useful.

A quantum internet is a completely different entity, and a completely different scale of technical challenge. In its fullest realisation, a quantum internet would allow direct connection between individual quantum computing systems for distributed processing (Rohde, The quantum internet: The second quantum revolution, 2021) (Wehner, Elkouss, & Hanson, 2018). These could include high-capacity, high-performance quantum servers and smaller, even individual-user quantum computers. In our first report on quantum computing (Langford & Devitt, 2023), the far future of quantum computing technology may end up realising the construction of only a handful of quantum computing systems, due to the cost of manufacturing and deploying fully fault-tolerant, error-corrected systems, or in a future of ubiquitous quantum computing systems, where qubits become as cheap to manufacture as classical transistors and quantum computers evolve into a full consumer market. Ultimately, the far future of quantum communications could also end up realising completely different scales both in geographical reach and computational power and complexity.
4. The quantum communication application stack

In many ways, future quantum communications systems will end up being driven by what the quantum computing landscape evolves into, while also benefiting from the technology developments achieved along the way. A network connecting numerous quantum computing systems is only desirable if there exist many quantum computing systems to connect. Assuming for the moment the most optimistic scenario where quantum computing becomes a ubiquitous technology, there is a plethora of communication tasks, including those related to security, that become available as quantum communication networks become larger and more sophisticated:

- **Quantum-enabled authentication (Security)** (Dutta & Pathak, 2021): Classical networks often rely on handshake protocols to ensure that two parties can authenticate they are talking to the right people – think of the two-factor authentication codes sent to your phone every time you try to log into a secure system. These tokens are vulnerable to hacking, interception or compromise of the mathematical problems that are used to build them. Replacing these protocols with distributed entanglement can result in much more secure quantum-enabled authentication tokens.

- **Full quantum encryption (Security)** (Diamanti, Lo, Qi, & Yuan, 2016): QKD systems allow for the distribution of keys to be used as the basis of more secure symmetric key protocols. Such encryption protocols could still be found vulnerable to classical or quantum cryptanalysis attacks. If a large amount of quantum entanglement is available, the quantum equivalent of one-time-pad encryption can be used. This type of encryption generates secret data using entanglement that is equal in size to the message being transmitted. This type of encryption does not rely on assumed mathematical complexity to guarantee security and can be used to provide in-principle guaranteed information theoretic security, subject to implementation.

- **Distributed quantum computing (Computation)** (Rohde, The quantum internet: The second quantum revolution, 2021): The power of a quantum computing system scales much differently from that of a classical computer. Connecting classical computers increases the computational power of the system in an additive way. Two classical computers can provide up to twice the computational power when connected compared to each individually. But the power of connected quantum computers increases multiplicatively! Two identical quantum computers, when connected, have a combined power equal to the square of their individual computational power. This creates a massive incentive to provide communications infrastructure that can provide the distributed quantum entanglement required to connect fully fault-tolerant, error corrected machines, and highlights the immense potential of such a fully connected quantum computing network.

- **Blind quantum computing (Computation)** (Fitzsimons, 2017): By combining the concepts of distributed quantum computing with those of quantum cryptography, researchers in the late 2000s developed the idea of blind quantum computation. This was, at the time, unique to quantum technology – in recent years, homomorphic encryption has allowed for the same in the classical world. Blind quantum computing is where a user wishes to utilise the quantum computing power of an external system, but wants to keep secret not only the output of their quantum program, but even the details of what kind of algorithm they are implementing. Blind quantum computing requires the user to prepare and transmit quantum information to a quantum server, who then can enact the algorithm without learning anything about the computation the user wishes to perform.

- **Entangled quantum sensor networks (Networking)** (Van Meter, Quantum Networking, 2014) (Rohde, The quantum internet: The second quantum revolution, 2021): Quantum sensing is often held to be one of the earliest success stories of second-generation quantum technology applications. Currently, researchers and private companies are building small-scale quantum systems that can act as sensitive magnetometers or gravity sensors. While these systems may have some initial value over current sensor solutions, the main payoff from quantum sensing arises when collections of individual sensors can be networked.
together using shared entanglement. Entanglement-enhanced quantum sensors are known to allow for significant increases in sensitivity. Distributed networks of sensors, mediated by a quantum communication network, will be required to fulfill the ultimate promise of quantum-enabled sensing. It may even enable new types of sensing from the delocalisation of the individual sensors, like the massive astro-telescope arrays which provide access to completely different detection regimes.

- **Shared secure networking (Communications)** (Van Meter, Quantum Networking, 2014) (Rohde, The quantum internet: The second quantum revolution, 2021): For highly secured communications, networks are often physically segregated from the global communications grid. The concept of an “air-gapped” network is one where no physical mechanism exists for data to exit the secure network and be transmitted on any piece of physical infrastructure that is considered part of the public internet. This is a costly exercise, as segregated networks are essentially mini-internets that have to be built and maintained. A quantum internet would circumvent this challenge by enabling both highly secure communications and public information on the same physical infrastructure.

Achieving each of these applications requires increasing quantum resources. Quantum authentication and QKD systems require only low-bandwidth, low-fidelity entanglement, while large-scale computational and sensing networks will require extensive infrastructure to achieve flexible high-bandwidth, high-fidelity entanglement across global distances. As with computation, the ultimate nature and scale of quantum communication technology will depend on how cheap and ubiquitous the underpinning quantum technology becomes.

5. The Quantum Communications End Game

5.1 A Future Entanglement-based Economy

If the peak ambition of quantum computing researchers and developers is the creation of a consumer-based quantum computing industry that rivals the current classical computing industry in terms of the sheer number and types of classical computing devices, the peak ambition of the quantum communication industry is the deployment of infrastructure that turns quantum entanglement into a fungible commodity. Quantum entanglement is the resource that is ultimately produced by a quantum network and it is this resource that is consumed for QKD and authentication, all the way up to fully distributed quantum computing.

In many ways, one can make an analogy of quantum entanglement networks with the electricity grid. Various technologies exist to both produce and distribute electricity across nations and continents. But, from the consumer’s point of view, we do not think about this extensive base infrastructure on a day-to-day basis and work only with the abstract resource that we refer to as electricity. When I plug my computer into a mains outlet, the exact way the electrons that I am using were produced—did they come from a coal-fired plant, nuclear or renewables?—is not something I can determine. Nor is the means by which that power was distributed. Utility companies, networks and governments generally take care of the details of how generation and distribution occurs, how grids are interconnected, how base-load and peak-power demands are balanced, and what happens if distribution systems are damaged or destroyed.

The ideal end point for quantum communications systems will be similar to a utility grid, however in this case the resource commodity will be quantum entanglement that is utilised to realise the variety of quantum communication protocols described earlier. The specifics of the technology used to create and distribute this entanglement will be largely irrelevant to the end user. The base technology could be fiber based, satellite based, or even based on a model like Netflix’s original model of physically sending data storage devices through the mail, known as a sneakernet (Sneakernet, n.d.). However, in the case of a quantum sneakernet, these devices would be the quantum equivalent of a hard drive and we won’t be sending DVDs filled with data representing...
the latest Hollywood blockbuster, but instead they would be hard drives filled with quantum entanglement, criss-crossing the planet at high volume, generating a global, high-bandwidth, quantum communication network (Devitt S., 2016).

Quantum entanglement would then be sold as a communications resource, delivered by hardware ostensibly built and operated by the quantum service provider. How this commodity is priced and utilised by the world will then ultimately depend on its value for certain applications. Does the need for encryption keys that are “unhackable” provide sufficient value over utilising the same quantum entanglement to connect two quantum computers together? Can quantum entanglement provide value to people in their everyday lives? Or will it be a reserved resource for the most computationally valuable tasks?

Figure 2: A mock-up of a group of quantum hard drive units that could be used to enable a sneakernet model of quantum communication. Quantum hard drives are connected locally to create entanglement. Each unit contains active error corrected qubit arrays that act as memories, storing information reliably for weeks/months. Each unit is a self-contained system, carrying power, refrigerant and classical control computers. Units are physically distributed around the world and then communicate via the classical internet to perform quantum protocols using the shared entanglement they store. Image courtesy of S.J. Devitt and Turing inc.

As with other infrastructure that services general commodities such as power, water or even food, standardisation will be of crucial importance. We already understand the consequences of incompatible networks in times of need. One of the most striking examples came in 2011 after the Great Tohoku earthquake in northern Japan and the subsequent meltdown of the nuclear reactors at Fukushima. The Japanese government immediately shut down nuclear powerplants across the nation and due to damage in the north of the country, brownouts and rationing began to occur. The southern regions of Japan at the time were producing a power surplus, but it was generally unknown, even to the general population in Japan, that the electricity grid in Japan is geographically essentially divided. The northeastern part of the country operated at 50Hz and the southwestern part at 60Hz – a historical oversight caused by the eastern grid being built on the 50Hz German standard and the western grid on the 60Hz U.S. standard. So the power that was desperately needed in the northern regions could not cross the infrastructure divide in their national power grid (Japan, 2022).

Lessons like this from history, generally caused by standards developing in an ad-hoc manner while technologies evolve, can and should be avoided as far as possible in the context of quantum technologies. The technology itself is so nascent as to give the opportunity of developing core standards across the many nations developing the technology, such that interconnectedness and compatibility is ideally embedded from the ground up before the technology reaches the scale of wide adoption. And this is especially important for quantum communication, where geographic boundaries inevitably play a very significant role.
5.2 The Geopolitics Of Entanglement

One of the more interesting discussions surrounding the goal of a global quantum communication system is how this will influence geopolitics. Discussed extensively in his book, “the Quantum Internet” (Rohde, The quantum internet: The second quantum revolution, 2021), Peter Rohde has pointed to the fundamentally different computational scaling of quantum computers compared with classical computers as a potential driver for drastically different dynamics in which nation states collaborate or compete in a quantum-enabled environment.

