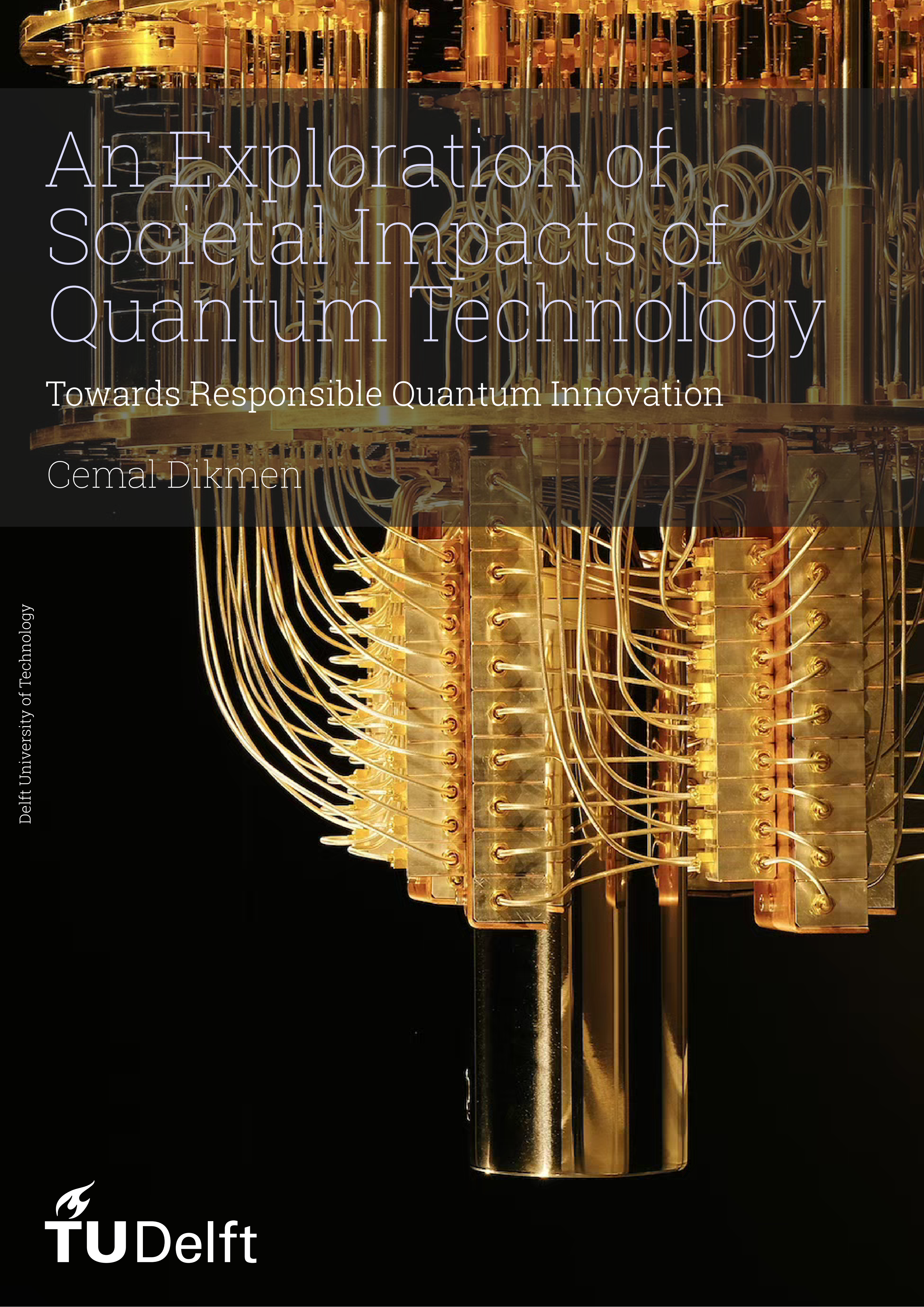


An Exploration of Societal Impacts of Quantum Technology

Towards Responsible Quantum Innovation

Cemal Dikmen

Delft University of Technology

An Exploration of Societal Impacts of Quantum Technology

Towards Responsible Quantum Innovation

by

Cemal Dikmen

Student Number: 4599209

Second Supervisor & Chair:	Prof.dr.mr.ir. N. Doorn
First Supervisor:	Prof.dr. J.R. Ortt
Daily Advisor:	Dr. M.J. Wiarda
Company Supervisor:	R.G. Fransen, Senior Manager
Company Advisor:	B.B. Blok, Senior

Faculty of Technology, Policy and Management

Cover: IBM Quantum Computers and accelerated discovery (Modified)

TUDelft

Preface

All praise and thanks are due to Allah, may His blessings and peace be upon Muhammad, his household and all his Companions. I would like to thank my dear mother for her strong support and guidance throughout my life.

I want to use this section to retrospect on the process of designing and conducting research and writing this master thesis. This thesis trajectory was a complex endeavour with many ups and downs. With the guidance of my supervisors, I learned and discovered a lot about the art of research. The professionalism, strong character and critical view of my second supervisor and chair, Neelke, has provided me with valuable lessons during the entire project. You guided all the formal meetings with care, and have given me the right toolset to conduct this research. Thank you. The eagerness and enthusiasm of my first supervisor, Roland, along with his strong expertise in emerging technologies gave me the necessary tools, ideas and inspiration to complete the thesis in difficult times. You have shared many valuable life lessons. Thank you. From the very first day I met my daily supervisor, Martijn, you have inspired me with insightful brainstorm sessions and countless points of advice. The feedback was always clear and very helpful. Your excellent research skills and often opposing views have taught me a lot. Thank you.

Having done this thesis as an internship at EY, I want to thank the Technology Risk department and all the colleagues at the Rotterdam office. You all made my time at EY very pleasant and this has helped with the successful completion of the thesis and internship. I want to thank my company supervisor, Rick, for his support throughout. Your business mindset helped me with focusing the thesis. Moreover, your efforts have helped me with the search of participants in this study. You have guided me with making decisions regarding the next steps in my career. Thank you. My company advisor, Berry, has been a guide to EY and everything related to the internship. We had many conversations, related and unrelated to the internship. Without you, the internship would not be a success. Thank you. I want to extend my thanks to the everyone that participated in this study. New and interesting insights were revealed and you were all enthusiastic to help me. Thank you.

Finally, I want to extend my salutations and thanks to many friends and family, making my studies in Delft and abroad *exquisite*. Thank you all.

I hope this study on the negative societal impacts of quantum computing and communication will be beneficial to society. To anyone reading this thesis, I give my greetings to you and I wish you good health. Hopefully you will learn a thing or two.

Cemal Dikmen
Delft, April 2024

Management summary

Like any new and emerging technology, quantum computing and communication (QCC) has both positive and negative impacts. The aim of the study was to identify and understand negative QCC impacts in society. Employing a mixed research approach encompassing a systematic literature review followed by qualitative expert interviews, various QCC impacts are identified and a comprehensive framework is developed. The findings reveal a range of impacts, from the proliferation of cyber security threats stemming from cryptographic vulnerabilities, to inherent limitations within quantum technology itself.

In categorising the impacts, a distinction is made based upon the origin of the impacts. Endogenous impacts are impacts that are stemming from the quantum technology itself, while exogenous impacts are stemming from the application of quantum technology in a societal context. It is recognised that this distinction is not binary in reality, and many impacts exhibit attributes of being both endogenous and exogenous. However, this distinction is useful in the mitigation of the impacts and provides a clear categorisation for stakeholders.

The two themes within endogenous impacts are quantum technology limitations and quantum illiteracy. Quantum technology limitations is only mentioned in the literature. Within this theme are impacts that characterise certain attributes of quantum particles. As such, qubits are portrayed to be unstable due to their susceptibility to environmental noise. This means data in the form of quantum information might be fragile which poses negative consequences to privacy and trust of end-users. Moreover, the absence of a linear relationship between input and output data results in opacity in which outputs cannot be linked to inputs. Interpretation of results might be difficult and this means that there is a lack in transparency of potential applications, resulting in a 'quantum black box'. To continue the qubit limitations, quantum key distribution (QKD), in which secret keys are distributed over an unsafe network, has several shortcomings as well. These shortcomings pose opportunities to different types of attacks on QKD, making communications not sound and safe. This requires extensive error-correction techniques that are currently in development. These quantum technology limitations portray a low technological readiness level.

Quantum illiteracy is a topic that is discussed in the literature and it is raised as a concern during the interviews as well. As quantum technology is a complex technology based on quantum physics, stakeholders might have the idea that they do not grasp the technology and this results in a lack of public participation around decision making and participatory technology assessment. Moreover, quantum illiteracy extends to a lack in organisational readiness. It is characterised as endogenous because of the inherent complexities of quantum physics that facilitate this illiteracy.

Several exogenous impacts are elicited from the literature and the interviews. To start, the potential impacts within the theme of cyber security stem from the current cryptography vulnerabilities. With the development of Shor's algorithm, different cryptosystems currently in use will become obsolete. Utilising a quantum computer with a sufficient amount of qubits, Shor's algorithm can solve a traditionally complex mathematical problem: prime number factorisation. Different types of cryptosystems rely on the complexity of this problem, such as the RSA cryptosystem. This means that the societal systems that depend on cryptosystems such as RSA will be insecure from a cyber security perspective. This threat allows several impacts to occur, such as decreased cloud security, decreased software durability and decreased communication security. When these impacts enfold, several other impacts will arise as a result. Privacy and trust concerns are values that are mentioned in this context as a result of cyber security concerns.

Post-quantum transition and standardisation efforts are much needed but still lacking and limited in society. Updating and incorporating post-quantum cryptography into existing infrastructures is a challenging and lengthy process. QKD does not fit well with current existing network architectures. Resource constrained devices, such as IoT devices, cannot run post-quantum cryptography systems yet. Moreover, because of the governmental- and business dependencies on current systems, a hybrid infrastructures is expected to emerge in which both classical and quantum systems are working in parallel. Such a hybrid structure is new and poses several other challenges to scientists and engineers.

As QCC has both a potential to bring strategic advantage and military capabilities, scholars speak of an unequal distribution of knowledge, power and wealth. In this case, some governments and companies own the technology, while others do not. This poses a situation in which there may be a bigger global imbalance of power. Moreover, companies with quantum computing capabilities may be in a position in which they have an unfair strategic advantage over other companies that do not have access to quantum computing. This uneven access to the technology on a corporate level, and on a governmental level, is called the quantum divide.

QCC can be used for military applications, enhancing current capabilities and providing opportunities for new military capabilities on the battlefield. Scholars call this usage quantum warfare. These dual use capabilities may result in a wider global imbalance of power and result in geopolitical turmoil. Furthermore, because of the military usage, there is a lot of secrecy involved in the development of QCC, limiting the inclusion of stakeholders. This hinders responsible innovation.

The interviews provided a more balanced set of impacts with respect to the literature, highlighting unknown application areas as a negative impact, the environmental impact, the enhancement of known impacts and company culture as a confounding factor for negative impacts. Furthermore, the interviews revealed the recognition of company culture as a pivotal factor in anticipating and addressing QCC-related cyber security threats, and the respective migration to post-quantum systems. This underscores the importance of organisational readiness and adaptability in navigating the evolving landscape of societal impacts posed by QCC advancements. Moreover, the lack in coordination and central authority in migration efforts into post-quantum cryptography systems is concerning.

An overview of the total themes of impacts can be found in Figure 1. The themes that are exclusive to the interviews are highlighted in green, and the theme that is exclusive to the literature is highlighted in blue. The categorisation of impacts in relation to their respective themes provides a structured framework for understanding and addressing challenges posed by QCC impacts.

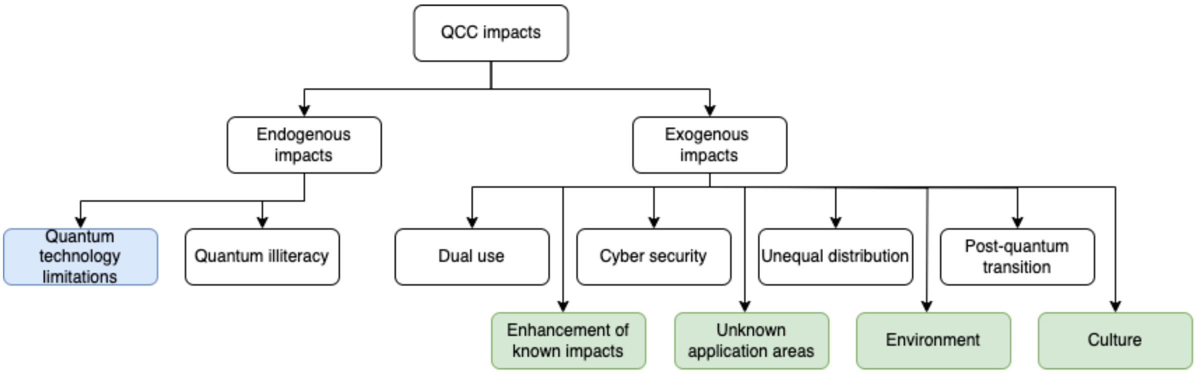


Figure 1: Complete overview of themes of impacts

It is found that the impacts are not mutually exclusive and often form complex interrelations among each other. One impact may cause several other impacts to occur, causing a cascading effect of impacts in society. Moreover, the impacts are often ambiguous, portraying both positive and negative effects to society.

Utilising known classifications of impacts, and incorporating the acquired insights of this study, a new generic classification is proposed in the anticipation of emerging technologies. It separates itself from the existing classifications due to the inclusion of specific distinguishing features of QCC, such as the transition period and technology limitations.

- Unequal distribution of knowledge, power and wealth
- Privacy
- Trust
- Autonomy
- Sustainability

- Geopolitics and international relations
- Cyber security
- Dual use potential
- Technology limitations
- Organisational readiness
- Infrastructural fit

Managers and policy makers can utilise these insights to formulate strategies in the anticipation and mitigation of QCC impacts, both on a organisational level as well as on a national level. In light of these findings, multiple managerial implications are highlighted. Organisations should focus on facilitating an assertive culture, allowing for anticipation of impacts and long-term strategy. Moreover, it is advised that organisations should incorporate learning programs for their workforce and relevant stakeholders. Fostering an open innovation culture can allow for stakeholder engagement and informed decision-making on QCC anticipation and strategy.

Contents

List of Figures

List of Tables

Nomenclature

Abbreviations

Abbreviation	Definition
QT	Quantum technologies
QCC	Quantum computing and communication
RQI	Responsible quantum innovation
RRI	Responsible research and innovation
QRNG	Quantum random number generation
QKD	Quantum key distribution
RI	Responsible innovation
ELSPI	Ethical, legal, social and policy implications
ELSA	Ethical, legal and social aspects
ELSI	Ethical, legal and social implications
RA	Risk analysis
eRA	Ethical risk analysis
AI	Artificial Intelligence

1 Introduction

1.1. An emerging and breakthrough technology

Quantum technology is an umbrella term, encompassing several applications of quantum mechanics. These novel technologies utilise parts or attributes of quantum mechanics to improve current systems, or develop completely new systems. Improvements such as highly detailed radar imaging, ultra fast super computers and simulations of extremely complex phenomena are but a few examples [1], [2], [3]. Quantum technology can thus be seen as a stimulating technology, amplifying the potential of other existing and emerging technologies such as AI and bio-engineering [4]. This hybrid use, however, comes with an important implication: quantum technology, in combination with other technologies, can also amplify the negative existing impacts of such technologies, resulting in a multiplier effect of bad outcomes [4]. Moreover, as quantum technology is also advancing military technologies [5], it can be considered a dual-use technology which has both military and civil applications [6]. The usage of quantum technology for military goals and advanced weaponry raises multiple other ethical concerns [7].