Quantum computers differ fundamentally from classical computers in the way that computational power scales with machine size. Classical computational power increases in an additive manner, with two connected classical computers performing, at best, as a single computer of twice the size. Quantum computers, in contrast, compound multiplicatively: So two identical quantum computers, when connected, behave like a single quantum computer with computational power equal to the square of the power of the individual computers. This makes a very significant difference when considering how individuals, groups, corporations, nations or even international alliances will behave when considering if and when to connect their quantum computing infrastructure through a future global quantum communications network. The ability for computational power to be greatly enhanced or greatly diminished by connecting or disconnecting quantum communication links will make these technologies arguably some of the most critical national infrastructure. If the day comes where a national quantum network, consisting of multiple, interconnected quantum computing systems is providing significant computational resources to the economic success of a nation, crippling a single quantum communication link would completely collapse the ability of that computational infrastructure to operate. This potential interplay between quantum computing, quantum networking and geopolitics would then strongly influence how these networks are constructed, deployed, and maintained.

Standardisation may allow for greater interconnectedness between nations that possess the technology, allowing for an exponential increase in computational ability by interconnecting their respective networks. On the other hand, standardisation may also prove to be undesirable for certain actors who do not wish to add to the computational power of another nation. They may therefore wish to ensure their quantum infrastructure is effectively “walled off” from everyone else, simply by making the fundamental technology incompatible from hardware or protocol standpoints.

5.3 The Technology End Game

As with the quantum computing space, it is hard to predict the near- and mid-term future trajectory of quantum communications. The broad narrative surrounding the quantum communications landscape still has its sights set firmly on a future, global, fully functional quantum internet, yet many of the most advanced technology demonstrators still focus exclusively on implementing the much narrower problem of QKD. It can be convincingly argued that the goal of a quantum internet is substantially more technologically difficult to achieve than a large-scale, fault-tolerant quantum computer. However, quantum communication networks, like their classical equivalents, have a complex history and interplay with their computational counterparts.

Classical communication systems evolved over a period of nearly a century before the advent of the modern microprocessor and were dedicated to connecting people, rather than computational devices. The development of the first electronic telegraph systems, the first trans-oceanic communications cables and the invention of the radio all occurred before the advent of the valve-based computer, let alone transistors and microprocessors. Voice communications and primitive coded messages (such as morse code) were the sole application of these technologies, and it wasn’t until the 1950s and 1960s that we saw the emergence of communication systems that were designed to allow for communication between computational systems.
Just like in the classical space, the first applications of quantum communication systems are likely to operate at low data rates and prioritise secure communications. QKD has already matured to the level in which nascent systems are commercially available for purchase, and there are governments investing significant capital to build out dedicated quantum-enabled networks, ostensibly to provide a level of security for heavily encrypted and highly sensitive communications. The evolution of quantum communication networks beyond this initial security-focused application will then, as it was with classical networks, be dependent on the evolution of complementary computational systems. If quantum computers reach the point where there are enough of them to be networked, there will not be the incentive to simultaneously develop the connecting quantum networking systems.

Standardisation in quantum communications will be driven by the need to provide compatibility and interconnectedness between the technology that will utilise a quantum network. If the capital costs and utility of quantum networks are relegated to dedicated, high-cost QKD systems that are only viable for governments, interconnectedness will likely remain a secondary concern, and standardisation less important.

As with quantum computation (Langford & Devitt, 2023), to side-step some of the uncertainty regarding specific timelines and development paths, we instead look forward to the far future to imagine where the quantum communications industry will end up, and consider the implications this may have on its eventual requirements, applications and supporting infrastructure, as well as on the roles that standardisation could play to reach that end point. Specifically, we envisage five different scale scenarios, ranging from quantum-resilient security (only) being provided by classical technologies (no quantum deployment involved) to ubiquitous, global scale deployment of fully quantum-connected quantum computers. Which scenario ends up eventuating will obviously depend on how far as-yet-unknown future technology innovations are able to drive commercial and performance parameters, from infrastructure costs to distributed entanglement fidelity, but also driven in large part by parallel technology developments in quantum computing.

1. **Post-quantum cryptography (PQC)** ( Bernstein & Lange, 2017): The major value proposition of post-quantum cryptography is that it is deployable today. Furthermore, it is compatible with the physical classical communications infrastructure we already have, although it must be noted that broad adoption of post-quantum cryptography will require very significant (and massively expensive) changes to the classical software infrastructure used to mediate the physical key exchange processes. Designed as a possible hedge against the threat of quantum computers, PQC schemes may turn out to be a reliable solution to the vulnerabilities that traditional public key cryptographic schemes exhibit against fully fault-tolerant quantum computing. The key unknown remains their reliance on the assumed difficulty of certain mathematical problems that underpin the new key-exchange protocols, and it is likely that this loophole may never be closed. Despite this, post-quantum cryptographic protocols may yet be a “good enough”, or even “best available” solution to the threat of quantum computing, particularly when considering the R&D, capital, and deployment costs of dedicated QKD networks. Unless QKD networks can solve the problem of providing dedicated keys at reasonably high bandwidth, in an on-demand way to thousands or potentially millions of users around the world, PQC may be the only scalable technique to protect classical data from the threat posed by quantum computing systems. If this is the case, the deployment and use of QKD networks may not find utility among the general public.

2. **Only QKD**: This scenario represents the case where QKD can provide local benefits over post-quantum cryptography (e.g., implementation vulnerabilities are resolved (NSA, n.d.) (NCSC, 2020) or new quantum computing algorithms crack proposed “post-quantum” cryptographic protocols), but where technological restrictions limit the utility of quantum communications networks to low-bandwidth, low-fidelity and limited-range systems. This would effectively relegate quantum communication networks to point-to-point QKD networks or systems that rely on so-called trusted nodes. Trusted-node scenarios involve QKD links...
being used between repeater stations, which then convert quantum to classical information before establishing a new quantum connection to the next repeater. These schemes do secure the information effectively during link transmission, but the trusted node has a security vulnerability if anyone gains access to the node, as they can just copy the information once it is converted to classical. Depending on the infrastructure costs of these systems, they may ultimately provide little utility if post-quantum cryptography does make the need for pure quantum cryptography solutions unnecessary. It is also worth noting that the trusted-node does not in fact provide security from a cryptographic perspective in situations where the users are in control of the entire network, which is limited to a very small subset of cases where networks are internally run by government organisations or large corporate entities.

3. **Trunk lines and quantum data centres:** In this scenario, quantum communication systems become advanced enough to provide high-quality, high-bandwidth entanglement, but the associated infrastructure is so costly and complex that quantum communication links are reserved or only economical for dedicated trunk-line connections between future quantum computing data centres. This would allow for limited distributed quantum computation, feasible only for governments or corporations that have the resources and incentives to build out the infrastructure.

4. **The quantum ARPANET:** In this scenario, quantum communication systems are still complex, capital-intensive systems. But they have the range, rate and fidelity to be able to modest networks. Similar to the first incarnation of the internet (the ARPANET (ARPANET, n.d.)), quantum links using various modalities such as satellite, fibre and sneakernet, could link together quantum computers being operated by governments, companies and universities to increase computational power over modest geographical regions such as cities, municipalities, or even potentially countries. This scenario would require quantum computers to reach a scale similar to classical computers in the 1960s and early 1970s, where they are reasonably ubiquitous, but still expensive, and limited to cloud-based access for the average person. Unique multipath-routing capabilities of quantum networks, powered by teleportation, entanglement swapping and entanglement purification, will necessitate the use of new control software to optimise network entanglement-distribution performance (Leone, 2021)

5. **The entanglement-based economy:** For this scenario, quantum computing hardware would need to be manufactured at an extremely small scale and qubits would have to become as ubiquitous as transistors. Quantum technology would be embedded in all different types of technology, and global entanglement distribution would be occurring at phenomenal rates. The commodification of entanglement, like that of electricity, would require a huge user base, to drive a scenario where this communication resource would connect together both large and small quantum computers in large numbers, as well as dedicated quantum sensing networks. Based on the current theoretical models for systems such as fibre and satellite-based quantum communication systems, it is highly unlikely that these modalities alone could ever service an entanglement-based economy at this scale. New, paradigm-changing ideas and distribution techniques, potentially making a complete break from classically-inspired approaches, would have to be developed as qubit systems evolve, in order to realise this far-future outcome. This is the scenario that could most appropriately be called a real quantum internet.

In a similar way to the possible long-term future of quantum computing, the last two scenarios would require extraordinary, not-easily-predicted technology breakthroughs. The current state of quantum communication systems is focused almost entirely on scenarios 1 and 2, while researchers are quietly optimistic that scenario 3 is possible. Scenarios 4 and 5 will depend heavily on how quantum computing technology evolves.
### 5.3.1 Scales and requirements

The table in Figure 3 summarises some of the practical constraints quantum communication systems would face in each scenario.

**Figure 3: Quantum communications requirements at different deployment scales**

<table>
<thead>
<tr>
<th>Post-Quantum Cryptography (POC)</th>
<th>QKD only</th>
<th>Trunk-line Quantum communications</th>
<th>Quantum ARPANET</th>
<th>Quantum ARPANET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementable today</td>
<td>Possible today</td>
<td>Medium-long term progress required</td>
<td>Long-term progress required</td>
<td>Far-future development only</td>
</tr>
<tr>
<td>As many nodes possible as the classical internet</td>
<td>10s-100s millions of nodes possible</td>
<td>10s – low 1000s of nodes required</td>
<td>1000s – millions of nodes required</td>
<td>Billions of nodes required</td>
</tr>
<tr>
<td>No quantum technology required</td>
<td>Qubit distribution crucial, but error correction not required</td>
<td>Full quantum error correction required</td>
<td>Full quantum error correction required</td>
<td>Full quantum error correction required</td>
</tr>
<tr>
<td>Should enable long-range, high-rate key production</td>
<td>Requires only limited key production range/rate</td>
<td>Very high-rate entanglement sharing required to maintain quantum data centre links</td>
<td>Very high-rate entanglement sharing required, but more local-scale networks will suffer less sharing loss</td>
<td>Extremely high-rate, global, ubiquitous, varied entanglement sharing required</td>
</tr>
<tr>
<td>No qubits required</td>
<td>Simple travelling qubits required, already relatively inexpensive, even accounting for long-distance losses</td>
<td>Cheap entangled qubits required for high data rates</td>
<td>Very cheap, commercially available entangled qubits required for high-data rates and wider deployment</td>
<td>Requires qubit costs/numbers similar to transistor tech available today</td>
</tr>
<tr>
<td>Extant quantum computing not required for implementation</td>
<td>Could be implemented only with quantum measurements and state preparation (no quantum computing)</td>
<td>Mini quantum computers needed on satellites or for repeaters (up to a few 1000 qubits)</td>
<td>Compact quantum computers needed on satellites or for repeaters, with little to no maintenance requirements</td>
<td>Sneakernet model a likely candidate to achieve bandwidths required and flexibility of entanglement distribution: will require high-density, inexpensive and portable quantum hard drives</td>
</tr>
<tr>
<td>Uses existing classical fibre-based or satellite communications networks</td>
<td>Fibre-based networks could utilise a trusted node model (e.g., Beijing-to-Shanghai QKD link)</td>
<td>Requires satellite constellations with on-board quantum computers, or fully quantum fibre-based repeater networks</td>
<td>Requires satellite constellations with on-board quantum computers, or fully quantum fibre-based repeater networks</td>
<td>Radically new entanglement distribution mechanism likely required</td>
</tr>
<tr>
<td>Physical infrastructure exists, but wide-scale adoption requires major overhaul of classical software infrastructure</td>
<td>Physical infrastructure in early-stage development; Network models developed; Uses existing classical software</td>
<td>New, non-existing physical infrastructure required; Error correction may require complex classical data processing</td>
<td>New, non-existing physical infrastructure required; Error correction may require complex classical data processing</td>
<td>Radically new physical and software infrastructure crucial – new technology paradigm</td>
</tr>
<tr>
<td>Post-Quantum Cryptography (PQC)</td>
<td>QKD only</td>
<td>Trunk-line Quantum communications</td>
<td>Quantum ARPANET</td>
<td>Quantum ARPANET</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>----------------------------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>High costs associated with major classical software infrastructure overhaul</td>
<td>Modest costs for quantum communication devices, very high costs to build new communications grid, extremely high cost for high-volume long range systems (incl. satellites launches)</td>
<td>Very high cost required for dedicated links and receiving stations (perhaps incl. satellites), but at low deployment volumes for high-value activities</td>
<td>Simplified (e.g., Starlink like) receivers or cost-effective fibre node quantum receivers will be required to achieve wider deployment volumes</td>
<td>Error-corrected quantum hard drives will have to be cheap for a sneakernet model to be viable, but distribution can potentially run via existing, low-tech transport technology</td>
</tr>
<tr>
<td>Redundant if quantum computing systems never eventuate</td>
<td>Can be implemented independently of progress in quantum computing (though may benefit from crossover tech)</td>
<td>Powerful quantum computing data centres required at nodes to warrant significant infrastructure costs</td>
<td>Only provides benefit if quantum computers reach the scale where locally operated quantum clusters become widespread</td>
<td>Small to medium-scale quantum computing systems become as ubiquitous as current classical computing desktop machines</td>
</tr>
<tr>
<td>Could be broken by classical or quantum computers at any time</td>
<td>With compliant QKD systems and protocols, security is underpinned by laws of quantum physics</td>
<td>Full high-fidelity entanglement distribution can enable provably secure key sharing and information processing</td>
<td>Full high-fidelity entanglement distribution can enable provably secure key sharing and information processing</td>
<td>Fully quantum enabled, but local protocol power may be limited by size and complexity of receivers</td>
</tr>
<tr>
<td>First round of PQC protocols currently being standardised by NIST, creating clear path towards adoption as defacto and then formal standards</td>
<td>Formal standardisation processes already underway, but arguably lagging behind industry requirements</td>
<td>Minimal standardisation underway</td>
<td>Minimal standardisation underway</td>
<td>Minimal standardisation underway</td>
</tr>
<tr>
<td>Formal Specifications and Quality Assurance standards, including detailed attack research (incl. quantum attacks), required: rapid global standardisation efforts crucial and urgent, to build out forthcoming defacto standards</td>
<td>Formal Specifications and Quality Assurance standards urgently required: accelerated international standardisation efforts required, potentially via industry/national bodies</td>
<td>Minimal standardisation yet required</td>
<td>Minimal standardisation yet required</td>
<td>Minimal standardisation yet required</td>
</tr>
</tbody>
</table>

Beyond the development of QKD-only systems (either via quantum satellites or fibre-based quantum networks), quantum networks will parallel the development of quantum computing systems. Fundamentally, the classical internet is a collection of computers. The fibre-optic or microwave transmissions that happen over long distances (through fibre or up to satellites) is mediated by an extensive array of computers acting as routers, signal transducers, error correction machines, encoders and decoders. The same will be true for quantum networks. The evolution of quantum networks will ultimately depend on the evolution of quantum computers themselves. As error correction forms the ultimate foundation for both computation and communications, these devices will either be deployed as computational machines connected to the classical internet or they will be used as error correction devices to facilitate the transmission of quantum information through lossy fibre systems or across dense satellite constellations. In the case of a sneakernet model for quantum networking, the quantum hard drives required are completely identical to a fault-tolerant, error-corrected quantum computer. The only difference
between a device used exclusively for computation and a device needed to form a sneakernet communications network is the ability to package the computer into a cargo container and physically move it, while it is operating.

The challenges of an extensive quantum communications network therefore all those we already detailed in our first report on quantum computing standardisation (Langford & Devitt, 2023). In addition, there are some unique challenges and potential roadblocks to quantum communication platforms that we summarise in the table in Figure 4.

**Figure 4: Roadblocks to quantum communications at different deployment scales**

<table>
<thead>
<tr>
<th>Scale</th>
<th>Key roadblocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellites</td>
<td>Launch costs, Extreme loss rates to ground, integration of small-scale quantum computers on the platform to increase data rates, inter-satellite quantum links, ability to capture entanglement and store it on the ground in long-term quantum memories (error-corrected quantum computers). New interconnections required for certain quantum computing modalities (microwave-to-optical photon transduction)</td>
</tr>
<tr>
<td>Fiber repeaters</td>
<td>Limited single-photon transmission range due to fibre attenuation. Dense repeater stations (mini quantum computers max 21km apart due to 50% loss threshold for fibre at 0.14dB/km (Hasegawa, 2018)), repeater station deployment in hostile locations, low levels of maintenance possible over long distance connections, parallel repeater links to achieve high data rates. Infrastructure intensive deployment for new network links. New interconnections required for certain quantum computing modalities (microwave-to-optical photon transduction)</td>
</tr>
<tr>
<td>Sneakernet</td>
<td>Massive number of qubits required for a dense, sneakernet-based network. Quantum computing systems required to be portable, even while operating. New interconnections required for certain quantum computing modalities (microwave-to-optical photon transduction)</td>
</tr>
</tbody>
</table>

### 5.3.2 Scales and applications

Different quantum communication applications effectively “come online” as the bandwidth and fidelity of the network increase. In the table in Figure 5, we summarise the main communications applications that will be achievable and relevant given the scale of the quantum network that is realised.
As with classical communications, the ability to connect quantum computing systems – whether in the context of trunk-line systems only connecting dedicated quantum data centres, or a more extensive network that can connect together smaller quantum computers at universities or even at the consumer level – will increase the total computational power and utility of these networks. But the fundamental differences between the power scaling of networked quantum and classical computation will have a dramatic effect on the impact that scaling up system sizes will have. The computational incentives to network quantum computers are extensive and will provide more than enough justification to accelerate R&D and deployment of these systems once quantum computing systems reach a scale where they are providing commercial or scientific utility. The possibility of a full-scale quantum internet and what this would mean for the computational capacity of humanity cannot be overstated, but the road ahead will be long and arduous. A large-scale quantum network will be substantially more difficult to achieve than a large-scale quantum computing system and what technologies ultimately underpin this type of network are unlikely to be the technologies we are discussing today.