One of the early concerns came in the form of a quantum algorithm that could factor large prime numbers in seconds [8]. The development of this algorithm comes with numerous implications, because the very foundation of modern day cryptography lies in the fact that computers cannot factor large primes fast [9]. In a society that is becoming increasingly more digital, and dependent on digital systems, both on the micro level and macro level, this poses a great cyber security threat: bank payments, digital identification and defence systems all rely heavily on cryptography. One can imagine the possible negative impacts involved with this development. Moreover, it remains largely unknown what other algorithms are being developed currently, or are possible in the future [10]. In addition, it is not yet completely known what can be done with quantum processors [11].

For these reasons, it is critical for the government, academia, business and civil society to anticipate both possible and plausible negative impacts and act correspondingly by taking countermeasures sooner rather than later. To be able to act accordingly, the possible negative impacts need to be identified first. However, most research focuses primarily on the advantages and opportunities of quantum technologies in adjacent fields such as machine learning and metrology [12], [13], [14]. Conversely, the research about quantum technology impacts and technology assessment lacks behind, neglecting possible negative impacts. Research regarding ethical, legal, social and policy implications of quantum technology, referred to as Quantum-ELSPI, is a novel multidisciplinary field of research. Scholars have recently urged for the contribution to research in this field [4].

1.2. Research objective and scope

An identification of potential negative impacts is linked to the ability to anticipate negative outcomes and consequences, and act accordingly [15]. To delineate the scope of the research, the focus will be on two main branches of applied quantum engineering: quantum computing and communication (QCC). Both quantum communication and quantum computing depend on each other. Advancements in quantum computing allow for further development and testing of quantum communication protocols and its applications. Furthermore, the research regarding QCC is rich and the prospected diffusion and maturity of the technologies is relatively developed [11], [16].

The focus of the study is on the technology itself rather than on a single industry or specific application domain of QCC. This has multiple reasons. First, the current possible range of applications remains limited and under explored. Second, applications of QCC are interdependent and influential in various other existing fields, and potential upcoming fields. Thus, the potential negative impacts could manifest throughout society, without being bounded by a specific sector. Third, a technology-focused scope may allow for cross-pollination of ideas. Stakeholders from different sectors and research fields may explicate their views and ideas on the topic, resulting in an interdisciplinary and cross-sectoral amalgamation of standpoints and opinions on the matter. As potential negative impacts are not limited to a certain aspect of society, this exploratory research tries to encompass and address potential impacts of QCC to business, governments and the general public, including potential environmental hazards as the population could be affected by this. This scope is encompassed as *society* in this research.

Moreover, the scope is not delineated to geographical areas. As a dual use technology, quantum technology has various military applications, making it a broader geopolitical point of discussion, encompassing ethical, legal and social implications [7]. A global collaboration on responsible quantum innovation is encouraged for the same reasons as interdisciplinary and cross-sectoral benefits on this matter [4].

This exploratory research study aims to address the knowledge gap and lack in understanding of societal quantum impacts by 1) understanding and identifying potential negative QCC impacts on society and 2) creating a classification and categorisation of potential negative impacts to guide policy makers, managers and researchers in acting upon those impacts. In this light, two different research methods will be applied. First, a systematic literature research will be conducted to elicit anticipated potential negative impacts of QCC.

Second, to build upon the knowledge of the systematic literature review, qualitative expert interviews will be conducted to gain insights from academic- and industry experts. The commonalities and differences between the literature and expert interviews will be discussed to form a holistic view on QCC impacts. Furthermore, shese impacts will be categorised based on their origin and theme. Moreover, utilising the knowledge of the impacts and their categorisations, in combination with known classifications of impacts in the context of emerging technologies and society, a new classification can be proposed. With this identification and classification of potential impacts, firms and policy makers can develop strategies to tackle dangers and unknowns systematically. This research thus has both managerial and policy implications.

In this light, a deeper understanding of the possible negative impacts involved in the diffusion of QCC may assist managers and policy makers in anticipating possible impacts, and further guide decision-making in these unknown times of quantum technology. The main research question is: *What are potential negative impacts of quantum computing and communication on society?* Therefore, this research contributes to the following: i) highlighting possible negative impacts that could pose dangers to society, ii) provide a more holistic view of looking at QCC impacts in order for stakeholders to anticipate and steer accordingly, iii) start building further in the emerging RQI literature by addressing the gap in research about QCC impacts, and iv) suggesting possible mitigation strategies and future research directions for scholars.

1.3. MoT relevance

The MSc. Management of Technology programme views engineering and technology as valuable corporate resources. These resources are utilised in order to obtain different positive outcomes, such as sustained competitive advantage. However, in the innovation processes of developing and utilising such technologies, various ethical dilemmas need to be considered and addressed. Emerging and breakthrough technologies tend to have various business applications, and their patterns of diffusion may be used strategically.

Nonetheless, despite the potential benefits of the application of technology in a corporate setting, the MoT curriculum underscores the importance of taking into account potential negative outcomes and innovating responsibly. One such example is Shor's algorithm, which showed that current cryptosystems are in jeopardy once a powerful enough quantum computer is developed, making these negative outcomes a question of time. It is therefore essential for both managers and policy makers to proactively anticipate and address potential negative impacts of QCC in order to act accordingly. An illustrative example is the potential impact banks may face which could manifest further into society, because of modern society's dependability on banks.

This research thus has both managerial as well as societal implications, and tends to address these uncertainties in a multidisciplinary approach. In this context, managers and policy makers can benefit from this research. By utilising the results, they can produce strategic roadmaps for mitigating and anticipating potential negative impacts that come with QCC implementations in the near-future. Through proactive engagement, stakeholders can work together towards a more ethical and responsible adoption of QCC, thereby focusing on the potential benefits, while minimising the potential negative impacts.

1.4. Structure of the report

The rest of the report is structured as follows. Chapter 2 provides a background of quantum technology. Offering insights in the historical development, underlying principles and theoretical concepts of QCC. Chapter 3 provides background information into the field of technology assessment. In chapter 4, the methodology utilised in this study is explained. Highlighting the research design, the research strategy and data collection methods. Chapter 5 presents the findings and results of the study. Chapter 6 provides a discussion of these findings, addressing theoretical- and managerial implications and providing recommendations for future research directions. Finally, chapter 7 concludes the study.

2 Quantum Mechanics, from Past to Present

Scientific breakthroughs allow for the engineering of innovative solutions for contemporary problems in society. As such, in the beginning of the 20th century, the First Quantum Revolution resulted in novel ways of explaining laws of physics on the sub-atomic level [16]. What was considered as a paradox, particles can behave as waves, and light waves can behave as particles, turned out to be true. These discoveries allowed for advances in semiconductors and the modern personal computers were born. Utilising these laws of quantum physics in order to engineer systems, instead of understanding natural phenomena, is the foundation of the Second Quantum Revolution and modern quantum technologies.

In the past decades, quantum technology has seen various interests from academia and business because of its breakthrough applications. Quantum technologies rely on various fundamental attributes or principles of quantum mechanics. To elucidate these principles, it is crucial to underscore the concept of a quantum particle. Quantum particles, such as photons, protons, and electrons, exhibit dual characteristics, possessing traits of both 'hard' or 'matter' particles and waves. This wave-particle duality gives rise to the phenomenon known as tunnelling, wherein a quantum particle can probabilistically appear on the other side of a classically impenetrable barrier, even when its energy appears insufficient [17]. However, due to the quantum particle's non-continuous nature, it does not possess a continuous energy wave function but rather occupies discrete energy levels, referred to as quantised states. An illustrative example of quantisation can be found in the discrete energy levels of electrons orbiting the nucleus of an atom.

Quantum particles also exhibit the property of entanglement [18], whereby they can become interconnected or linked, with one particle's state being intrinsically tied to the state of another, irrespective of the distance separating the two particles. This phenomenon violates classical causality notions, as changes in one particle instantaneously influence the other [19]. Einstein and his colleagues named this phenomenon the 'spooky long distance effect' and concluded that quantum theory might be incomplete at the time [20]. However, this property has indeed been confirmed through various experiments [21].

Additionally, quantum particles adhere to Heisenberg's Uncertainty Principle, which dictates that it is impossible to simultaneously determine both the precise position and momentum of a particle [22]. This leads to another key attribute called superposition, where quantum particles can exist in multiple states concurrently [17].

These characteristics, or attributes, collectively define the unique and often counter intuitive behaviour of quantum particles. This provides an accurate framework for the understanding and prediction of the behaviour of such particles at the quantum level, allowing for scientific breakthroughs and technological innovations.

2.1. Quantum technologies

The various characteristic attributes of quantum mechanics can be utilised and applied in various fields. Beginning in the early 20th century, quantum technologies have since then evolved and show differ-

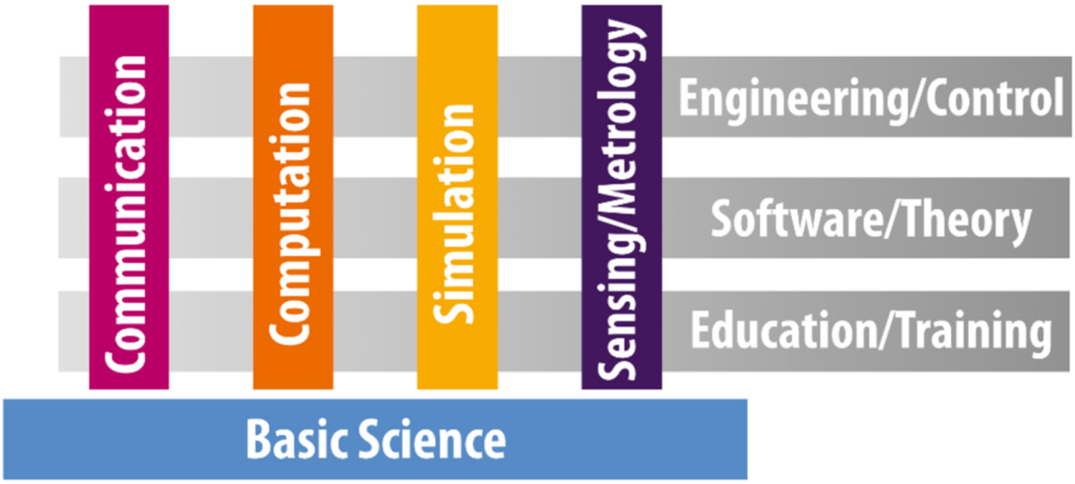


Figure 2.1: Four domains of quantum technology [11]

ent forms of diffusion through society. An excellent article discussing quantum technologies and their pattern of development and diffusion is written by Ortt [23]. The committee of the European quantum technologies flagship initiative have distinguished four main research fields of quantum technologies [11], as can be seen in Figure 2.1.

2.1.1. Quantum communication

In cryptography, secure communication is accomplished by encrypting a message with a key, and decrypting the message once it arrives at the receiver's end. Quantum cryptography utilises two important concepts for this goal: quantum random number generation (QRNG) and quantum key distribution (QKD) [24]. Traditionally, encryption relies on the generation of large random numbers for the creation of the key. These numbers are generated by a generator that gives an approximation to a random number. Meaning that the number is not truly random. QRNG produces truly random numbers. Furthermore, quantum communication protocols have quantum key distribution (QKD) at their foundation [24]. QKD is in place to distribute the randomly generated key securely and privately in two locations.

These concepts are at the foundation of the quantum internet. What began as a simple network of nodes in which experimental messages were sent, the Advanced Research Projects Agency Network, or ARPANET, formed the very first Internet as we know it today. Currently, engineers and scientists are in the works of creating a quantum internet [25]. Apart from QKD, central to the notion of the quantum internet are the so-called quantum bits, or qubits [26].

Whereas classically, information is stored in bits, values of 0 or 1, in quantum computing information is stored in qubits. Qubits are mathematical representations of quantum particles, characterised by two states, denoted by $|0\rangle$ and $|1\rangle$.

Qubits can assume a superposition in which they can be a 0 and 1 at the same time, in addition to the states of classical bits. If this is combined with entanglement, in which two qubits are entangled, their states are instantly correlated over great distances. This means that alteration of a qubit q^1 will be recognised and detected immediately, because its entangled qubit q^2 will be altered accordingly. This attribute can thus provide a provably secure system [25]. Qubits can thus be utilised to acquire and transmit information in new ways.

2.1.2. Quantum computing

Quantum computing is a complex concept. A quantum computer needs to satisfy a set of five criteria, known as the DiVincenzo criteria [27]:

1. A scalable physical system with well characterised qubits
2. Initialisation of the state of qubits
3. Long relevant coherence times
4. A set of quantum gates

5. Measurement of qubits

A qubit is well characterised if its attributes are clearly known. This includes information about the energy levels, the interaction with other qubits and possible links to external sources that might change the state of the qubit. This ties into the second criteria, namely the ability to initialise the initial state of a qubit. In classical computing, registers need to be initialised to known values before computation starts. This translates to qubits being initialised in quantum computing. If qubits are used in computation, their state can be altered based on their interactions. This alteration can take some time to happen, and if it is too fast, meaning, faster than a qubit clocktime, it can result in faulty error correction. This time is called the coherence time of a qubit. Moreover, digital information processing is classically done using bits. Bits can be used to encode information in binary data and this will then be transferred and processed. To this end, digital logic gates are used to process and encode binary data. Different gates can be combined to create complex circuitry and processors. In quantum computing, these gates are called quantum gates and they are used to deal with the complex nature of qubits and their ability to be in a superposition of 0 and 1. The quantum gates are used to make complex circuitry in order to solve quantum computations efficiently [26].

While computation is important, communicating this data is only natural for the realisation of the benefits of quantum computing. Two more criteria are added in order to ensure communication: the ability to interconvert qubits from a stationary phase to a mobile or 'flying' phase, and the ability to transmit these qubits securely [27]. Advancements in quantum computing result in advancements in quantum communication, making the two sub-fields interdependent. One example is the theoretical development of quantum algorithms, waiting for an implementation of a quantum computer to be run efficiently. One of these algorithms is Shor's algorithm for prime factorisation.

Quantum simulation and quantum metrology are two fields of research with a long history. The concept of quantum simulation dates back to 1980's where Richard Feynman introduced the concept of simulating quantum phenomena with dedicated machines [28]. There are many applications of quantum simulation in (quantum) physics, nuclear physics, chemistry and biology, among others [3].

When things are measured, be it time, distance or radio frequencies, small statistical errors can occur as a result of the type of measurement or system of measuring. The central limit theorem can be applied to minimise the error by performing many measurements *n* after which the standard error will be minimised by distributing the standard deviation over the squareroot of the number of measurements. Utilising quantum attributes, such as entanglement, measurement can be done more accurately [14]. This is the idea of quantum metrology, conducting measurements with higher degrees of precision, accuracy and efficiency. The applications of quantum metrology are numerous. One of such applications is the atomic clock [29], [30]. The precise measurement of time has itself many applications and benefits in applied engineering such as GPS.