---

**Figure 5: Relevant quantum communications applications at different deployment**

<table>
<thead>
<tr>
<th>Application area</th>
<th>Relevant protocol</th>
<th>Bandwidth and fidelity requirements</th>
<th>Post-Quantum Crypto</th>
<th>Trunk Lines/Data Centers</th>
<th>Quantum ARPANET</th>
<th>Entanglement Based Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate the cryptographic threat of quantum computers</td>
<td>Quantum resistant classical encryption algorithms</td>
<td>None</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Authentication</td>
<td>Bell violations</td>
<td>200-300 Bell states per authentication token</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Key Exchange</td>
<td>BB84, E91 and variants thereof</td>
<td>Hz to KHz of raw qubit information per user</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Quantum Encryption</td>
<td>Quantum one-time-pads</td>
<td>MHz to GHz of raw qubit information per user</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Green</td>
</tr>
<tr>
<td>Connecting two fault-tolerant quantum computers</td>
<td>Bell-state mediated lattice surgery operations</td>
<td>MHz of raw qubit information, per user, per logical gate operation</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Multi-user quantum network</td>
<td>Creation of logically encoded graph states for distributed algorithms</td>
<td>GHz of raw qubit information, per user, per logical gate operation</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Server/client blind quantum computation</td>
<td>Large-scale quantum server farm, servicing numerous inbound connections</td>
<td>THz of raw qubit information, per server, per logical gate operation</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
</tr>
<tr>
<td>A global quantum internet</td>
<td>Massive interconnected quantum network</td>
<td>PHz or more of entanglement distributed to numerous end nodes around the world.</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Green</td>
</tr>
</tbody>
</table>

(Green = likely relevant; Yellow = possibly relevant; Red = unlikely relevant)
6. The role of Standards in Quantum Communication

One of the main goals of this report is to discuss the role that standards and standardisation can play in the future development of quantum communications systems and networks. Like quantum computing, the field of quantum communications is growing and changing very rapidly, as it transitions more and more into the commercial domain. In the specific case of QKD systems, this transition is already significantly more advanced than in other second-generation quantum technologies. In the next section, we discuss three case studies which highlight how urgent the need for formal adoption of detailed standards is already becoming in certain parts of quantum communications industry. We then provide a summary of existing standardisation activities within each of the five end-game scale scenarios introduced in Section 5 above.

In Section 6.3, we discuss the needs and opportunities for developing quantum communications standards in the context of each end game (Section 6.3), and identify areas where standardisation can best contribute now. Due to the close dependence that far-future quantum communications technologies will have on parallel outcomes in quantum computing, many considerations for quantum communications standardisation at more advanced scales map across directly from those relevant to quantum computing. Finally, we consider what specific contributions standardisation can make within each of five spheres of stakeholder engagement for the quantum communications industry (Section 6.4) (Langford & Devitt, 2023).

As an overview to the more detailed discussion, we summarise the most important points from Sections 6.3 and 6.4 on the needs and opportunities for quantum communications standardisation in the table in Figure 6 below.


Figure 6: Needs and opportunities for standardisation in quantum communications: Key points

1. Engaging within the community
   - Different hardware modalities for quantum communications networks make standardisation difficult, but arguably even more necessary, especially for ensuring the interface compatibility which is so crucial to networking environments.
   - Standardisation will improve communication and compatibility between different technology platforms and layers.
   - Post-quantum cryptography will require detailed standardisation to allow the major transition away from existing quantum-hackable cryptography to proceed smoothly.
   - Information-theoretic security offered by QKD networks could be classified across tiers according to architecture and protocol robustness, and vulnerability mitigation. Standardisation of hardware modalities may be required for large-scale networks.
   - Networking relying on any “quantum-safe” cryptography will require detailed protocol standardisation to certify genuine benefit and compliance to best practice.
   - Entanglement-distribution-based networks inherit standardisation requirements from both QKD networks and data-centre/HPC-cluster scale quantum computers, while facing additional new requirements to achieve more extensive interfacing.
   - While the benefits of a fully quantum-enabled entanglement-based economy would be wide and profound, the technical challenge would be at least equally so, and most standardisation activities would currently be meaninglessly speculative.
   - As with quantum computing, focussed initiatives by governments, broad industry consortia or key players are proving most agile at starting to develop standards.
## 2. Engaging with suppliers

- Quantum communications technologies demand key aspects of performance from supporting technologies far surpassing what they were originally developed for.
- Developing **Requirements Specifications** for supporting equipment will provide near-term benefits from formal standards development for scaling up quantum networks.
- If QKD networks are to be deployed at scale, this offers new economic opportunities for enabling technology manufacturers willing to engage with new requirements.

## 3. Engaging with end users

- Establishing rigorous implementation and quality assurance standards will provide important increased confidence for early adopters of PQC and QKD-only networks.
- New algorithms and use cases for quantum computing and distributed quantum information processing could strongly influence its reach across sectors, and the technology scales it could be usefully deployed at.
- Developing them requires highly interdisciplinary collaboration with end users.
- Significant innovation is required to understand how fully distributed entanglement networks can facilitate new applications for end-user sectors.
- New standards for negotiating network access will change how end users connect individual quantum computers into a larger network to access exponentially improved computational power for distributed and blind quantum computing.

## 4. Educating a quantum workforce

- Innovation is still required, to identify if standardisation can play a substantive role in helping to grow the broader quantum workforce pipeline.
- Detailed **PQC implementation Specifications** can help quantum algorithms experts target their efforts at developing new quantum attacks on new PQC protocols.
- The best opportunity for standardisation is to establish **Terminology and Requirements standards** to help train expert technicians and engineers in supporting areas, especially those required for PQC and QKD-only networks.

## 5. Engaging with the wider community

- In the rapidly developing industry, we are seeing the emergence of so-called "quantum" providers who are not delivering genuine quantum benefits, which risks damaging public and investor confidence.
- Developing robust, objective, widely adopted (and developed), comprehensive and accessible **Quality Assurance standards** to enable due diligence and regulatory oversight will be crucial to maintain end-user, investor and government confidence.
- Good terminology and informative standards could facilitate better communication with external stakeholders, to help build confidence and public licence.

## 6.1 Standardisation Case Studies

### 6.1.1 Case Study 1: Qkd Without The D

What counts as a Quantum Key Distribution platform? At what point, as a commercial vendor, should you be allowed to say I am selling quantum communications technologies? This is a very relevant question today as there is a big expansion, in the start-up space, of nascent companies who claim to be quantum encryption companies, but are arguably not fulfilling the basic properties that motivated the development of quantum communications. This presents an opportunity for the community to develop stronger standards, not only for future compatibility and network compliance, but also for consumer protection and regulatory compliance.

The words in the term, Quantum Key Distribution, provide an apt description of the three core properties critical to genuine QKD platforms. They should: (i) be built from **second-generation quantum technology**, (ii) be designed to produce cryptographic keys, and, arguably most importantly, (iii) **distribute** them between two parties. The core security problem that is solved with QKD is the distribution of shared randomness (the keys) between two parties in a way such that quantum mechanics can verify that this shared randomness isn’t intercepted by an
eavesdropper. By contrast, several new start-ups appearing in the past 3-5 years define QKD or quantum encryption systems in a fundamentally different way. Instead of relying on a quantum communications network to distribute quantum information, generating shared randomness that can be used as a cryptographic key, they instead utilise another quantum device to generate something else.

A Quantum Random Number Generator (QRNG) (QRNG, n.d.) is a quantum device that can produce a bitstring that is completely random through certain physical processes. One way of producing random bits is to fire a single photon into a 50:50 optical beam splitter and then observe (with photon detectors) which output of the beam splitter the photon comes out. If the source, detectors and beam splitter work correctly, the photon will be detected at each output of the beam splitter with a probability of exactly 50% (Ma X., 2016).

The value proposition of some “Quantum key distribution” companies is to use these devices – which can be purchased as integrated computational modules from companies such as Swiss-based ID Quantique or Australian-based Quintessence labs – to produce random bit strings of classical data. They will distribute this data over the classical internet to two users using a complex protocol stack. Once these random bit strings are received by the users, they can be utilised as keys to perform further encryption on their sensitive data.

The issue with these offerings is that they do not actually do the fundamental thing QKD systems were invented for: QKD systems use quantum mechanics to solve the distribution problem, whereas keys distributed in the way described above are no more secure than the classical protocols used to distribute what is an entirely classical bit string. The randomness of how keys are produced for cryptography can certainly be a problem – an insufficient source of randomness can be an attack vector on cryptographic protocols – but this was already a known problem, suitably solved by using appropriately designed classical pseudo-random number generators. While QRNGs can indeed be used as part of a correctly implemented QKD protocol, this is a sideshow to the actual QKD platform and protocol. It is not even just that this does not deliver the entire QKD protocol: it does not deliver the crucial technologies that are central to a QKD protocol.

Marketing these “solutions” as being related to true QKD networks is an attempt to leverage the reputation of quantum to offer distribution solutions that are not guaranteed by quantum at all. This creates due diligence risks for investors and consumers who are trying to navigate the rough waters of an emerging new technology, as well as reputational risks for quantum communication technologies more broadly. Broad adoption and recognition of formal Terminology Standards for definitions, and Requirements Specifications for QKD platforms, along with any Measurement and Test Methods needed for compliance testing and certification, for known, and validated, QKD protocols will be crucial to mitigating these risks. Existing activities on standardisation must continue to be developed apace to create formal Specifications with sufficient detail for formal compliance processes, and existing efforts must be recognised by and built into appropriate government regulatory frameworks to start enabling QKD technologies to be supported by standard consumer and investor protection processes. As is the case for quantum computing (Langford & Devitt, 2023), it is vital to ensure that these standardisation activities are driven in close collaboration between both quantum experts and experts in standardisation, and overarching strategic direction is required to ensure efforts are best focussed on areas of urgent need to the emerging quantum communications industry and to the broader community of government, investors and the general public. Correctly implemented, these activities will also provide significant added value to the emerging quantum communications companies that are aiming to develop true quantum solutions to key distribution, by providing both a competitive advantage for them when seeking capital investment, and concrete target benchmarks to guide their technology development.
6.1.2 Case Study 2: Quantum Hackers

In the early 2000s, Vadim Makarov, a colourful Russian researcher based in Norway, started publishing results that, at one workshop attended by one of the authors of this report (Makarov, 2010), literally had quantum communications experts laughing aloud from both surprise and dread. This researcher and his group had built an experimental device, contained in a guitar case (Fig. 7), that could be connected to an optical fibre system being used to distribute quantum information to create keys, and successfully be able to “hack” this system. He had done what QKD said was not possible: fully compromise the keys established in a QKD system by only having access to the fibre channel used to distribute photons.