3

Technology Assessment and the Dilemma of Control

3.1. The Collingride Dilemma

The emergence and proliferation of a nascent technological innovation may result in both numerous benefits and advancements in society, as well as unforeseen dangers and hazards. Indeed, when such a new technology is in its infancy stages, the potential societal impacts and perils remain difficult to forecast. Simultaneously, it is relatively easy to control and influence the technology at this stage. In contrast, when the technology matures, the previously uncertain impacts and risks become known, but it might be difficult to control the technology. This conundrum of technology governance is called the Collingridge dilemma [31].

This dilemma can be explained by numerous historical scientific and engineering breakthroughs. A notable illustration lies in the top-secret Manhattan Project during World War II, which mirrors the essence of the Collingridge dilemma. During the early stages of development, the project was shrouded by secrecy and lacked comprehensive understanding of its societal implications. However, when the consequences were clear, the project already advanced in the development of the atomic bomb and the geo-political landscape was set. This example indicates the importance of responsible research and innovation, paying attention to ethical considerations from the start of new scientific breakthroughs and at the advent of emerging and breakthrough technologies.

However, a focus solely on risk as a result of uncertainty, or incomplete knowledge, is inadequate as this neglects information that decision-makers need [32]. *”Risk”* is a contested term used in different settings with multiple meanings and definitions. The terminology of risk lacks academic coherence and its epistemology is ambiguous [33]. In an attempt to standardise risk, the International Organisation for Standardisation (ISO) defines risk as a combination of the probability of a certain event occurring and the consequences of this event [34], [35]. This terminology follows the work of Frank Knight [36] in which he made a clear distinction between risk and uncertainty. Risk is something measurable, whereas uncertainty is not.

Notwithstanding, in the engineering of new technologies, many unknowns exist. History shows that new innovations can come with unforeseeable outcomes. It is difficult to forecast what kind of success a new product will have, or what the various products even will be like. Indeed, with such technologies there remain many unknowns at first, making risk assessment and risk analysis problematic [37]. In the case of quantum technology, the probabilities of both positive and negative outcomes of quantum computing and communication are unknown and uncertain, yet there are some foreseen dangers or hazards such as the cyber security implications of Shor’s algorithm. In this case, the domain of ignorance [38] and the concept of uncertainty [37], [39] are relevant. Ignorance is explained as the crossroads of unknown processes and unknown variables [38]. As a radically new technology in its premature stage, quantum technology deals with known dangers, and potentially many more unknown dangers. Hoffman-Riem and Wynne [38] argue that novel risk assessment is limited by the adversity of considering these crossroads of unknowns. To assess unwanted outcomes of quantum technology, a more holistic approach is needed to guide managers and policy makers in their decision-making processes. Therefore, this paper will use the terms 'potential negative impact' to address uncertainties, unknowns and risks in combination with known negative consequences of quantum technology, that may or may not happen in the future.

Following the Collingridge Dilemma, Technology Assessment (TA) is an interdisciplinary field of research that utilises various systematic methods for anticipating potential negative impacts in an early stage in order to prepare and shape the technology. [40]. Unforeseen impacts of technology are the focal point of TA, focusing on the dilemma of control. More specifically, TA deals with technologies and their unintended impacts and uncertainties that arise with the application of technology in society [41]. An emphasis lies in knowledge creation and the subsequent evaluation of this knowledge to make recommendations on a societal level [42]. It is impossible to predict what kind of success a new product will have, or what the product will be like in the future after diffusion has occurred. Indeed, with such technologies there remain many unknowns at first, making risk assessment and risk analysis tasks that are captivated by uncertainty [37]. Moreover, the potential hazards of new technologies and innovations are often overlooked, as scientists and businesses usually focus on the adoption, profitability and general performance of a new innovation, rather than ethical consequences. This narrow focus leads to many unknowns in the pattern of development and diffusion of the technology, and can neglect negative outcomes. Furthermore, modern risk analysis is based on probabilities of unwanted outcomes. However, in early stages of new technologies, these probabilities and the effect of the possible impacts are unknown. Hence, the concept of uncertainty is relevant [39], [32]. Moreover, focusing solely on (known) probabilities of such unwanted events in risk analysis neglects important information that decision makers need [32]. This is the reason Hansson [39] suggests that an ethical risk analysis should supplement traditional risk analysis, focusing on human values and ethics.

Moreover, the difficulty in anticipating societal impacts of new technologies lies in the growing complexity of technological systems [42]. Different aspects of society are interwoven in complex networks of interconnected technologies. An example is the payment system in online banking. Different banks, technologies, standards, communication protocols, safety protocols and laws are all linked together to form a comprehensive system that allows online banking and payment to take place safely and securely. If one technology is changing, it affects the entire system and causes differing levels of uncertainty in terms of reliability and safety on the many technologies linked to it. The question here is how can society, that is increasingly dependent on online banking, be protected against negative impacts when a new technology is introduced that is affecting the current system in place? Hence, TA is characterised by normative elements in anticipating technological impacts. One element is determining the impact of technologies to society in order to prepare and take countermeasures beforehand [42]. The goal here is to anticipate potential negative impacts and reducing the negative effects on society. This way of TA is also called constructive TA in which social issues are addressed at the early design stage of a new technology [43]. This approach involves governmental actors and NGO's.

Participatory TA (pTA) is the set of TA methodologies in which various stakeholders are involved to include broad societal perspectives in the decision making process of emerging technologies [44]. Other scholars have proposed a different view of pTA that focuses on in-depth analysis of social consequences by means of involving all social stakeholders [45]. The goal here is to influence technology design by not only including public participation, but also focusing on gaining a deeper understanding of social consequences of technology.

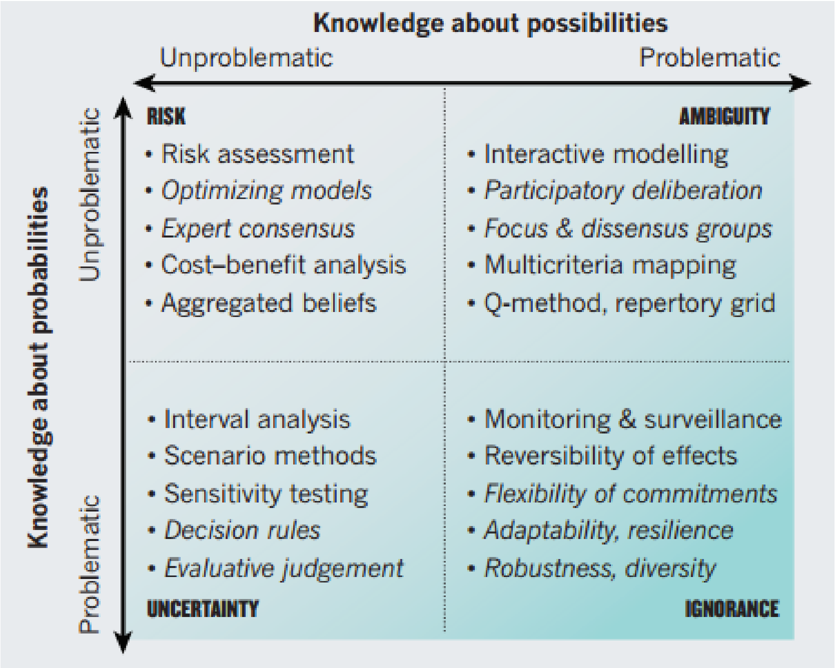
As technology is socially shaped, TA evolved into constructive TA to consider social behaviour around technologies. Historically, TA had multiple areas of focus, ranging from advising decision makers in regulation and funding, to shaping the technology itself corresponding to social values [41]. As technology and society change, so do different TA approaches change and adapt accordingly, depending on the need and given context [41]. One of such changes in approach is called Real-Time Technology Assessment [46]. In this approach, instead of allowing decision makers to react to technology, values are incorporated during the research and development phase. This allows the technology to be steered in real time, incorporating values early on. In addition, Palm and Hansson [47] have proposed a new form of TA that focuses specifically on ethical implications of new technologies: ethical Technology Assessment (eTA). It is argued that due to the complexity that revolves around novel technologies, illiteracy can become a barrier that refrains people from partaking in the discussions regarding new technologies and asking questions about ethical issues that may arise. Addressing moral issues during the entire life-cycle is needed as different issues can emerge at different stages of development and diffusion [47].

3.2. Towards a classification of impacts

A classification of potential impacts has several benefits, especially for new and emerging technologies in which many aspects remain unknown and uncertain.

First, it allows for a structural and systematic approach in understanding potential negative impacts. The classification of impacts into distinct categories may aid decision-making processes by giving stakeholders generic insights into what potentially could go wrong. This can support proactive strategic decision-making efforts in the distant future. Second, companies and different stakeholders may have differing values and priorities. A categorisation can aid in the creation of such a prioritisation and therefore helping stakeholders and companies allocate resources accordingly. Third, based on the perceived importance and overview of impacts in categories, risk mitigation strategies may be formulated. A classification provides a clear and simple visual representation of such impacts, aiding in this process. Fourth, a classification of impacts into understandable categories can enhance stakeholder engagement. The organisation of impacts can aid in communication efforts, allowing for a greater awareness on the topic. Moreover, it can help with the development of policies and regulations on the topic. Policymakers can utilise the classification to address specific groups of impacts by means of regulatory frameworks.

There are some examples in the literature of such classifications of negative impacts of technology. Stirling has proposed a framework of looking into a broader definition of problems instead of having a narrow focus on risk only [32]. The distinction is made between risk, ambiguity, uncertainty and ignorance. An overview of the matrix can be seen in Figure 3.1. The goal here is to acquire knowledge about the problems in order to move to the first quadrant where more is known about the problem's possibility and probability, hence being called a risk.



Knowledge about possibilities

Unproblematic — Problematic

Knowledge about probabilities

Unproblematic — Problematic

RISK
- Risk assessment
- *Optimizing models*
- *Expert consensus*
- Cost–benefit analysis
- Aggregated beliefs

AMBIGUITY
- Interactive modelling
- *Participatory deliberation*
- *Focus & dissensus groups*
- Multicriteria mapping
- Q-method, repertory grid

UNCERTAINTY
- Interval analysis
- Scenario methods
- Sensitivity testing
- *Decision rules*
- *Evaluative judgement*

IGNORANCE
- Monitoring & surveillance
- Reversibility of effects
- *Flexibility of commitments*
- *Adaptability, resilience*
- *Robustness, diversity*

Figure 3.1: Stirling's uncertainty matrix adapted from [32]

To continue on risk and uncertainty, other scholars [48] describe systemic risks as risks that are not calculated based on linear probability functions. They are characterised by uncertainty, complexity and ambiguity. These 'risks' are called systemic risks because of the degree they are integrated in the societal context, involving different inter-dependencies of actors and institutions. This makes these risks more prone to potential harm on society [48]. Moreover, systemic risks are complex because of these inter-dependencies. They are characterised by uncertainty as future consequences are not always known or certain. Furthermore, systemic risks are ambiguous. In the positions of different stakeholders, they can be seen as either tolerable, acceptable or unwanted. This gives no clear understanding of the consequence such a risk can have as it provides different values to look at. Risk governance is a conceptual framework of dealing with such risks. It is argued that uncertainty stems from complexity and the combination of uncertain outcomes and complex problems allow for ambiguity [48]. Taebi et al. [49] put forward the debate about the concept of normative uncertainties in risk governance. Uncertainty is present when an event lacks sufficient information, marked by a state of ignorance. Furthermore, this not only applies to the present knowledge of the event, but also on the normative implications of the event itself. If there are multiple normative perspectives on actions to take in an event with limited information, then that event falls under the category of normative uncertainty [49].

In contrast to the complexities of normative uncertainty, a more zoomed-in view of looking into impacts and their classifications can be found in the safety factors approach from structural engineering [50], [51]. This deterministic approach looks at the ratio of a measurement against the maximum value possible without resulting in a failure of the system. Safety margins are used to allow for variability among the possible events that might occur, without resulting in failure. This approach looks at five possible sources of failure in structural engineering [50]:

1. Higher loads than those foreseen
2. Worse properties of the material than foreseen
3. Imperfect theory of the failure mechanism in question
4. Possibly unknown failure mechanisms
5. Human error

The safety factors method classifies sources of failure as either risks or uncertainties. Possible events 1 and 2 are foreseen and they are classified as risks, even though their probabilities are not always known. Whereas sources of failure with events that are difficult or impossible to assign probabilities to, such as numbers 3 through 5, are classified as uncertainties. Moreover, in anticipating sources of failure, the distinction is made between safety and security. Safety is defined as the protection in cases of unintended harm, whereas security is defined as protection in cases of intended harm by an intelligent adversary. Security revolves around the identification of vulnerabilities of the system and respective mitigation strategies to reduce the vulnerabilities. So the safety factor approach distinguishes the classifications of risk and uncertainty in anticipating sources of failure and thus tries to encapsulate unknowns in this regard[50]. This can be extended to the identification of possible negative impacts of QCC in which probabilities are unknown and many uncertainties persist.

Other authors propose a more in-depth view of generic values that could be affected by new technologies. In order to discuss ethical issues of new technologies at an early stage, before the technology manifests throughout society and its potential negative impacts proliferate, Palm and Hansson propose a systematic approach in the form of a check-list in order to elicit ethical issues lingered with new technologies [47]:

- Dissemination and use of information
- Control, influence and power
- Impact on social contact patterns
- Privacy
- Sustainability
- Human reproduction
- Gender, minorities and justice
- International relations
- Impact on human values

Continuing with this line of reasoning and building upon the foundations of eTA, another similar, but larger, set of values or principles, information technology should adhere to, is provided by Wright [52]. Autonomy is added in which the authors focus on individual autonomy, dignity and informed consent. The focus is on a zoomed out view on ethical considerations in which they have the following five themes:

- Respect for autonomy

- Non-maleficence (avoiding harm)
- Beneficence
- Justice
- Privacy and data protection

Furthermore, the Dutch Rathenau Institute[1] is an organisation that does research about new technologies in a TA approach. They have developed a similar generic list of ”social values” that could be undermined by new technologies. This list is made in the context of quantum technologies in general, and their interaction with society and the societal concerns that may arise. In comparison with the aforementioned frameworks, this list specifically highlights cyber security and military security:

- Cyber security
- Privacy protection
- Military security
- Justice
- Strategic autonomy
- Knowledge security
- Trust
- Sustainability

[1] https://www.rathenau.nl/

4 Methodology

4.1. Research design

The research is exploratory in nature because not much is known about the potential negative impacts of QCC. The research objective is therefore to investigate potential negative societal impacts linked to quantum technology. More specifically, this research aims to identify and understand potential negative societal impacts of QCC and make a classification of these impacts. In this light, the following research questions are the heart of this study:

Research question

What are potential negative impacts of quantum computing and communication on society?

Due to little understanding of QCC and its potential negative impacts, the main research question tries to tackle these unknowns. *Society* is used in this case to encompass negative impact in general, without focusing on a single industry or application domain. In order to answer the main research question, several sub questions have been formulated.

To start, a classification and categorisation of potential negative impacts may provide an overview of various insights of these impacts. As such, it aims to give knowledge about differences and similarities in order to create and provide a deeper understanding of potential negative impacts. Stakeholders can use the classification to anticipate and steer accordingly.

Sub-question 1

What negative impacts to society are mentioned in the literature of quantum computing and communication?

Sub-question 1 forms the basis of this research for eliciting QCC potential negative impacts from existing literature. These impacts can then be categorised according to the knowledge gained from the review, and the themes of impacts elicited from the literature.

Sub-question 2

What negative impacts of quantum computing and communication to society can be anticipated, according to experts?

Asking about the potential negative impacts in the view of experts may provide interesting insights. First, there might be impacts anticipated by certain experts, that cannot be found in the literature. Second, experts from different fields could have different ideas of such impacts, depending on their expertise and industry. Third, the anticipated impacts by experts will be categorised and these found impacts can be different from the previous findings in the literature. This may result in a deeper understanding in addressing unknowns and uncertainties, providing insights into commonalities and differences.

Sub-question 3

What are the implications of potential negative QCC impacts on society?

Classifications are considered to be suitable with emerging technologies in a societal context. The goal here is to formulate a classification in order for managers and policy makers to utilise and steer development of QCC in society. This indicates a form of actionability of the research. Based on the findings from the literature and expert interviews, the known classifications can be combined and a new framework can be made utilising new insights linked to QCC anticipation. The intention behind this is to investigate if QCC is inherently different to other emerging technologies in general, and how this distinction can be addressed. Sub-question 3 aims to make the findings actionable by forming a complete framework of found impacts. Identifying and classifying impacts is trying to address gaps in literature. The next step in anticipating impacts is considering different options of the origins of such impacts and how to take action to mitigate negative consequences of these potential impacts. This highlights the practical implications of the Collingridge dilemma. Which actors can do what? What is the role of the government in mitigating impacts? How do firms play a role in mitigation? This is an interdisciplinary and multidisciplinary task. Utilising the answers of these questions, the main research question can be answered, forming a holistic view on negative QCC impacts.

4.2. Research strategy

In order to identify and understand the potential negative impacts of QCC, a systematic literature review has been chosen as the main research strategy. The systematic literature review will be conducted according to the PRISMA principles [53].

This literature review can be seen as a bottom-up approach. However, as this novel topic is relatively under explored, there are many uncertainties and there may exist unknown impacts of QCC. To investigate possible uncertainties and unknowns, the literature review will be supplemented by semi-structured expert interviews. The goal is to put forward the synthesised potential negative impacts of QCC in order for experts to i) verify the found impacts, ii) identify unknowns and uncertainties, and iii) highlight possible mitigation strategies. This approach of data triangulation tries to strengthen the internal validity of the literature research. The interviews will be held with both academic and industry experts on QCC risks and negative impacts. Experts from both the academic world and the industry will provide a more holistic, interdisciplinary and cross-sectoral view on the matter, trying to strengthen the external validity of this research. A graphical overview is given below in Figure 4.1.

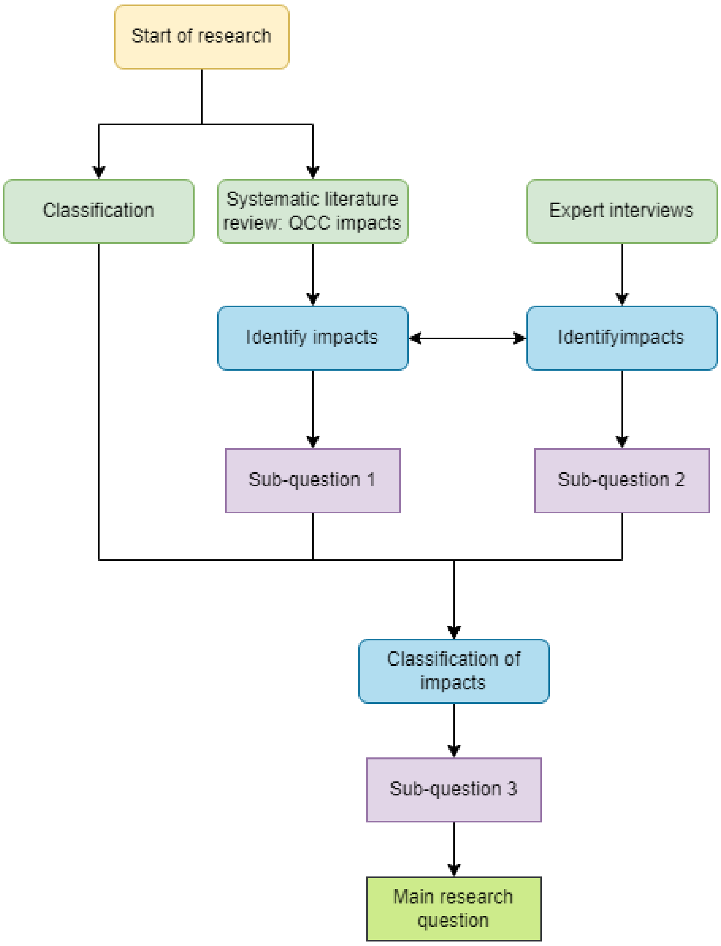


Figure 4.1: Graphical representation of the research design

4.3. Systematic literature review

Scopus is chosen as the research database as it is currently the most comprehensive and inclusive scientific database [54].

To this extent, adhering to the PRISMA guidelines by Moher *et al.* [53], the following search strategy will be used for searching relevant literature on QCC and its possible negative impacts: (”quantum tech*” AND (”quantum comput*” OR ”quantum communic*”)) AND (unknown* OR uncertaint* OR risk* OR danger* OR vulner* OR ethic* OR hazard* OR threat* OR impact* OR ramificat* OR peril*).

As quantum computing and quantum communication is central, it is enforced using parenthesis, in combination with quantum technologies in general. Both ’computing’ or ’communication’ or other variations of the words could be relevant, hence the usage of the asterisk wildcards: comp* and comm*. Furthermore, in identifying potential negative impacts and risks, QCC is relevant only in combination with words related to impact and risk. With this in mind, synonyms such as threat, danger, hazard and vulnerability are included in the search. QCC is then used in combination with these synonyms using the boolean operator AND. All synonyms are separated by the boolean operator OR, and the wildcard asterisk is used with each word to allow for other variations. The search results are not confined to a specific field of study as an interdisciplinary view is welcomed for a holistic perspective on QCC impacts. Moreover, the search results are limited to the English language only. There will be no geographical delineation in searching for documents, nor a publication date requirement. Duplicates are filtered in the search process.

This initial approach resulted in 175 unique documents found. The search was performed on 19 October 2023. The documents are saved and are subsequently screened by going over the title and abstract of the documents with the goal of excluding articles that are not relevant for the aim of this paper.

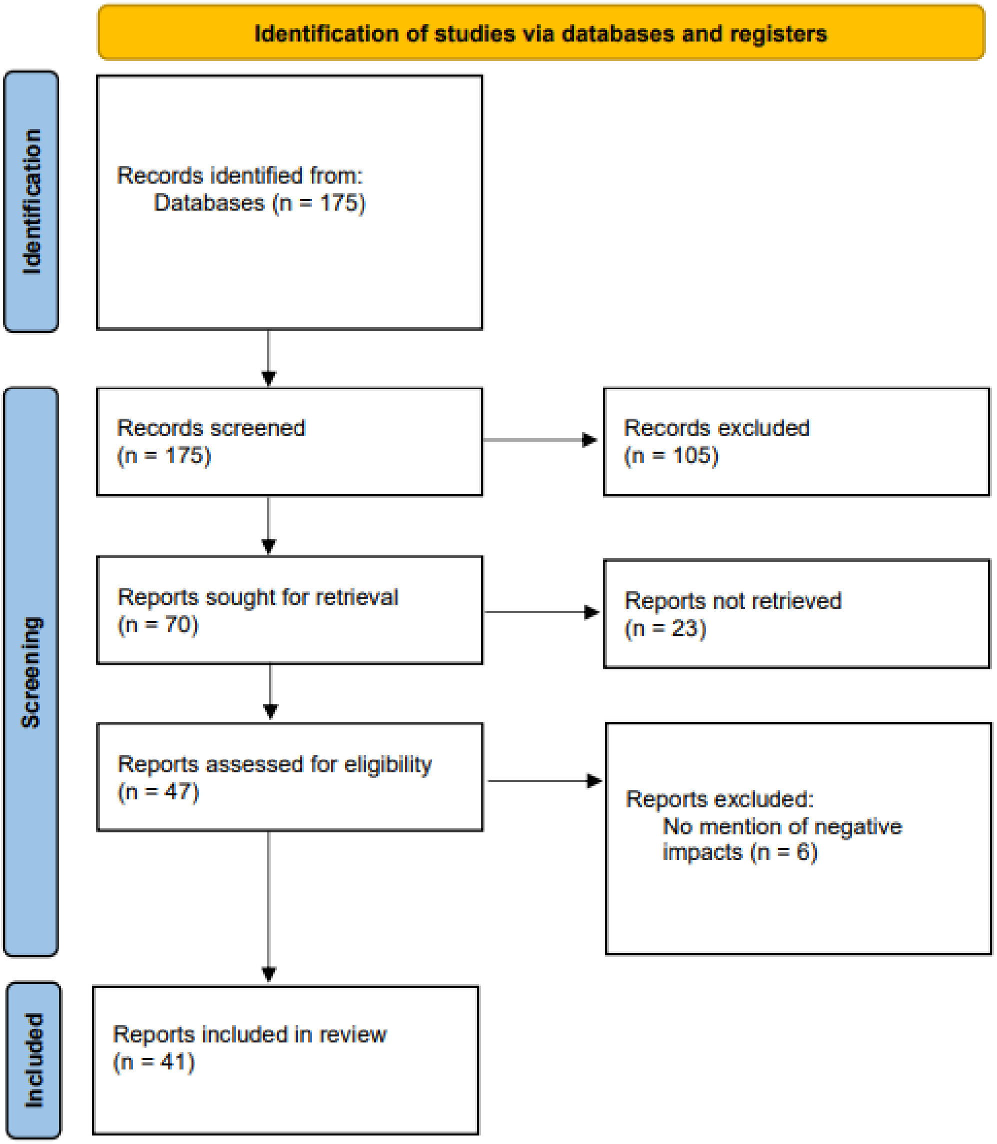


Figure 4.2: PRISMA flow diagram of the selection process (following Moher et al. [53])

A review protocol has been developed to carefully review the eligible documents. The 175 documents were screened by going over the titles and abstracts with the intention of filtering articles that mention any potential negative impact of QCC. From the 175 documents, 70 documents were eligible to be carefully reviewed on a full paper basis. These documents were saved in scopus and their meta data was exported to a MS Excel file in rows, numbered 1 to 70, sorted on the most recent addition to scopus. These articles were then downloaded and read thoroughly to elicit potential negative impacts of QCC on society.

From the 70 articles, 23 reports were not retrieved due to unavailability or restricted access. Articles to be included should describe potential negative impacts, risks, unknowns and/or uncertainties of QCC to society specifically. If an article does not describe a specific negative impact of QCC it will be discarded. The full article screening will thus focus on identifying impacts that are described to have potential negative consequences in a societal context. More specifically, the data sought in the articles should encompass negative impacts. From the initial 70 documents, 47 reports were assessed for eligibility after which 6 documents were excluded as they did not mention any negative impacts. Finally, 41 documents were included in the systematic literature review of this study. An overview of this selection process can be seen in Figure 4.2.

The full texts will be read to elicit potential negative impacts of QCC on society. These impacts can be any negative consequence as a result of the proliferation and diffusion of QCC. Moreover, unknowns and uncertainties are important to consider as these can result in negative consequences as well. To this extent, as not much is known about possible impacts of QCC, an inductive approach is chosen in the data extraction method. Identified negative impacts will be grouped into themes and categories to develop theory. This is done in a thematic analysis of the impacts. Moreover, this will help in the classification process of the found impacts. The impacts will be assessed and categorised by their nature and societal focus. Finding the impacts in the reports is done with coding on the paragraph level. This is coding strategy is chosen because there is no standard in naming or classifying impacts. For example, the word 'risk' is usually used in the context of negative impacts, even though there are no *risks*, by the epistemology of risk.

Moreover, there will also be a focus on potential unknowns and uncertainties that authors may highlight as these could be classified as potential negative impacts. The extracted data will be categorised and labelled with codes around a certain theme from which it emerged in the article. In this way, impacts can be synthesised and grouped after which they can be classified. This extracted data in the form of negative impacts will be saved and processed by storing them and counting them, using a spreadsheet tool such as Excel. In this way, a distinction can be made about what is given more attention in the literature, and what is underdeveloped in this regard.

To this extent, the following five points are important aspects of an impact to consider, and are explicitly looked for during the review:

1. impact
2. theme of impact
3. societal aspect of impact
4. provided solution/mitigation strategy
5. unknowns and uncertainties

A potential impact and its theme provide information on the origin and nature of a future concern stemming from QCC. Moreover, impacts may be named differently in different papers. Labelling an impact with a theme groups the same impacts with different names in the same category. Furthermore, the effect of an impact is seen in a societal setting and thus mentioning the societal aspect of an impact may provide more information on the potential implications. Some articles may also give information on solutions or mitigation strategies of certain impacts. This information is also collected as it may be useful to mention during the interviews in terms of anticipating problems. Finally, collecting unknowns and uncertainties on impacts forms a more complete view on an impact and may guide researchers into directions in anticipation and mitigation of such impacts.

4.4. Interviews

This research deploys multiple data collection methods and research instruments. Interviews are chosen to supplement and build upon the results of the systematic literature review. In this light, the rationale behind the sampling design is explained.

Semi-structured interviews allow for the exploration of different opinions and views regarding this unknown and complex topic [55].

As QCC is highly competitive and emerging, the subjects of this study will remain anonymous. The questions of the semi-structured interview will focus on the potential negative impacts of QCC and not on business strategies, research developments or other information that may be deemed sensitive or confidential. First, conducting the interviews and saving the data will be done according to the TU Delft Regulations on Human Trials and it will be compliant to the European General Data Protection Regulation (GDPR) [56]. Second, an informed consent form needs to be signed by the interviewees. This informs them what the research is about, what kind of personal data is collected and where this is stored and that participation in the research is completely voluntarily. This form can be found in Appendix A.

4.4.1. Sampling design

The target population of this research will be limited to stakeholders in the Netherlands. This is chosen to take into account the scope and timeframe of this thesis project. With a focus on the Netherlands, the

Table 4.1: Overview of participants included in this study

Participant	Position	Industry background
1	Quantum Engineer	Banking Industry
2	Security Policy Advisor	Banking Industry
3	Security Officer	Insurance Industry
4	Professor	Academic Institution
5	Researcher	Academic Institution
6	Researcher	Research Institution
7	Professor	Academic Institution
8	Policy Advisor	Government Agency

aim is to feasibly conduct semi-structured interviews. 'Stakeholders' is a broad term. In this research, stakeholders refer to experts in society, regarding QCC. This includes managers, policy makers and researchers, each contributing to different aspects of the QCC domain.