While Makarov and his group – known as the Quantum Hacking group – were eliciting a lot of nervous giggles when demonstrating his hacking device, what he made clear was that he was not claiming to have found a fundamental flaw in quantum theory that was allowing him to compromise the keys established by the QKD system (in his case, the work was published by attacking the fibre QKD network established at the Centre for Quantum Technology at the National University of Singapore in 2011 (Lydersen, 2011)). What his group was doing was exploiting the physics of how photon detectors worked. They had discovered that they could construct an optical device that could “blind” certain photon detectors used on the Bob side of a QKD network, by exploiting this physics. Instead of attacking the fundamentals of quantum key distribution or quantum mechanics, he was attacking the technological components of the QKD implementation (a side-channel attack).

![Figure 7: The QKD hacking kit that compromised a test QKD system deployed in Singapore in 2011. Image courtesy of the Quantum Hacking lab. 2009 Vadim Makarov.](http://www.vad1.com/lab/)

Since that time, the quantum hacking lab has continued to produce multiple results per year (Gerhardt, 2011) (Huang, Laser-damage attack against optical attenuators in quantum key distribution, 2020) (Huang, Laser-seeding attack in quantum key distribution, 2019), all focused on the same basic theme of attacking quantum communication protocols through flaws in the devices used to build these rudimentary networks. Perhaps regrettably, few other researchers have yet followed in their footsteps.
As we are now seeing the emergence of corporations and new start-ups dedicated to developing and deploying rudimentary quantum communications and QKD systems, the processes underway to establish rigorous Quality Assurance standards frameworks (from System Architecture standards defining protocols and implementations, to Measurement and Test Methods for compliance) that are needed to benchmark and certify these systems have become more urgent. And it is crucial that QKD hacking developments are actively incorporated into these processes to ensure the most rigorous underpinning technology for QKD. Even for companies honestly developing the hardware for QKD platforms, it is largely unknown what vulnerabilities particular implementations have. Are they built from off-the-shelf devices that may have flaws that can be exploited? Or are they using more custom hardware where it is not even necessarily known how they work internally? With many of these systems beginning to be deployed in sensitive environments, this will only continue to get more and more critical in the next few years.

6.1.3 Case Study 3: Post-Quantum Cryptography

Post-Quantum Cryptography is often included into the catalogue of second-generation quantum technology, but it should not be classified alongside technologies such as quantum computers, sensors or communications systems. Post-quantum cryptography is not a quantum technology, it is a response to a potential threat of quantum technology.

When Shor released his algorithm for factoring in 1994, researchers found that the general technique utilised by Shor could be utilised to attack a large class of public key cryptographic systems. The factoring-based cryptosystems, such as RSA were not the only ones that were susceptible to attack by a quantum computer. QKD systems offered one potential solution to the problem of the existence of a quantum computer, while another was to find new cryptographic protocols that were not vulnerable to attack by a quantum computer. This is the field of post-quantum cryptography.

It has been identified as a viable alternative to QKD as it does not rely on the development of new hardware technology. Indeed, there are strong motivations to prefer post-quantum crypto over QKD. Post-quantum crypto schemes can be utilised today on standard classical computers and communication networks, hence the cost of re-factoring fundamental encryption schemes that sit at the foundation of nearly everything we do over the internet would be significantly lower.

The problem is that post-quantum crypto schemes ultimately rely on the same underlying assumption as protocols that are now susceptible to quantum attack, namely that they base their security on the assumed difficulty of certain mathematical problems. Just as schemes such as RSA were based upon the assumed difficulty of factoring large numbers into their prime composites, post-quantum crypto schemes rely on other mathematical problems that have not yet been compromised by quantum algorithms.

The post-quantum cryptography field has accelerated rapidly in the past 10 years. We have seen executive orders issued by the Biden administration mandating that all government agencies start transitioning all their infrastructure to quantum resilient cryptographic protocols within the next several years (Biden, 2022). The National Institutes of Standards and Technology in the US (NIST) have recently moved to the final stages of certifying a new suite of protocols to replace both public key encryption standards and digital signature standards for US, and likely global, adoption (NIST ITL, 2022).

The major criticism to this approach is that there is no guarantee that new standards for post-quantum encryption schemes won’t be broken tomorrow. As quantum algorithms researchers have discovered who are trying to develop new beyond-classical algorithms for quantum computing, it is much more difficult to prove that computational tasks cannot be solved, than to
show that they can. We have already seen CRYSTALS-KYBER, the “public-key encapsulation mechanism” candidate which NIST chose in 2022 to begin drafting as a formal standard (to be released as a final standard in 2024) (NIST ITL, 2022) has recently been subjected to what is known as a “side-channel attack” (Ji, Wang, Ngo, & Dubrova, 2023). This is not an attack on the core mathematical problem that underpins the algorithm, but instead focuses on a hardware-based implementation vulnerability. Another promising candidate selected to proceed to another round of evaluation, the SIKE algorithm, was broken, by a classical computer, over the course of a weekend (Castryck & Decru, 2022).

The post-quantum cryptography community has recruited a significant talent base from the crypto community to develop these new protocols. However, they have not yet been studied extensively by the best quantum algorithms researchers in the world. Most of the researchers – and there aren’t that many – who would be considered world leaders in quantum algorithm development have been largely spending their time focusing on quantum algorithms related to chemistry, material science and other domains that corporations developing quantum computing hardware identity as having significant commercial value for their computers. It is still not clear what the outcome will be if there becomes a sufficient commercial advantage for these experts to refocus their attention on these new cryptographic protocols.

The standardisation process of post-quantum crypto algorithms is now already rather advanced. The main part of this work has been led by NIST in the US (NIST-PQC, n.d.), but parallel activities have also begun through ETSI (ETSI-QSC, n.d.), the ISO/IEC JTC 1 (JTC 1/SC27-PQC), the Internet Engineering Task Force (IETF) (IETF-QIRG, n.d.) and others. It is unclear if other nations around the world will be issuing mandates soon to migrate all digital systems to these new cryptographic standards, but the examples above highlight the need for rapid progress in both formal and informal standardisation processes to advance both the assessment and stress testing of these new cryptographic protocols. In particular, the greater agility offered by informal standards development in the initial stages, may provide valuable benefits for the speed of development, especially if guided by reputable, but more local, national or industry bodies.

6.2 An overview of current standardisation activities in quantum communications

In this section, we start by discussing how the context of quantum communications standardisation is closely connected to the parallel context of standardisation for quantum computing. We then provide a brief overview of what standardisation activities already exist in the context of each of the end-game networking scales we introduced in Section 5.

6.2.1 The broader context of quantum communications and quantum computing

As is the case for quantum computing, quantum communications standardisation is not yet keeping up with the rapid-pace evolution of the quantum industry, even though it has already been under development in some contexts (namely, QKD) for more than 10 years, much longer than similar activities in quantum computing. Furthermore, quantum communications face an interesting juxtaposition. In its earliest incarnation of QKD-only communications, we are already seeing commercial deployment of simple QKD systems, and there is an urgent need for broad adoption of concrete architecture, validation and benchmarking standards. Yet the big commercial value for quantum communications ultimately lies in the applications enabled by a fully quantum-enabled entanglement-distribution network, and the quantum information processing capacity that offers (Rohde, The quantum internet: The second quantum revolution, 2021). And as we have already emphasised, this scale of technology is necessarily much harder to realise even than building a scalable quantum computer, since it presupposes that multiple or even many operationally compatible quantum computing machines are available to be
networked in the first place. And given how much fundamental uncertainty exists about the future trajectory and ultimate destination for quantum computing technologies, this creates even greater uncertainty about potential future requirements for eventual entanglement-distribution networks.

In our report on standardisation in quantum computing, we discussed that one of the main challenges we currently face in that area is that formal international standards development processes are only able to ramp up very slowly, and that the most agile standards development is currently being driven by national and regional standards bodies, like the European CEN-CENELEC and US-based Quantum Economic Development Consortium (QED-C). We have also seen this play out in quantum communications, e.g., in the leading roles played by the European Telecommunications Standards Institute (ETSI) and the US National Institute for Standards and Technology (NIST). There has recently been significant ramp-up of activity from the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), and advanced standards are now also imminent from the ISO/IEC JTC 1. Yet this leads to new challenges, particularly in relation to broader strategic considerations, with ongoing activities fragmented across multiple large-scale standards bodies forming a complicated Venn diagram of contributing nations. One positive step towards more strategic coordination was taken by the IEC in establishing the Standardization Evaluation Group (SEG) 14 on Quantum Technology, which is tasked with investigating technical capabilities and the need for standardisation in quantum technologies and has now been asked to deliver its final recommendations to the IEC Strategic Management Board in October 2023.

Because existing standards structures, like the way topics are divided up into different subcommittees and groups, have arisen out of classical and first-generation quantum technologies, there is currently no natural home for quantum technology standardisation to be managed in a coordinated fashion. This results in proliferation, replication and misalignment of standardisation efforts, which in turn overextends the capacity of the quantum experts needed to drive these efforts, given the rapidly expanding industry is already struggling to fulfill its own growing workforce requirements. It also results in key strategic decisions about quantum standardisation activities being made in higher-level committees of NSBs and SDOs where the domain expertise of the delegates involved mainly sits outside quantum technologies. While these delegates are usually able to seek domain-specific advice from local quantum experts to inform their positions, they do not always do so, and they are certainly not able to actively consult on topics when they are under discussion during the meetings.

We have argued strongly here that the development of fully quantum-enabled communications networks is intimately tied to that of quantum computing. It is therefore also vitally important that standardisation activities in these areas should be closely coordinated. To this end, it makes much more sense to maintain complementary quantum technology standards efforts under the one roof and to then coordinate between different SDOs and committees when needing to ensure compatibility between quantum technologies and their supporting classical infrastructure, than trying to do this the other way around. We therefore believe that the growing momentum towards establishing a single unified home for quantum technology applications, including both quantum communications and quantum computing, and ideally also second-generation quantum sensing technologies, will deliver very positive benefits for quantum standardisation and quantum technologies overall, and also for the role of quantum technologies in the wider community.

### 6.2.2 Post-quantum cryptography

To date, the main lead on PQC-related standards has been taken by the regional standards bodies ETSI (Europe) (ETSI-QSC, n.d.) and NIST (US) (NIST-PQC, n.d.):

- In 2015, ETSI assembled a team of relevant experts to publish an introductory white paper on “Quantum Safe Cryptography and Security” (ETSI-WP8, 2015) for the wider...
Information and Communication Technology community. This report notes that data security professionals have been trained to exclusively use standards-based cryptography, and that updated standards, while sometimes a slow process, would be critical for an orderly transition to new supposed (if not proven) quantum-resilient cryptographic protocols.

- In 2016, NIST then commenced a public, “competition-like” process “to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms”, and do so by enlisting help from the global classical cryptography community. After first establishing minimum acceptability requirements and evaluation criteria, in Dec 2016, they published a first call for nominations for candidate algorithms. In 2022, at the end of a third round of evaluation (NIST ITL, 2022), NIST announced they will proceed to draft standards for four different protocols and chose a further four to proceed to further evaluation. The first round of final standards are due to be released in 2024 to augment their existing formal public-key cryptography standards.

- Following the recommendations in this white paper, the ETSI Quantum-Safe Cryptography (QSC) working group published several informative reports in 2016 and 2017 exploring different aspects of quantum-safe algorithms and the quantum computing threat. Its parent ETSI Technical Committee CYBER has since then published a series Technical Reports on various aspects of PQC adoption, as well as a normative Technical Specification aiming to help speed up the incorporation of PQC candidates eventually chosen by the NIST PQC standardisation process (ETSI-CYBER-TS, 2020).

6.2.3 QKD-only networks

Standardisation activities are much more advanced in the context of QKD-only communications than they are in other second-generation quantum technologies (QIT4N-D2.5, 2021). Telecommunications focussed standards bodies like the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), have published a range of both normative (requirements specifying) and informative standards:

- Most QKD standardisation activity in ITU-T, which started relatively recently (roughly the last 5 years), is taking place within ITU-T Study Groups 13 (Future Networks) and 17 (Security). To date, this work is mainly delivering quite high-level Requirements specifications and overviews on various aspects of QKD networks from the quantum layer to architectures and quality of service assurance (SG13) and various security considerations from quantum random number generators to (under development) trusted nodes (SG17).


- The ETSI QKD Industry Specifications Group (ISG) (ETSI-QKD, n.d.), established to support quantum cryptographic networks, has been operating longer and has (since 2010) published more detailed standards ranging from use cases and vocabulary to security proofs, component characterisation and QKD module security specification.

- QKD standardisation has also now reached the point of full international Requirements Specifications standards being under development. The JTC 1 Subcommittee (SC) 27 has now progressed two companion Specifications covering security Requirements and Test and evaluation methods for QKD to Draft International Standard stage [DIS 23837-1 and DIS 23837-2] (JTC 1 /SC27-DIS, 2022). Once published, these will provide the first detailed Quality Assurance standards to provide formal security benchmarking and compliance for current and future commercial QKD systems.
6.2.4 Trunk-line-connected data centres and quantum ARPANET

Currently, standardisation activities in the realm of full quantum-enabled entanglement-distribution networks are very limited:

- The ITU-T FG-QIT4N (JTC 1/SC27-PQC) was tasked with looking at broader “Network aspects of quantum information technologies” as well as “QKD Networks”, publishing three reports: (D1.1) collecting together in-progress terminology definitions from other quantum standardisation activities (including an early version of those being prepared by the ISO/IEC JTC 1 WG14 that the authors of this report are members of); (D1.2) an initial survey of use cases; and (D1.4) a brief report on standards, which mostly collates information from other reports, but provides a useful snapshot existing standardisation activities, as well as recommending caution is undertaking standardisation activities, and supporting the creation of Standardisation Readiness Levels for assessing when to begin standardisation activities.

- The Quantum Internet Research Group of the Internet Engineering Task Force (IETF) are also in the process of drafting initial reports on use cases and architectural principles of a quantum internet. At this stage, a lot of this is guesswork, since the use cases for distributed quantum computing applications are even less well explored than standard quantum algorithms research, and there is immense uncertainty about the physical hardware architectures that will ultimately be required to drive either quantum computing or quantum communications networks to the scales and performance involved in these scenarios.

6.2.5 The entanglement-based economy

There is good reason to suppose that none of the existing conventional communications hardware modalities (e.g., fibre and satellite networks) will be adequate for providing the entanglement-distribution backbone of a full quantum internet scenario. As a result, there has really been no existing standards development yet relevant to this scale.

6.3 Needs and opportunities for standardisation in quantum communications at different scales

In this section, we consider each of the different scale scenarios identified in Section 5 and discuss potential needs and opportunities for standardisation in each of these scenarios to contribute the development of the new quantum communications ecosystem. As in our report on quantum computing standardisation (Langford & Devitt, 2023), we do not focus on how (or how fast) quantum standardisation may develop moving forward, but instead skip forward to the imagined communications networking end game, and ask what standardisation might be required to support the industry at that scale. As relevant, we then also discuss where the best opportunities may lie in the short term, or in some cases, for urgent consideration now. The key points from this discussion are incorporated in the table in Figure 6 above.

6.3.1 Post-quantum cryptography

The need: There are two very significant challenges facing the deployment of post-quantum cryptographic algorithms that good standardisation processes will be crucial to address:

- Ensuring they are secure against quantum and classical attacks—As outlined in Case Study 3, proposed PQC protocols may be subject to both algorithmic and implementation vulnerabilities. They are already being actively explored for classical attack vulnerabilities, but still rely on the presumed complexity of their underlying mathematical task against quantum attack. This is yet to receive significant attention from the world’s top quantum algorithms researchers.
• Rolling out the implementation—The classical software infrastructure that implements secure connection protocols penetrates almost every communication and computing device our society deploys, from computers and smartphones, to remote sensors, environmental monitors, smart appliances and devices across the Internet of Things. While post-quantum cryptography can use the standard physical infrastructure of classical telecommunications, rolling out broad adoption of PQC protocols will be an immense undertaking, requiring a significant overhaul of secure communications software infrastructure deployed across the whole communications ecosystem.

The opportunities: There are significant opportunities for standardisation to help address the above challenges to upgrading to quantum-resilient secure communications are:

• Security—Detailed, actively maintained implementation standards for any PQC protocols being adopted will be required for identifying, and where possible addressing, both quantum and classical attack vulnerabilities. This, along with explanatory, non-normative Technical Reports to accompany the implementation standards, will especially help quantum algorithms experts engage with the field and focus their research on the most directly relevant areas.

• Implementation—Establishing and maintaining strict, open, internationally adopted quantum-resilient communication standards will be crucial for broad deployment of PQC protocols, especially for use in high-sensitivity contexts. These processes are already well underway, led primarily by NIST (NIST-PQC, n.d.) and ETSI (ETSI-QSC, n.d.), but significant international cooperation and action will be required to ensure that these regional standardisation efforts keep pace with industry developments and are globally adopted.

• Adaptability—Given the potential uncertainty that exists for any secure communications protocol relying assumed mathematical complexity (as opposed to the possibility of provable security offered by QKD), especially as quantum algorithms research progresses, it would also be extremely beneficial, if possible, to develop System Architecture standards that could streamline the roll-out of protocol changes that may be required in the future.

The short term: Arguably the most important open question in post-quantum cryptography is whether the proposed PQC protocols are vulnerable to attack by a quantum computer. However, this is very much a research question, and will not be resolved on a well-defined timeline. Standardisation therefore most urgently needs to focus on implementation, by setting up the frameworks to facilitate rapid deployment of the new PQC protocols:

• In parallel with supporting NIST’s ongoing efforts to develop new PQC implementation standards, international efforts need to ensure that these new standards can be formally adopted by international SDOs as rapidly as possible, e.g., streamlined via a Publicly Available Specifications process (Abdelkafi, et al., 2018).

• It will soon become urgent to establish a full suite of Quality Assurance standards, including both Requirements Specifications (implementation) and Measurement and Test Methods (for compliance and certification).

• Comprehensive and rigorous frameworks will need to be established to implement an orderly migration of our existing encryption infrastructure to PQC-powered encryption (e.g., (ETSI-CYBER-TR, 2020)). This will need to include training for professionals in the wider IT security community.