The sampling frame is thus a representation of experts on the topic of QCC. However, as the population itself is broadly defined there is no physical representation of all the elements in the population. Hence coverage error occurs because the sampling frame does not exactly match the population. This problem is recognised, but considered acceptable in this research as QCC is in its infancy stages and the potential impacts are under-explored in literature. On the contrary, a broad sample may portray differing views on the matter and can result in a more complete picture.

The research aims to qualitatively explore unknowns and uncertainties of potential negative impacts of QCC. Therefore, a non-probabilistic sampling design is chosen in the form of purposive sampling. With this sampling design, specific target groups are selected for the interviews, to elicit information regarding potential negative impacts of QCC.

More specifically, as a limited number of people have the knowledge on the information sought, the purposive sampling design of judgement sampling is selected [57]. In this way, subjects are selected specifically based on their knowledge and expertise on QCC. Expertise may be defined as having experience in decision-making regarding QCC topics in a firm, having academic experience in researching QCC or having experience in guiding policy regarding QCC. For the academic experts, the emphasis is also put into the expertise on ethics about QCC and society. The goal is not to draw statistical inference, thus probabilistic sampling is rendered purposeless in this research.

The expert interviews were conducted throughout January 2024, both in-person and online, based on the availability of the participant. These participants were selected because their involvement and backgrounds with QCC formed a broad and holistic set of expertise within different societal aspects.

A total of eight participants were interviewed, four from different industrial and governmental backgrounds, and four from research backgrounds. Six interviews were conducted in Dutch, and two in English. An overview can be found in Table 4.1.

The selected participants are asked about their opinion and view regarding unknowns and uncertainty of negative QCC impacts. Moreover, there is a focus on impacts that the experts anticipate. These anticipated impacts might differ from the impacts found in the literature. To look at the implications and next steps in anticipating impacts, the experts will be asked about potential mitigation strategies by focusing on what actions to take. This will be done in a semi-structured manner using open-ended questions. In this way, interviewer bias is countered [58]. The goal in this approach is to gain more knowledge and insights of these impacts in order for managers and policy makers to take appropriate steps and raise awareness. This aims to give the reader a comprehensive and holistic overview of potential negative impacts of QCC. It is therefore important to select subjects from different backgrounds to counter data bias.

Interview questions

The purpose of the interview is to elicit potential impacts of QCC on society. This is done by interviewing multiple experts from different fields in the industry, from academia and the government. This will be in place to strengthen and verify the systematic literature review to provide a holistic view on the matter at hand.

As the interviews will be semi-structured in nature, the main goal is to elicit negative impacts and the following questions can guide the interview:

- What are potential negative QCC impacts you anticipate?
- Why is this impact negative?
- What is the origin of this impact? What aspect of QCC allows this to be an impact?
- What are the societal consequences of this impact?
- How can we get a better understanding of these impacts?

4.4.2. Qualitative data analysis

The data analysis approach is based on the work of Miles and Huberman [59]. In this light, the interviews are recorded with permission of the interviewees. The recording is done utilising Microsoft Teams, which also allows for automatic transcription of the interview with timestamps. The transcription method of Microsoft Teams is a literal, denaturalised transcription of the audio, including uttering, mistakes and repetitions [60]. These denaturalised, or full verbatim, transcriptions are then compared to the audio file to correct and adjust mistakes made by the tool, while staying intelligent verbatim in order to elicit data. The reason for this choice is that potential verbal cues during the interviews, such as laughter or sobbing, are not deemed important in the context of the interviews, as the questions focus more on the expert knowledge of the researcher about the specific topic of QCC. However, the academic or industry background of the researcher is important to consider as this may affect the viewpoint on QCC impacts.

The data in the form of intelligent verbatim transcripts is then reduced in the form of descriptive inductive coding to synthesise empirically induced labels. These codes are revisited iteratively when more patterns can be found among the different interviews through thematic analysis [59]. Moreover, the interviews are conducted both in Dutch and English, depending on the preference of the interviewee. The Dutch interviews are analysed the same way as the English interviews are, and translated where needed to include in this report. This thematic analysis allows the data to be reduced and categorised to identify and analyse patterns to form theory [61]. The goal of the interviews is to get a more holistic view on potential negative QCC impacts and their implications on society. Found impacts from the data analysis process will be categorised to extract meta-data. These findings can then be displayed to give the reader an overview and to finally draw conclusions.

5
Results

5.1. QCC impacts in the literature

A limited set of different impacts are mentioned in the literature. These impacts are discussed in varying details among the different articles. Some impacts are analysed, where others are merely mentioned as possible concerns. To this extent, a distinction can be made between these impacts in terms of their origin. Some impacts stem directly from quantum technology itself, where others are a direct or indirect result of the application of the technology within a societal context. To make this distinction clearer and underline the difference between these categories, two new terms are introduced in this context: endogenous impacts and exogenous impacts. Endogenous impacts are impacts that are the result because of certain attributes and characteristics of quantum technology. Exogenous impacts are impacts that may occur because of the application of technology in a societal setting. With this important distinction in mind, the impacts will be introduced and explained around a central theme that characterises the impacts. The impacts are presented by means of a central theme they belong to.

Moreover, it should be noted that some impacts are portraying attributes of being both endogenous and exogenous and that the distinction is not always straightforward in this regard. This ambiguity is further discussed in chapter 6.

5.1.1. Endogenous quantum impacts

Quantum technology limitations

The theme of impacts around the topic of *quantum technology limitations* (10 out of 41 articles 24%) portrays various attributes of QT that may limit its potential, and could cause negative impacts. To start, quantum information has two characteristics that can form negative impacts. The no-cloning theorem of qubits portrays that unknown quantum states of qubits cannot be copied. Moreover, quantum states are characterised by complex numbers, called coherence, which is needed for the aforementioned quantum principles such as superposition and entanglement. Over time, quantum states can decohere because of environmental interactions, making these complex numbers probabilistic [62]. Hence, quantum states are unstable in nature [63]. This means that data in the form of quantum information is both fragile and unstable because it cannot be copied and stored [64]. Fragile data has negative impacts on privacy for individuals and this can harm trust of the users as well.

Furthermore, because of the stochastic attributes of quantum computing, there is no clear linear relationship between the input and output of a quantum system [62]. This results in *opacity* in which it is unclear why a certain outcome was given, based on a known input. This lack of transparency thus relates to the issue of accountability when unwanted consequences occur as a result. Moreover, qubits are characterised by the so-called ”measurement problem” [62]. When a qubit's data is extracted, the qubit is measured. This measurement results in the collapse of a qubit's wave function and gives a final observable state, meaning that the qubit's state is disrupted and altered upon measurement [62]. The wave function portrays how a qubit came into its state, and when the wave function collapses, this data is lost. This loss makes interpretation of processes and outcomes more difficult, resulting in a 'quantum black box' in which it is unclear how or why a result belongs to a certain measurement [62]. The difficulty in interpreting these results may cause a negative impact in explainable QCC applications.

A critical component of post-quantum communication comes in the form of quantum key distribution (QKD). Utilising qubits, a theoretically secure and random key is distributed between two parties intending to share data securely over an insecure channel [65]. With quantum properties, an eavesdropper in the channel can be detected, making the system more robust and secure. However, where QKD is in play to securely send information, it has some limitations and is susceptible to attacks as well [63]. QKD, like other quantum technologies, is still experimental with a *low technological readiness level* [66]. Qubits are currently susceptible to environmental noise and errors, making them unstable and requiring the need for extensive error-correction protocols [67]. Moreover, as qubits are represented in the form of quantum particles, such as photons, they suffer from loss at longer distances [63]. This loss results in QKD information leakage, posing a serious negative impact on its information security and allowing for side-channel attacks to occur [65]. The leakage of information is exponential by the distance over which the keys are distributed, severely limiting the physical range of application over which qubits can be sent [63]. Some solutions are given utilising satellite communication to allow for intercontinental transmission of keys [68]. However, in achieving this, there need to be space qualifications and standards for these technologies, which is a costly process in terms of time and money [68]. Similarly, integrating QKD in current networks proves to be a difficult task. As QKD is theoretically secure, potential attacks could focus on vulnerabilities on the side of the receiver or transmitter. This means that there needs to be profound security certifications on both hardware and software systems, again resulting in a costly and time-consuming process [63].

Error-correction for qubits is different in comparison to error correction for classical bits, as qubits cannot be copied per the no-cloning theorem [63]. The fragility of qubits and their decoherence time result in quick loss of information. In error-correction for qubits, the distinction is made between physical qubits and logical qubits. Physical qubits are qubits represented by a physical quantum particle. Logical qubits are formed by means of multiple physical qubits together [63]. In addition, these logical qubits are supplied with error correction codes, and this results in less fragility and a near-infinite coherence time, making them more resistant against environmental interactions [63]. However, one logical qubit may consist of up to 10,000 physical qubits in certain error correction protocols, making this technology not ready and mature yet [63]. These limitations make QKD and thus the future of post-quantum cryptography and the quantum Internet uncertain and unknown at this point in time.

Quantum-enhanced attacks are seen as a threat to current cryptosystems. Post-quantum cryptography is usually given as one of the solutions for different cryptography limitations of these legacy systems. However, although post-quantum cryptography can be a solution for mitigating specific quantum attacks, it has different limitations and shortcomings in countering other types of cyber attacks, such as side-channel attacks [69] and man-in-the-middle attacks [64]. Chowdhury *et al.* [69] provide a comprehensive analysis about cyber security vulnerabilities of post-quantum cryptography. One of the problems mentioned is that due to the relatively new post-quantum cryptography schemes, many vulnerabilities are not tested or evaluated, making the effects of post-quantum cryptography uncertain. This means that proposed solutions may not be completely fault tolerant and hype in addition to over-promising may lead to false expectations and neglectfulness. Svozil [64] calls these promises misleading and deceptive, as many quantum goals portrayed are based on strong assumptions. He argues therefore that it is not yet known what QT is fully capable of. Therefore, QT suffers from technology hype, over-promising and unknowns in terms of technological capability [64]. This technology hype is compared with the concept of threat inflation in which there is an exaggeration of a potential threat, usually with political ambitions in mind [70]. Both technology hype and threat inflation are characterised by uncertainty and over-promising, and this exaggeration of potentials can lead to undermining security threats.

Another potential negative impact that may occur is the advent of a new ”*data deluge*” once there is a way to store quantum data [62]. Quantum technologies and their applications may allow for the generation and collection of large amounts of data, providing new types of Big Data. To store, process and use this data, new and complex data centres need to be designed and built, posing a potential negative impact on the environment and natural surroundings [62].

Quantum illiteracy and organisational readiness

Quantum illiteracy (5 out of 41 articles; 12%) is a theme of impacts around the concept of QT being difficult to understand and hence leaving both researchers and society illiterate in quantum technologies. QT is being portrayed as enigmatic and this narrative of quantum mechanics being incomprehensible to both scientists and the rest of the citizens has as a result that it also limits public participation and discussions about the development of QT [71]. This has negative consequences on public engagement and limits participatory technology assessment. It is argued that illiteracy should be framed differently and that a discussion can be held about a technology and its applications, without in-depth knowledge about its inherent workings [72], [71]. However, including stakeholders by focusing on QT applications rather than why QT can achieve those applications, may result in a lack of trust within society because of the perceived illiteracy[71].

Quantum software engineering is inherently a challenging task. This has multiple reasons. First, quantum software programming is different to the traditional concept of programming [73]. Second, designing software architectures based on quantum systems proves to be complex [74]. Quantum hardware providers are currently still limited, and the different hardware platforms currently available utilise different software stacks and technologies for developers to use [74]. Moreover, quantum research develops fast, making it experimental and perpetually changing. The available platforms to developers change and evolve alongside these new discoveries [75]. This change of platforms happens multiple times a year [74]. Keeping track of new tools and technologies available to developers is thus costly and time-consuming. Third, there is a lack of both specialists in the workforce, and professors educating in quantum engineering fields [73].

Quantum software engineering has influence across various domains, spanning from computational science to cryptography. However, developing and understanding quantum software is faced with both uncertainty and complexity, making it difficult to anticipate and steer correctly [75]. The reason for this is that projects involving quantum software development usually deal with a fast-changing and evolving experimental climate [75]. As quantum research develops fast, it is stated that current platforms change with new discoveries multiple times a year [74]. Keeping track of new technologies and platforms takes time and is expensive. Moreover, designing quantum software architectures is complex because quantum hardware providers are limited and the available platforms offer different software stacks and technologies for developers to utilise [74]. Additionally, there is a lack of guidelines, frameworks and good practices on how to develop quality code and manage quantum software engineering [76]. To add to this problem, managing and running hybrid projects involving both classical- and quantum computing is a novel phenomenon and requires new techniques and expertise from different scientific fields [75].

These reasons may indicate a state of *low organisational readiness levels* for companies trying to anticipate and develop quantum software, or work towards hybrid systems. In addition, a *lack in standardisation* efforts of quantum hardware platforms facilitates this challenge.

A complete overview of endogenous impacts from the literature can be found in Figure 5.1.

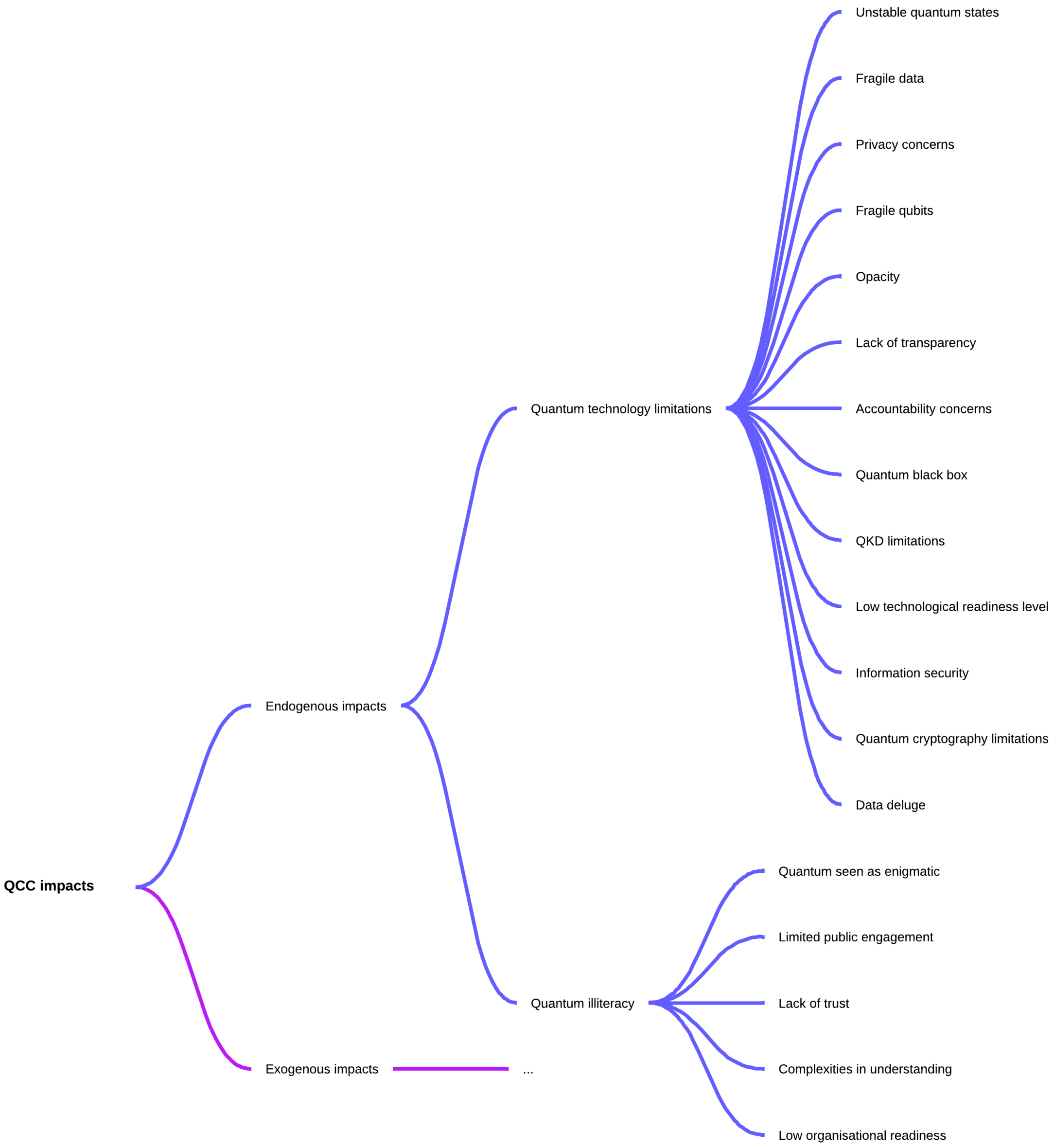


Figure 5.1: Overview of endogenous impacts from the literature

5.1.2. Exogenous quantum impacts

Post-quantum transition and standardisation

An extensive analysis of post-quantum cryptography (PQC) efforts is given by [77] and [78]. *Post-quantum transition and standardisation* (7 out of 41 article; 17%) is portrayed to be challenging and the development of post quantum cryptography is costly [79]. Furthermore, *standardisation* is a lengthy process that makes it more difficult [79]. This has multiple reasons. Incorporating and updating current systems with post-quantum security protocols is going to be a challenging and complex task because of the many different types of endpoints involved [80]. Moreover, QKD shows poor compatibility with existing network infrastructures [66].

Because of the anticipated cyber security threats and impacts, there is a large effort in the design and development of quantum-safe algorithms and protocols [77]. The National Institute of Standards and Technology (NIST) works since 2016 on different requirements of quantum safe algorithms and accepts public proposals. The American National Standards Institute has presented recommendations as far back as 2010. Furthermore, the Internet Engineering Task Force (IETF) works on different post-quantum Internet standards [77]. These efforts are portraying a lengthy process in the design and development of quantum-safe systems. Moreover, there are several challenges in the transition process to PQC when these standards and quantum-safe systems are ready.

Complete digital infrastructures are built on classical cryptography algorithms and protocols and migration to PQC is not a fast process. This is the reason scholars expect that there will be a transitionary period in which both classical and quantum systems are running in parallel [69]. This is a complex hybrid-system of algorithms and protocols with its own security problems and lack of standardisation [69].

Adding arguments to this expectation, legacy systems cannot be phased out and replaced immediately [76]. This has multiple reasons. These legacy systems are in place for a prolonged period of time. This comes with the consequence that these systems employ mission-critical knowledge, making it difficult and uncertain to replace completely [76]. Furthermore, quantum computing can have significant performance improvement in solving certain problems, whereas other problems do not require the usage of a quantum computer. This means that companies face a challenge in deciding which business processes are going to be run on quantum systems, and which on legacy systems [76]. These reasons mean that there will be a hybrid of systems in place in which quantum systems and legacy systems are working in parallel. This hybrid system is a new phenomenon and there is no specified methodology for adapting legacy systems to work with quantum systems in a hybrid architecture, and working towards this is uncertain and may proof to be challenging [76].

First, in the transition to PQC, the current cryptographic infrastructure of organisations needs substantial upgrades [77]. This means that different algorithms, company software and protocols may need adaptation or complete replacement to be made compatible with PQC. Consequently, the migration process will impose significant financial burdens and introduce serious complexity to organisations [77].

Second, the majority of potential PQC algorithms necessitate a larger key size in comparison with current cryptography algorithms. This results in encryption, decryption and message verification taking more time. The direct consequence of this is that more storage is needed in devices and establishing secure communication requires more time [77].

Third, PQC algorithms have more and stronger hardware requirements in terms of memory consumption and CPU cycles than classical cryptography algorithms require [77]. This especially becomes a problem on resource-constrained devices, such as Internet of Things devices, smart home sensors and smartphones [77]. Moreover, in the case of e-passports, the International Civil Aviation Organisation (ICAO) has design specifications and standards set for electronic travel documents [81]. Current post-quantum algorithms are not compliant with these ICAO specifications and standards. Moreover, the minimum chip requirement for electronic travel documents is 32 kilo bytes and no post-quantum certificate would fit on a 32 kilo byte chip [81]. This means that the ICAO has to work on adjusting their specifications and standards to allow for post-quantum cryptography implementations for electronic travel documents [81]. Furthermore, new electronic travel documents need to be shipped to all citizens, of any country, to prevent identity theft and fraud. The adoption and implementation of PQC thus requires flexibility and adjustability to run on these devices, while maintaining the security benefits. Hence there are feasibility issues regarding the implementation of PQC on devices [77]. These reasons make migration to PQC a global effort and it is a complex, time-consuming and financially heavy transition.

Cyber security

The most common theme of impacts mentioned in the literature is *cyber security* (34 of 41 articles; 83%). Impacts mentioned around this theme revolve around data security, information security and data privacy. The anticipated cyber security threats and dangers stem from Shor's algorithm for prime factorisation. Many modern day digital security mechanisms depend on a traditionally difficult mathematical problem to solve: factoring large prime numbers[82]. A quantum computer can, in theory, be used to solve specific mathematical problems that are classically known as infeasible-to-solve [83].

One of the main concerns of quantum computers is the cyber security threat introduced by breaking asymmetric cryptography by means of deploying Shor's algorithm [84]. Asymmetric encryption is build around generated public and private keys for encrypting and decrypting data, respectively [84]. This type of encryption is widely used nowadays. One example of this type would be the asymmetric Rivest, Shamir and Adleman (RSA) cryptosystem which is based on prime number factorisation. Factoring large prime numbers is classically a complex problem that requires a system to perform innumerable computations, making it too time-consuming and thus secure [62]. However, a quantum computer with a sufficient amount of qubits could compute the keys in a day and break these cryptosystems as a consequence [84]. ”Perhaps most disruptive is the impact on data security where in comparison to classical computers, quantum computers are capable of deciphering encryption codes in a fraction of the time.” [85]. This impact is also commonly referred to as the ”quantum threat” or ”breaking the Internet” as is anticipated by scholars [86], [67]. The RSA algorithm is important in the protection of data and the privacy of users. When RSA is broken, it portrays a big impact on information and communication security of society [77]. Grover’s algorithm can be used to perform brute-force attacks and break the Advanced Encryption Standard (AES) scheme [63]. Furthermore, cloud security is at stake because of these current cryptographic vulnerabilities [80]. Moreover, one of the direct consequences of the cryptography vulnerabilities as a result of the introduction of quantum computing, is the decreased durability and life-span of software in general [79]. he security impacts are ranging from military installations, governmental institutions, banks and electronic travel documents [81].

2048 bit RSA factorisation utilising Shor’s algorithm requires around 6200 qubits [63]. The most modern quantum computers have around 1,000 qubits in operation. Even though the negative impacts related to cyber security concerns seem to be a problem in the future once more powerful quantum computers are available, the threat is faced already today. A serious impact mentioned is a specific type of cyber attack called Harvest Now, Decrypt Later (HNDL) [82]. This attack has two steps in which encrypted data is acquired through various channels and is then stored until a sufficiently powerful quantum computer becomes available to the attacker. Utilising this quantum computer, the attacker can decrypt the acquired data, for example through the use of Shor’s algorithm, and subsequently access the acquired data. This has consequences for data that needs to be stored safely for decades, such as classified military documents and other governmental secrets [62], [82].

The timeline in which an organisation is transitioning to post-quantum cryptography, depends on three parameters [77]:

1. Migration Time (X Years): The number of years needed to develop, deploy and migrate to post-quantum cryptosystems.
2. Shelf-Life Time (Y Years): The number of years a cryptogrphic key is needed to remain confidential.
3. Threat Timeline (Z Years): The number of years before a powerful enough quantum computer can break current cryptosystems.

There is a cyber security problem when the Threat Timeline is shorter than the sum of Migration Time and Shelf-Life Time ($X + Y > Z$). In this case, the secret key is not confidential anymore, posing a threat to data security. The actual exact threat timeline is unknown and its prediction is not possible [77]. Hence, it is argued that companies are advised to migrate to post-quantum cryptography sooner rather than later. However, post-quantum cryptography algorithms are not resistant against side-channel attacks and their further resilience has not been studied and is currently not well understood [83].

QKD revolves around distributing a quantum key securely over a fiber network [87]. However, the distance over which this can be done is still limited. Quantum repeaters are in place to elongate this distance by transmitting the entangled state between a sender and receiver [88]. The quantum repeaters are having problems in their own right, such as stability issues and the ability to identify a repeater as trustworthy [88].

The cryptography vulnerabilities also extend to blockchain networks and their application [89]. ”The biggest impact of quantum computers on the blockchain is that hacker can easily utilise the defects of the traditional authentication to use the victim’s account to generate new transactions, which will have a devastating effect on the blockchain system” [89]. This means that the economy behind blockchain currencies would be compromised considering a malicious individual utilising a quantum computer could steal currency and commit fraud [89]. A solution to blockchain security is proposed by Zhang et *al.*, in the form of a post-quantum blockchain network over lattice [89]. However, the solution is theoretical and locally run and tested on simulations rather than a broad blockchain network with millions of active users.

When user data is not safely encrypted anymore, privacy issues emerge as a result [62], [72]. Some authors highlight the impacts on cloud security with implications on user data and privacy (e.g. Attribute-Based Encryption issues [90]). These impacts have profound consequences. When privacy is at stake and digital infrastructures are under threat of becoming vulnerable to attacks, a lack of trust and confidence in such infrastructures may emerge [91].

Furthermore, the impact of cyber security has several consequences throughout society as many systems depend on modern cryptography to function properly: blockchain networks and cryptocurrency markets, banks and the digital monetary systems, electronic passports, businesses and many other digital systems. The consequences of this are negative impacts in their own right: data privacy, trust issues stemming from this potential lack of data privacy, vulnerabilities of (industrial) IoT networks and defense systems, and the use of QCC for military purposes [86], [92], [85]. This shows that QCC can have a cascading effect of negative impacts influencing each other. Smart systems especially could pose security issues and privacy violations, impersonation and counterfeiting [92].

Unequal distribution of knowledge, power and wealth

There are various impacts mentioned belonging to the theme *unequal distribution of knowledge, power and wealth* (9 out of 41 articles; 22%). These impacts are mentioned in different contexts and will be highlighted here.

Within this theme, a potential impact mentioned is a change in the *global balance of power* once a country develops a quantum computer before other countries do [93]. Alongside academic efforts of quantum innovation, the United States has big corporations such as Microsoft and IBM working on QCC. The US is in direct competition with China [94]. Europe on the other hand is more focused on the academic efforts, while lacking the availability and innovative efforts of big corporations. This may result in an unequal distribution of knowledge, power and wealth in which one country, in theory, can decrypt encrypted communication and has a strategic advantage over other countries in this regard [72], [85]. This inequality also raises national security concerns [93]. Moreover, this *uneven access to the technology* can be extended within one country between government and civil society, or between businesses. When a government has access to a technology and its citizens do not, the balance of power between government and civil society grows larger and raises ethical concerns with regards to privacy and trust among the citizens [93].

When only certain individuals or companies have access to QT, negative impacts around fairness and equitable access may emerge [85]. Moreover, this extends to the equitable access to post-quantum cryptography and its transition. When some countries or companies are post-quantum ready, and other are not, it presents a clear divide and inequality [85].

New ideas and innovations are often protected and rewarded utilising intellectual property rights (IPRs). One mentioned potential negative impact is *overprotection of quantum technologies using IPRs* [95]. This overprotection could result in an anticompetitive environment in which innovation is hindered and market barriers are formed. The inability of acquiring a quantum computer, due to a lack of knowledge or financial resources, is likely to increase inequality within society [86]. First movers can strategically utilise a combination of IPRs which ”could result in an unlimited duration of global exclusive exploitation rights” [95]. In this case, it could allow for a winner-takes-all situation for first movers, characterised by unfair competition and market skewness [95]. On the other hand, IPRs could protect start-ups and their inventions in a high-tech environment by securing their inventions with patents and raise needed venture capital funds [95]. Internationally, China is the leading country with the most granted patents related to QT [72].

If only a limited group of companies has access to a quantum computer, it may increase inequalities because of the potential strategic advantages of a quantum computer. One of such advantages is the increased automation capabilities of various tasks enabled by quantum computing in certain industries [85]. This benefit to companies can have negative consequences for employees. In this light, certain authors mention the potential of job loss and employment instability due to this improved automation as a result of quantum computing, highlighting an increased unequal distribution of wealth (e.g., [85], [93]). Even though automation may result in job loss, the development and maintenance of quantum systems requires different types of skills and currently faces a scarcity in trained personnel [96]. This scarcity poses a significant challenge that could hinder both the growth and sustainability of the quantum technology industry [96]. A list of quantum technician skills and potential solutions for a shortage of workers is given by Hasanovic et *al.* [96].

Some authors call this distinction between the companies or countries that develop QT, and those that do not, the *quantum divide* [71]. This problem of unequal distribution and power imbalance is complex and has ties with the dual use characteristic of QT [72]. Because QT can be seen as a military technology, such as nuclear engineering, there is a lot of secrecy involved in the creation of knowledge. Sharing this knowledge is sensitive and ties into geo-political considerations, often bounded by export controls [97]. This has several consequences.

Even within a country, corporate espionage is mentioned which can result in the creation of unfair monopolies for companies owning quantum computers, while their competitors do not [97]. This can be extended to the application of QCC to organised crime, making fraud, hacking and theft more efficient and successful [97].

Additionally, when a country is increasing their safety with post-quantum cryptography to safeguard its systems from potential quantum attacks, some noteworthy remarks are made. Primarily, this proactive stance may imply an amplification of governmental authority, hence the government would be in a more powerful position than it currently is. This means that the existing power dynamics are altered. This governmental control concerns the privacy and autonomy of companies and citizens and potentially leading to a shift towards less transparent governmental activities [62]. Moreover, the decision-making process about the implementation of post-quantum cryptography systems needs more examination. When a government decides what is best for its citizens, without consulting them first, the negative impact of *paternalism* may occur and is highlighted in this context [62].

The narrative of the threat of quantum computing also has different consequences that feed the inequality impacts. When quantum computing is seen as a potential military weapon due to the cyber security threats, it might justify the exclusion of different stakeholders or countries in the debate [72]. Moreover, this prevents quantum computing in becoming democratised.