6.3.2 QKD-only networks

The need: The key value proposition offered by QKD is that, unlike conventional classical cryptography protocols like PQC which rely on a presumption of security based on underlying mathematical complexity, the security of a shared key can be verified by the laws of physics. But for QKD to be adopted widely as an alternative to classical cryptographic approaches, it will require a massive roll-out of physical and control-software infrastructure across the
telecommunications network. Currently, there are major open questions about how far this scaling-up process can reach while still relying on existing classical telecommunications networking principles (fibre-based and satellite networks). But however widely QKD technology is deployed, if QKD is going to play any significant role in quantum-safe cryptographic technology, even in the form of metropolitan or regional point-to-point networks, then extensive standardisation will be required across many levels:

- **Ensuring systems are actually quantum**—As outlined in Case Study 1, in a nascent, rapidly changing market like quantum technologies, products can emerge that trade on the reliability of quantum-assured security without actually implementing the underpinning quantum technology that provides that security.

- **Maintaining security against quantum and classical attacks**—As seen in Case Study 2, while correctly implemented QKD offers unconditional algorithmic security, they are still subject to implementation vulnerabilities (ETSI-WP27, 2018) (NSA, n.d.).

- **Rolling out the implementation**—Broad adoption of QKD will require either extensive use of existing classical communications infrastructure, or deployment of a new parallel global communications grid, potentially based on dramatically different technology, like a sneakernet.

**An “exception to the rule”:** It is often stated that it can be risky to develop formal standards too early in the development stages of a new technology or industry, for fear of stifling innovation or locking in monopolies (e.g., ITU-T Q1T4N D1.4 (Q1T4N-D1.4, 2021)). Interestingly, however, the case of QKD provides a counter example to this, where it is possible to start developing full Quality Assurance standards, covering aspects from architectures to performance benchmarking, even while industry is still in early development stages. This is because the main value proposition of QKD is that it offers the potential for key distribution technology where the security is underpinned by rigorous principles of quantum physics. This means that Requirements Specifications around both architectures and performance could be defined strictly in relation to physical laws and information theoretic proven security limits, rather than based on more fluid and fungible community agreed performance levels.

**The opportunities:** In the longer term, to realise even a QKD-only network at scale, the key opportunities for standardisation lie in two key areas—security certification and infrastructure implementation:

- **Security**—Depending on the complexity of known attacks/vulnerabilities, and the countermeasures required to circumvent them, some vulnerabilities may be easier to prevent than others. There may even end up being an ongoing consumer market for systems with multiple levels of quantum-assured security, just as different organisations implement different degrees of cyber-security today, depending on the sensitivity of their data and operations. System variations impacting formal QKD security compliance across hardware platforms, protocols, and implementation vulnerabilities, could still be accommodated within rigorous formal Specifications and Requirements standards:
  - **QKD System Architectures** could be categorised via some kind of tiered system. For example, one could define “Tier 1” QKD systems to be those that provide full end-to-end “quantum secure” key distribution and complete classical privacy amplification, including entanglement-powered quantum repeaters which never decode the quantum information, while a QKD network which involves full quantum link distribution, but relies on “trusted repeater” designs where shared bits need to be decoded and then re-distributed, could receive a lower designation.
  - **Requirements Specifications** could maintain a comprehensive list of known QKD vulnerabilities and their appropriate countermeasures, such as decoy-state QKD to mitigate against photon-number-splitting attacks, along a companion Test and
Evaluation Methods to allow systems to receive compliance certifications for the protocols implemented.

– Even at a fundamental level, established entangled-pair distribution fidelity thresholds define various degrees of security “conditionality” and could be specified to define the level of risk tolerance required to utilise a given system.

• Implementation—Infrastructure at such massive scales, crossing continents, oceans, and international borders, always requires extensive rigorous, open standards. This is especially true for achieving full quantum-assured security, which requires genuine quantum information sharing between any network node, since conversion between incompatible local standards could require protocols which would violate no-cloning.

  – Piggy-backing QKD on existing classical telecommunications networks, e.g. (Mao, 2018) would require detailed standards describing strict compatibility Requirements, especially in case of any infrastructure upgrades being required.

  – Running QKD networks parallel to existing classical networks (e.g., using the same fibre cabling) would be technically easier but much more logistically formidable, and would still necessitate strict System Architecture and Requirements standards to prevent interference with ongoing classical communications operations.

  – At larger network scales, standardisation may also be required to resolve the existing competition between hardware modalities, either by facilitating reliable interfacing, or in identifying and standardising an eventual preferred modality.

The short term: Significant QKD standardisation efforts are already underway across multiple international and regional organisations, including ETSI, ITU-T and ISO/IEC. Building on these existing efforts, key short-term opportunities for standardisation in addressing the above challenges associated with deploying and maintaining a global QKD network include:

• Quantum compliance—By providing formal Requirements for implementing QKD systems, the forthcoming ISO/IEC 23837 QKD Specifications (JTC 1 /SC27-DIS, 2022) will be a crucial part of preventing the proliferation of misleading and unreliable products, but not enough on its own. Active engagement with governments and other regulatory bodies will also be required to ensure standards are adopted and broadly applied, so that existing consumer- and investor-protection mechanisms can be leveraged to respond to violations.

• Advocacy—Standards development can continue working to establish broader awareness of QKD, and the problem that it solves, for external stakeholders across the IT security community, governments and data-sensitive industries like defence and public health (e.g., (QIT4N-D2.2, 2021), (ETSI-WP8, 2015)).

• Future focus—in a rapidly developing environment, standards development needs to be forward looking, building Frameworks and high-level Requirements to guide future standardisation in key aspects of QKD, like devices, network protocols, control interfaces, etc.

6.3.3 Trunk-line-connected data centres and quantum ARPANET

The need: At these scales, quantum communications networks incorporate an entire new level of system complexity, with distribution nodes becoming quantum computers in their own right, and large scalable quantum computers to connect to at the end-user nodes. As such, full entanglement-distribution-based networks inherit much or all of the needs and opportunities for standardisation from both QKD-only networks and data-centre/HPC-cluster scale quantum computers (Langford & Devitt, 2023). In addition:

• Interfacing—The need to interface with (potentially one or more types of) quantum computing nodes dramatically increases the complexity of interfacing requirements at these scales, over the comparable requirements of QKD-only repeater nodes. This results in increased
heterogeneity and interoperability that must be accommodated at interfaces across the network: e.g., at nodes connecting different hardware modalities, and between nodes and distribution links.

- Microwave compatibility—Many leading quantum computing hardware platforms rely on cryogenic microwave systems, and would require microwave-to-optical frequency transduction to be compatible with the likely optics-based networking platforms.
- Network routing—Entanglement-distribution networks will only achieve optimal performance by exploiting quantum features such as entanglement purification that do not exist in classical telecommunications networks (Leone, 2021).

The main difference for standardisation between these two scenarios would be in how they would need to be managed:

- For trunk-line-connected data centres, it may still be possible to manage the additional specific networking complexities via internal standardisation processes, or at a more local level (whether that be government- or corporate-level).
- For the quantum ARPANET scale, however, broader standardisation processes would be required.

We argue it will not be possible to realise this technology scale (or beyond) without quantum technology standards being managed in a closely strategically coordinated fashion, by some kind of dedicated international quantum standardisation organisation.

The opportunities: As we have discussed, realising a full entanglement-enabled quantum communications network will be even more complex than building data-centre/HPC-cluster scale quantum computers. In addition to all the existing standardisation required on the path towards QKD-only networks, networks at this new scale will provide new opportunities for standards, especially in interfacing and network routing:

- Interfacing—At a hardware level, detailed interfacing Specifications will be required for all elements of the network. This will also likely have a flow-on impact onto software control frameworks.
- Network routing—Unique quantum features of entanglement routing, will require new software-level network routing control standards to optimise network performance.

The short term: Any attempt to identify standardisation activities specific to these network scales, for example, beyond the opportunities already identified for QKD-only networks, must necessarily be regarded as very speculative:

- Entanglement resources—Probably the most important opportunity in this context for the near term is to undertake a detailed scoping analysis of what kind and amount of resources would really be required to enable practical distributed quantum computing to tackle some meaningful test-case scenarios, even if initially as simple as an updated implementation of Shor’s factoring algorithm across two networked quantum computers (Van Meter, Architecture of a Quantum Multicomputer Optimized for Shor’s Factoring Algorithm, 2006).
- Frameworks—Early standardisation could also take the role of developing general frameworks and Practice Guidelines outlining recommendations and possible capabilities for future entanglement-enabled network architectures. In a hypothetical far future of networked quantum computing nodes, however, such standards would like need to evolve into strict Requirements standards.
6.3.4 The entanglement-based economy

The need and opportunities: While its potential benefits are hard to overestimate, this scenario will require radically new hardware, distribution, designs, and infrastructure, subsuming the requirements for virtually all other end-game scenarios for both quantum communications and quantum computing. It will require such a radical shift in technology that it is impossible to say at this stage exactly where additional roles will arise for standardisation, other than just “everywhere”. What is clear, however, is that rolling out full networked quantum information processing infrastructure at this scale will require rigorous architecture, hardware and performance standardisation to a degree that far surpasses anything that has yet been realised or will be required for any type of quantum technology currently being considered, at any time to date or into the future. Indeed, the scale and breadth of standardisation required to realise this end-game scenario would by that time necessarily be on par with the current scale of information technology standardisation managed by SDOs and regional standards bodies like the ISO/IEC JTC 1, IEEE, CEN-CENELEC and ETSI.

The short term: It is likewise very difficult to speculate what standardisation activities might be useful now, to help facilitate a technology so far into the future. One rather speculative activity could be to consider different scales of an entanglement-based economy (e.g., where distributed entanglement is a resource readily available to individuals, or a controlled resource reserved for corporate or government use), and estimate the total amount of shared entanglement required to supply global levels of computation activity within that scale. The numbers are likely to be obscenely large, but they could still be informative.

6.4 Needs and opportunities for standardisation in quantum communications across different spheres of engagement

In our report on quantum computing standardisation, we argued that the fundamental goal of standardisation is to streamline interactions between disparate groups of society. We therefore introduced five spheres of engagement for the new quantum industry, and motivations and opportunities for quantum standards development within each sphere. Here, we discuss how quantum communications standardisation activities might vary across each of these spheres. Key points from this and the previous section are combined in the table in Figure 6 above.

6.4.1 Engaging within the community

Like quantum computing, the field of quantum communications is rather multidisciplinary, even at the PQC and QKD-only scales, and this can create significant challenges to communication across discipline boundaries. To develop these technologies, deep expertise is required across telecommunications engineering, quantum optics, classical cryptography, quantum algorithms, and more. Here, we define “within the community” to mean anyone within the different communities that would need to be actively collaborating to build these networks (as opposed to suppliers who might be selling products that will eventually be incorporated into the networks). While existing QKD-only technological platforms arguably share more commonality than current quantum computing platforms, the interconnected nature of networking infrastructure makes compatibility and interoperability, and perhaps even outright uniformity, even more critical. And this interdisciplinarity only becomes more pronounced when moving into the realm of full entanglement-distribution connected quantum information processing networks.

In an environment characterised by diverse, competing hardware platforms, cross-disciplinary dependencies and an uncertain endpoint, while standardisation is arguably more difficult, it also offers valuable opportunities to bridge the inevitable communication gaps:
• **Terminology standards** and companion, non-normative (non-requirements specifying) explanatory Technical Reports could help improve cross-disciplinary communication within the community.

• Accessible yet expert-driven, purely informative Technical Reports could be used to shed more light on potential development trajectories and key challenges.

• Communications networks, at whatever scale, will also inevitably involve interfacing potentially disparate technologies to connect different parts of the network, such as between quantum distribution links and quantum repeaters or computers housed within the nodes. Solving these challenges will require extensive collaboration between both quantum technology and telecommunications experts. Detailed System Architecture and Requirements Specifications will be crucial for ensuring that technological advancement and market competitors are able to maintain compatibility with existing grid infrastructure, which will in turn also benefit competition and affordability. Appropriate Measurement and Test Methods and certification protocols will of course be required ensure formal compliance with existing standards.

With NIST nearing the point of releasing the first formal standards from its eight-year Post-Quantum Cryptography Standardization process (NIST ITL, 2022), and the new formal QKD Specifications to be released by ISO/IEC (JTC1/SC27-DIS, 2022), the quantum communications industry is now nearing an potentially interesting turning point. It is not unreasonable to imagine that we might soon start seeing changing scales for commercial deployment of these first two scales of quantum communications-related technologies. The challenge for standards development will be to try and keep pace with the changes to come. The early progress in standardisation achieved by ETSI and NIST (at post-quantum cryptography and QKD-only networks scales) highlights the benefits of greater agility that regional standards bodies can bring to formal standards development processes when they take leadership in a new area, by lowering the barriers to effective and easy collaboration, and being able to better leverage established local networks of experts.

6.4.2 Engaging with suppliers

Over the last 20 years or so, developments in QKD have illustrated clearly how quantum technologies often place far more stringent requirements on hardware performance than the classical technologies that hardware was originally developed for. Where a classical telecommunications engineer would not bat an eyelid about 3dB (50%) of loss (just put in some more amplification), that already hits a threshold where some quantum communications networks can no longer function. Similarly, completely new detector technologies designed to minimise detection losses at visible and telecoms wavelengths played a crucial role in loophole-free implementations of the Bell experiments which are at the heart of quantum-assured security in entanglement-based QKD systems. Yet quantum communications networks will need to solve many challenges like these to reach the scales envisioned. This offers significant new economic opportunities for enabling technology manufacturers willing to engage with new requirements, and standardisation can help streamline this process. Without quantum-targeted specifications standards, this auxiliary technology development requires time-consuming industry engagement with classical technology providers whose attention (and production lines) is meanwhile focussed on their established large-volume classical clientele.

6.4.3 Engaging with end users

In the larger scale scenarios, which involve full entanglement-powered network-level quantum processing, end-user applications align strongly with the diverse sectors where quantum computing is predicted to have an impact. In our report on standardisation in quantum computing, we already discuss how standardisation can make a contribution in this context (see key points in Fig. 6) (Langford & Devitt, 2023). As discussed earlier, however, networked
quantum computers show a fundamentally different scaling of computational power (exponential) compared with classical computers (linear). This could have significant implications for end users who are able to connect their quantum computers into a larger network, e.g., for applications in distributed or blind quantum computing. This could be particularly pronounced at trunk-line-connected data centre & quantum ARPANET scales, where computational nodes will require high investment and not yet be ubiquitously available. Standardisation could have an important role to play in established processes that allow users to compound their individual resources for mutual benefit.

At the earlier scale scenarios of post-quantum cryptography and QKD-only networks, end users could include anyone engaging in electronically secure transactions, with the main initial stakeholders likely to come from governments, intelligence organisations, providers in data-sensitive industries and large corporations who may need to protect commercially sensitive information. For these end users, the main point of concern is likely to be trust and confidence in the technology. While quantum-resilient encryption can always be layered on top of conventional encryption protocols, such that migration doesn’t risk a loss in security, early movers will likely incur higher costs. As discussed already, standardisation will play an important role in establishing rigorous Quality Assurance processes and even Procurement standards for the new technologies, and will help provide customers the confidence needed to make the initial investment. Case Study 1 highlights how urgent it is for rigorous compliance processes to be developed and formally adopted, including by governments and consumer/commercial regulatory bodies.

6.4.4 Educating a quantum workforce

Due to the steep challenge involved with building a full entanglement-powered quantum communications networks, most of the current effort towards this end is targeted at developing either QKD-only networks or scalable quantum computers. While research currently taking place in the full quantum network domain is still rather early stage, rolling out and maintaining such a network will eventually require highly trained professional across a broad range of supporting or enabling areas, such as: telecommunications engineers, advanced device fabrication engineers, cryogenic engineers, and network and software engineers. As for quantum computing, standardisation can potentially have a positive impact in this direction: Terminology standards and companion explanatory Technical Reports could help bridge the communication gap, and detailed Requirements Specifications could be used to carefully define the technical aspects relevant to the scope of the supporting technician’s or engineer’s work.

The same approach should also be true for the earlier scale scenarios: For QKD-only networks, rolling out at large scales will require significant new training for network engineers and technicians installing, operating and maintaining the infrastructure. In post-quantum cryptography, standardisation can help address the key near-term challenge of training established professionals in the IT security community to be able to implement the new protocols. In the ETSI white paper on “Quantum Safe Cryptography and Security” (ETSI-WP8, 2015), it is noted that “security practitioners have been trained that, to prevent [problems] from occurring, it is important [...] to use standards based cryptography and protocols to limit the impact of system flaws and oversights.” Establishing detailed implementation Specifications will help guide this process, and could be used to develop standard short courses or technical certifications to provide the required cross-skilling or up-skilling to enable established professionals to roll out the new technology.

Arguably the biggest workforce gap in post-quantum cryptography, however, is in addressing the question of whether PQC protocols are vulnerable to quantum computing attack. The key challenge is that answering this question (or building confidence that the answer is “no”) likely requires the attention of world-leading quantum algorithms experts. But the quantum algorithms
community is rather small and currently all focussed on developing improved applications for quantum computing. This highlights an urgent need to increase the pipeline of quantum computer scientists entering the field of advanced quantum algorithms research, to grow the number of quantum algorithms experts focussing their attention on new quantum algorithms to attack PQC encryption. Ironically, the best opportunity for standardisation to help here is likely in providing detailed implementation Specifications to assist quantum experts better understand the classical encryption protocols.

6.4.5 Engaging with the wider community

If the quantum communications industry reaches one of the larger full quantum networking scales, it is clear that there will be broad impacts for the wider community, even at the trunk-line-connected data centres scale. As already discussed in our report on quantum computing standardisation (Langford & Devitt, 2023), standardisation and associated regulatory frameworks can play an important role in helping to build community, investor and government confidence (public licence) in new quantum technologies, including large-scale quantum communications networks.

But given how constantly we rely on secure communications technologies in vast areas of our day-to-day lives, large-scale deployment of PQC and QKD-only encryption already has the potential for sweeping impacts across the wider community. The saving grace is that quantum-resilient encryption can be layered on top of conventional encryption protocols. Nevertheless, standardisation, for example in the form of detailed Quality Assurance standards for full compliance testing and certification, has a very significant role to play in building government, business and ultimately public confidence in the new technologies.

Detailed Requirements Specifications for QKD systems will also help prevent products flourishing that exploit misleading claims and misunderstandings to attract customers and investors without offering significant benefit. However, as discussed above, standardisation is just one part of the solution. The standards development community also need to work closely with governments and other regulatory bodies to ensure broad adoption and application, so that consumers of quantum technologies can access the same protection mechanisms that are already available for other technologies.
Bibliography


Ma, X. (2016). Quantum random number generation. npj Quantum Information, 2, 16021.