Dual-use technology and national security

The dual-use characteristic of quantum technology (7 out of 41 articles; 17%) highlights the potential dangers and threats this can bring in the form of *utilising quantum technology for military purposes* [97]. Many potential negative impacts are speculations in the anticipation and application of QT in the military domain. For example, utilising quantum technology, a new range of possible quantum attacks is available to the assailant, making this type of warfare different from conventional- or modern warfare [82]. Several authors call this usage of quantum technology with both military defensive and offensive purposes, Quantum Warfare: ”warfare that uses quantum technologies for military applications that affect intelligence, security and defence capabilities of all warfare domains, and it ushers in new military strategies, doctrines, scenarios and peace as well as ethics issues.” [63].

QT has the ability to enhance current military capabilities such as measurement, communication, sensing and computational power [63]. Utilising QCC for (defensive) space-borne systems is seen to have great potential. Applying quantum communication protocols such as QKD over a quantum network in satellite communication systems may provide secure channels for military communications during critical missions and deployments [82]. Another military application that is mentioned is quantum radar reconnaissance and with the help of quantum AI, the enormous amounts of generated data can be efficiently extracted and processed, providing detailed information to ground troops [84]. Furthermore, the application of Grover’s algorithm to improve military logistics and optimising routes, allowing for advanced navigation of military material on the battlefield, poses a strategic military advantage [84].

These examples of applications could indicate an unfair advantage between countries in the advent of quantum warfare. Moreover, this may result in an even wider imbalance of power globally [93].

The potential dual use QCC capabilities are of great concern with respect to several security threats to the critical information infrastructure of a country [98]. The aforementioned cyber security impacts have multiple military implications. Sensitive classified governmental and military data needs to remain safe and confidential for several decades [84]. This means that the HNDL attack is a big negative impact to be anticipated, and a problem that is currently faced by governments. Moreover, the financial sector is increasingly targeted by cyber attacks, making it the the most popular sector to attack digitally [84].

The literature speaks of a quantum arms race between the US and China, highlighting a geopolitical impact [70], [72]. In a counter to China’s quantum programs and investments, the US has invested in many quantum research and development programs. The Defense Advanced Research Projects Agency (DARPA) was tasked with several dual-use QCC projects, focusing on logical qubits, optimisation algorithms and quantum cryptanalysis [98]. Export controls are in place for some aspects of QT, limiting knowledge spillover to other countries and further reducing transparency. This has ethical consequences as well in which there are situations where foreign students and scholars are declined admission to quantum programs in certain Western universities [72]. Moreover, this militarisation of QT thus limits public discussions and wide stakeholder engagements to include different perspectives on the matter [72]. This can limit participatory TA efforts.

A complete overview of exogenous impacts derived from the literature can be found in figure 5.2.

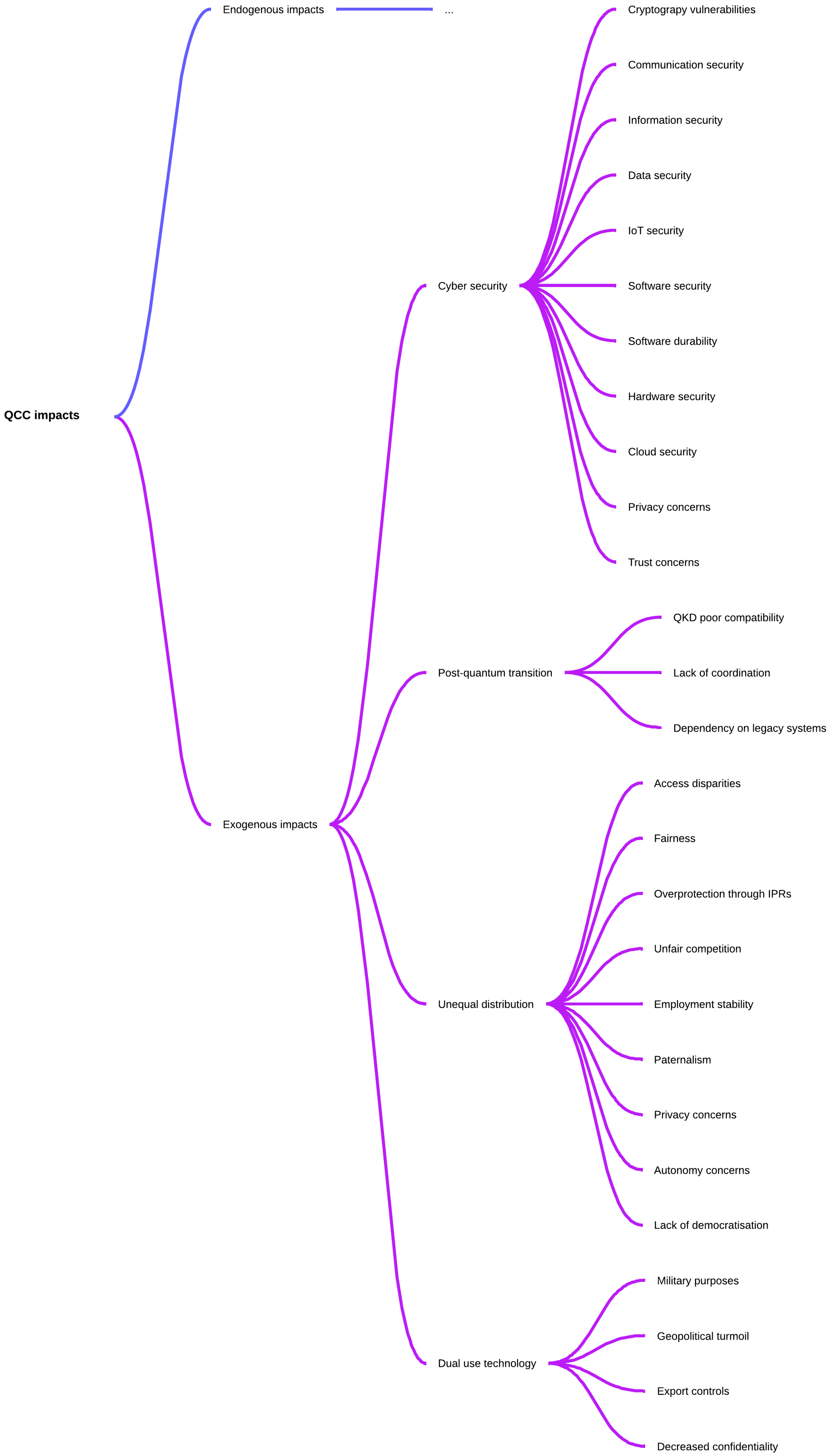


Figure 5.2: Exogenous impacts derived from the literature

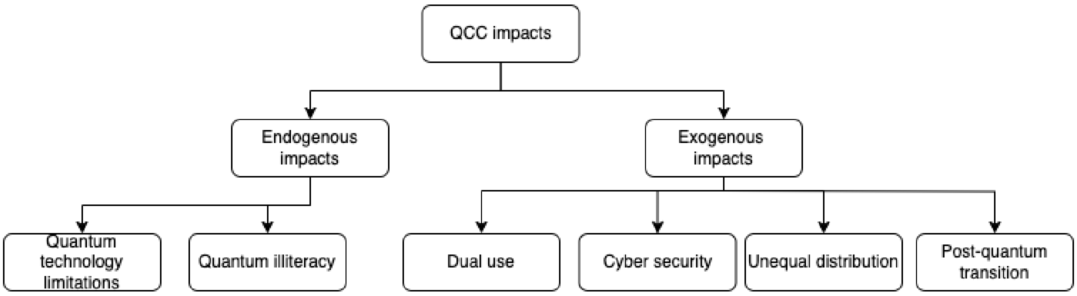


Figure 5.3: Overview of themes of impacts from the literature

An overview of derived themes from the literature can be found in Figure 5.3. The impacts are categorised on their endogenous or exogenous nature. Furthermore, an overview of the articles and the elucidated theme of impacts can be seen below in Table 5.1.

Table 5.1: Overview of articles and the theme of impacts from the literature

Theme	Reference
Quantum technology limitations	[62], [68], [63], [87], [88], [67], [69], [66], [65], [64]
Post-quantum transition	[77], [69], [81], [74], [76], [75], [73], [66], [80]
Cyber security	[62], [86], [82], [72], [85], [99], [90], [77], [96], [100], [101], [78], [102], [91], [68], [79], [92], [63], [83], [84], [87], [88], [98], [67], [103], [69], [70], [81], [89], [80], [65], [71], [64], [97]
Quantum illiteracy	[72], [85], [75], [73], [71]
Unequal distribution of knowledge, power and wealth	[62], [86], [72], [85], [99], [93], [96], [95], [71], [97]
Dual use technology	[82], [72], [63], [84], [98], [70]

5.2. QCC impacts anticipated by experts

The second step in the study is looking for impacts anticipated by experts within society. The semi-structured expert interviews provided an interesting set of additional impacts not found in the literature. Experts interviewed were from different professional and academic backgrounds, there is a clear distinction between the impacts mentioned by engineers, scientists and policy-advisers. The semi-structured interviews allowed for an interaction with participants on potential negative impacts they anticipate. To this extent, quantum illiteracy is the only endogenous theme that is derived. The rest of the themes are exogenous in nature.

5.2.1. Quantum illiteracy

Participant 5 mentions the lack of information as ”one of the main issues”. This lack of information ”comes hand in hand with misinformation and misguided hype” and it has as a result that ”citizens are not really informed about what this technology is and how it can potentially impact society”. Participant 4 mentions that technology hype can result in false promises. People are ”disappointed about the results”. Participant 6 mentions that “you often encounter slogans like ‘quantum computing will save the world’, or ‘a quantum computer will solve sustainability issues’”.. “You need to put enormous question marks behind such statements”. Although hype can lead to more funds for research and development, it can create false expectations and this can lead to “disappointment and an enormous withdrawal of financiers”. Moreover, hype can ignore negative impacts and people being affected. “Stakeholders are not being included” (Participant 6).

Participant 4 mentions that there is no need to fully grasp a technology in order to talk about it and form opinions on its anticipation. ”The danger is that people assume they can think about it when they know the applications of it”. This results in a perceived quantum illiteracy in which people assume they are illiterate on the topic to form opinions. Participant 5 says something similar in which ”it seems like it is a field that is completely inaccessible, because of course it is very complex and since the inception of the field of quantum mechanics and quantum theory, there has been a very strong discourse about how complex it is and how difficult to understand it is”. This has an intimidating effect on people thinking that the technology is too complicated to understand. Furthermore, the way quantum technology is presented in the media ”promotes a lot of misinformation and therefore people do not really know what to expect” (Participant 5). Nonetheless, quantum technology is a difficult and complicated technology that facilitates quantum illiteracy.

5.2.2. Cyber security

Cyber security is a recurring impact mentioned by most of the participants. This revolves around the ”impact on cryptography as it is used today” (Participant 2). This impact is ”the most concrete” because there is no expensive equipment needed to start working on assessing a company’s readiness level in terms of its cyber resistance with respect to quantum attacks (Participant 1).

It is expected that quantum computing will be predominantly done over the cloud. Potential negative impacts that are mentioned here revolve around how trustworthy data is in the cloud, and how confidential data will be (Participant 1). This is an extension of current issues within the cloud domain. This may have as a consequence trust issues among users as well as privacy impacts. Moreover, quantum computing may enhance AI models which can facilitate and strengthen different forms of cyber attacks, making it more difficult to protect a company and its data in the advent of an attack (Participant 1). Consequences of these cryptography vulnerabilities and cyber security concerns are banking security and financial certainty (Participant 1). Banks also rely on various cryptosystems to provide the services they offer to clients. When these systems are threatened by quantum-enhanced attacks, banking certainty and financial certainty might be difficult to guarantee as ”services to society” (Participant 1). Moreover, there are uncertainties about whether post quantum cryptography meets the industry security standards as solutions are new and complex (Participant 1).

The store now and decrypt attack later is mentioned by Participant 8 in which “there are currently groups that are collecting all kinds of information after which they can decrypt it in the future” once they have access to a quantum computer. This may result in “hurting the reputation” of the organisations from which data is decrypted.

Finally, classical cryptography may ”become completely unsafe” when quantum computers are constructed (Participant 8). The impact here is not necessarily the “massive breaches” of data, but more the “social response” and panic to this issue. This social response can result in panic.

5.2.3. Unequal distribution of knowledge, power and wealth

When quantum computing is done over the cloud in which a small set of companies facilitate this, other companies might be excluded from accessing quantum computing (Participant 1). Companies can be excluded based on the countries they are from. In this case, there is an unequal distribution of knowledge, power and wealth and this might result in unfair competition. Companies are also said to be in a state of ”fear of missing out” (Participant 1). If another competing company B has access to a quantum computer, company A might lack behind and miss business opportunities.

Participant 4 asks the question of who will own the technology. ”There is a chance that only big technology corporations and a few big countries will own it”. The benefits of QCC will then only be accessible to a select group of companies and countries. ”This is very bad for the development of the world and dangerous for the world order”. When a government is completely information-secure and no information leaks to the general public, there is a situation in which there exists an asymmetrical power distribution between a government and its citizens (Participant 5 and 7). This can be extended to governments among other governments, and companies among other companies (Participant 4). ”This can be very unhandy” (Participant 4). Participant 5 calls this ”asymmetrical knowledge access between citizens and their governments”. This asymmetry stems from the fact that QCC will be extremely resource intensive and expensive, resulting in most of the general population not having access to the technology.

Participant 7 mentions a similar notion. The power and resources to build a quantum computer are in the hands of corporations and large governments. “So it is unlikely that quantum computers will be consumer products.” This is because creating a quantum computer is resource intensive. With the various benefits and disrupting potential of QCC, there will be questions of power as big corporations will have the technology behind these disruptions. An example given is the potential to use quantum computing and simulation to model the folding of proteins to look for new molecules and potentially new types of drugs. This benefit could lead to a situation in which there is less competition and greater monopolies over drugs.

Participant 7 also mentions the issue of access to the technology. When a few corporations and governments own the technology, how is access going to be allocated? Who gets access? And who is excluded from this access? Some countries are being excluded by the IBM quantum program and they are not allowed to access quantum capabilities over the cloud. This is in stark contrast with current cloud offerings in which countries are not excluded from access. This is a form of closed innovation in which openness is limited. How can we make decisions on who to include or exclude? What is fair? A negative bias can be involved in these decisions (Participant 7). Quantum technologies are seen as critical technologies by the EU and this may impose further regulations and export controls around QCC. Moreover, technological sovereignty is at stake because of this. When a country cannot maintain ownership and sovereignty of components of the technology regarding its development or control, the country’s technological sovereignty is hindered (Participant 7).

As quantum technology has the ”potential to be extremely disruptive”, an unequal access to the technology might increase the already existing gap between the Global North and the Global South (Participant 5).

International collaboration is needed to make fundamental steps in the development of quantum hardware and software (Participant 6). However, the application of knowledge in this regard has national security concerns because of the disruptive capabilities of QCC and its dual use characteristic in the military domain as mentioned above. This means that protection of knowledge, intellectual property and export controls are being looked at (Participant 6).

5.2.4. Dual use technology

”When it comes to military uses of the technology for national defense, there is a lot of protectionism and a lot of secrecy about its potential applications”. (Participant 5). This national security aspect of the dual use characteristic of QCC ”contributes to not having open access and transparency” (Participant 5). This links to the cryptography vulnerabilities and the potential to decrypt state secrets. This results in ”hyper competitive climate for the development of the technology” (Participant 5). This is both on the geopolitical scale and on the corporate scale. Because of the race between countries and among companies, a form of innovation is introduced ”that is not always responsible” because of the urgency involved (Participant 5). Hence there is a tendency to overlook societal impacts as a result of this hyper competitive climate in which companies and governments want to be the first in acquiring a quantum computer.

Participant 8 mentions that quantum networks have the ability to send and receive data without an eavesdropper listening on the network. “So criminal organisations will be quick, when they have the possibility, to use quantum networks”. This is a negative impact for law enforcement agencies.

The negative impacts in its dual use are linked to the potential harm it may bring. “The development of weaponry that are unknown, the development of chemicals that are unknown, the development of viruses that are unknown” (Participant 8). Moreover, this potential development may be conducted in secrecy when using “blind quantum computing”. With blind quantum computing “you cannot go back and look what is developed”. This has to do with the fact that information does not remain when reading results after computation.

The malicious usage of QCC can be “existential in nature” (Participant 8). An example the participant gave was in the form of the development of a highly deadly virus or “the development of a quantum algorithm that could outperform financial markets”. Participant 8 mentions that “everything that you can do with it, will be done with it”.

5.2.5. Environmental impact

Components of quantum computers need to be ”close to absolute zero” in order to function properly (Participant 4). This means that a lot of energy is needed for quantum computers to run. Moreover, when this is going to be scaled, ”you have a situation in which there is an enormous increase in energy usage” (Participant 4). This however depends on the actual implementation of quantum computers (Participant 4). Participant 6 mentions that quantum computing has the possibility to run some calculations more efficient, which means that it is more sustainable. At the other hand, Participant 6 also mentions that quantum computers and their computing power can lead to a higher energy usage. “The superconducting variant of quantum computers needs to be cooled to absolute zero” (Participant 6). When multiple quantum computers are running simultaneously, this requires large amounts of energy.

Participant 7 mentions similar concerns that the energy usage of quantum computing is anticipated to be very high due to quantum computers being extremely power intensive.

Post-quantum encryption requires more computing power and thus more energy usage in comparison with current encryption techniques. “When you need to secure all the data traffic differently, you can make the calculations that it would require enormous amounts of energy” (Participant 6).

Finally, acquiring special metals and materials for the construction of quantum computers might pose negative impacts on the environment (Participant 4, 6 and 7). Participant 7 mentions that ”I do not want quantum to develop at all costs”.

5.2.6. Post-quantum transition

The transition to quantum-resistant cryptography is faced with uncertainty. It is not known when a quantum computer will come and be powerful enough to break cryptosystems currently in use. This leads to the following question: ”when do you need to be ready with your migration?” (Participant 2). Moreover, because of this uncertainty there is a sentiment that ”we have time enough” for the migration (Participant 2). It causes stakeholders to be reluctant with investing in quantum-resistant cryptography. This reluctance causes delay in migration efforts and delays investments for the transition. However, migrating to post-quantum cryptography is a complex endeavour that takes time and effort. First, fitting quantum-resistant cryptography into current existing infrastructures is difficult. The algorithms need to be ”applied to protocols” within the infrastructures (Participant 2). These protocols depend per business application and need for a company. Second, ”the implementation of an algorithm depends per hardware platform” (Participant 2). Different hardware platforms have different computing capabilities and might be constrained such as ”IoT devices” and ”legacy systems” (Participant 2). Moreover, ”some critical infrastructure” runs on legacy operating systems, making it difficult to incorporate quantum-resistant algorithms. Third, there is no coordination between companies in migration efforts. Multiple companies are working ”on their own solutions in their own domain”. This lack in coordination ”will drive up costs” (Participant 2). Moreover, migration and coordination are international efforts. ”The payment traffic does not stop at the Dutch border, and not at the European border” (Participant 2). It is unclear what central entity is going to take lead in the migration. This uncertainty creates a biding situation in which firms are not feeling the need to take the lead and are waiting for an entity to step up.

5.2.7. Enhancement of known impacts

Quantum technology has the ability to amplify known problems anticipated in other technologies such as AI (Participant 5). It could ”scale up outputs of machine learning algorithms” and hence making these algorithms more efficient. There are concerns regarding surveillance and its possible expansion through quantum technology. This is also a concern found in AI and “quantum can deepen and strengthen” (Participant 6) those concerns. Moreover, quantum communication can provide “more espionage possibilities” (Participant 6).

5.2.8. Unknown application areas

Unknowns of the potential of quantum computing is another theme of impacts that is mentioned by the interviewees. It is unknown whether quantum computers are capable of what is promised. Furthermore, it is unknown what the realisation of quantum computers will look like, or in what form they might diffuse in society (Participant 1). This also relates to unknowns about what laws and policy might change or restrict in the usage of QCC. Participant 3 said that the different complex quantum principles are portrayed to be ”badly translated into potential application areas”. The opportunities and applications of distinguishing features of QCC are unclear. ”Where are the application areas, where is it going to play a role?” (Participant 3). Participant 4 mentions the same thing in which there is currently a limited list of applications and it is difficult to think of more applications. Moreover, there is no need to utilise QCC for all business processes. Participant 3 said that he did not see any ’risks’ other than for modern cryptography, because we are not yet in a consumerisation phase.

5.2.9. Culture

Company culture and the culture of a country is mentioned as a negative impact in the anticipation and response to cyber security threats. It differs per company and country how assertive their culture is in making decisions and roll out solutions for future threats (Participant 1). Participant 1 said that there is predominantly ”a short-term focus” with companies, neglecting long term strategy. This indicates that culture is an enabling factor in cyber security readiness. Hence a predominant short-term focus underscores the negative impact of culture on this readiness. A complete overview of impacts derived from the interviews can be found in Figure 5.4.

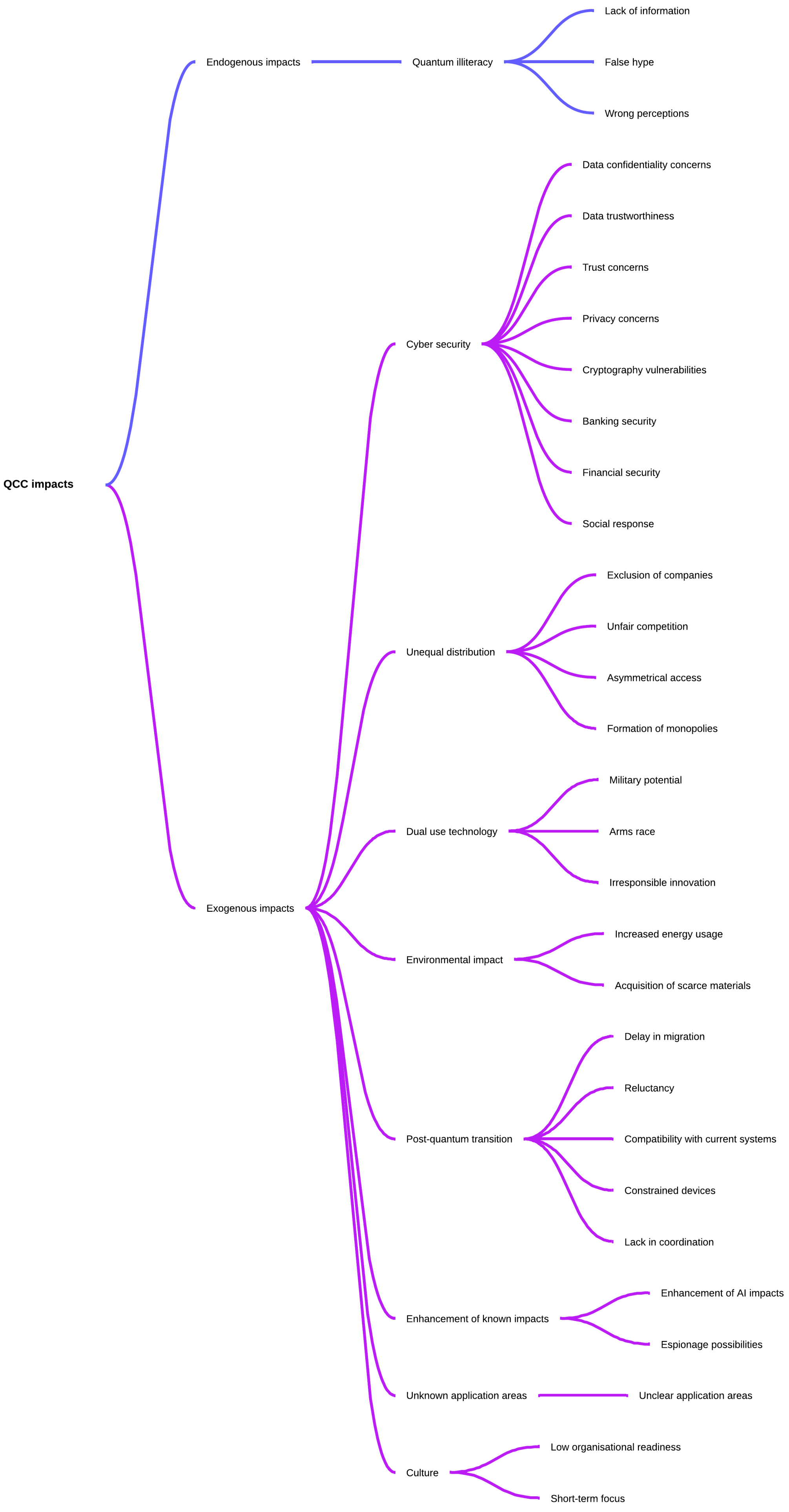


Figure 5.4: Overview of impacts derived from the interviews

Finally, an overview of the derived themes of impacts from the interviews can be found below in Figure 5.5.

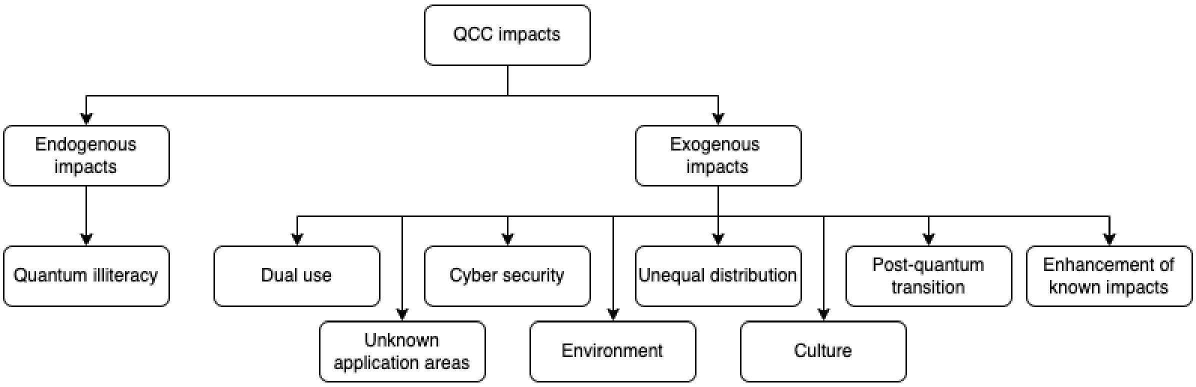


Figure 5.5: Overview of themes from the interviews

6

Discussion

6.1. Findings in brief

The objective of the research was to identify and understand potential negative impacts of QCC on society. Even though QCC has positive impacts and may be used to advance society into positive directions, the focus and emphasis of the study is solely on *negative* impacts. The reason for this can be traced to the Collingridge Dilemma. To reiterate, this dilemma states that the technology will be easy to steer in the beginning, but its potential side effects may be unknown. When the technology matures, and the side effects become known, it may be difficult to steer and alleviate the side effects effectively. Motivated by this dilemma, and given the fact that QCC is in its infancy stages, focusing on negative impacts may help society anticipate these impacts and prepare accordingly while there is still time. Moreover, examining these adverse effects may allow researchers to find root causes and develop effective mitigation strategies, promoting responsible innovation.

Subsequently, various potential negative impacts have been identified through a systematic literature review, followed by qualitative expert interviews. The impacts are categorised in themes based on their origin and effect within society. Moreover, a generic classification is presented based on known classification in combination with the new acquired insights of this study.

The included articles mentioned different impacts. However, these impacts are rarely explained in detail and often merely mentioned by the authors as a ”risk” that could emerge. Moreover, the distinction is made based upon the origin of the impacts. Endogenous impacts are impacts that are stemming from the quantum technology itself, while exogenous impacts are stemming from the application of quantum technology in a societal context. The findings of the study highlight distinct categories of impacts from QCC.

Under endogenous impacts fall impacts such as qubit instability due to environmental noise, resulting in data fragility and opacity in data interpretation. Additionally, the perceived quantum illiteracy present among stakeholders poses barriers to public participation, informed decision-making and general organisational readiness levels. This is further emphasised by the complexities in quantum software engineering and the fast pace of research developments.

Most found impacts fall under the category of exogenous QCC impacts. Cyber security is a prominent and recurring issue from both the interviews and the literature. Many impacts in this category stem from the current cryptography vulnerabilities, potentially leading to decreased security in cloud services, communication channels and software durability. This vulnerability comes from Shor’s algorithm and its ability to break mainstream cryptosystems such as RSA. Furthermore, challenges in the transition to quantum-safe cryptography are highlighted in both the literature and interviews. Difficulties in the integration of post-quantum systems into current existing infrastructures and the emergence of hybrid architectures belong in this category.

There are also concerns regarding the unequal distribution of knowledge, power and wealth due to restricted availability of QCC systems. Companies and governments with access to QCC may acquire an unfair strategic advantage. This may further increase the division of the global north and the global south, leading to an increased global imbalance of power and wealth. This imbalance is often refered to as the ’quantum divide’. Additionally, the dual use implications of QCC raises concerns with the military application potentially leading to geopolitical turmoil and limited stakeholder engagement due to secrecy. This potential military use for QCC results in a lot of secrecy around the topic. Moreover, it has a geopolitical impact as countries are actively trying to develop a quantum computer before others do. This can be extended to the corporate world as well. A quantum computer can have strategic advantages for a company, resulting in closed innovation practices. These aspects of secrecy, haste and closed innovation foster a situation in which responsible innovation is often overlooked. Furthermore, a lack of open innovation and cooperation between companies or governments, results in the absence of standards and further delays the post-quantum transition.

The interviews have identified additional impacts and challenges involved in QCC development and deployment. Noteworthy are the exogenous impacts of environment, culture and enhancement of known impacts of other technologies. Other than the indirect environmental effect of a potential data deluge, the literature does not highlight environmental impacts due to QCC. Several participants mention a direct environmental impact due to the increased energy demand of quantum computers. This could have significant environmental impacts because of higher power consumption. Moreover, the need for specific materials and metals is discussed as having a direct negative impact on the environment associated with mining and extraction of such scarce materials. Culture is mentioned as a negative impact in the anticipation and mitigation of cyber security threats linked to QCC. Cultural factors, such as short-term focus of organisations, hinders the anticipation and mitigation of these threats. A short-term focus neglects long-term strategy and leaves organisations vulnerable. Moreover, the ability of QCC to improve current technologies such as AI has as a result that it is also amplifying the impacts related to those technologies. The interviews complement the existing literature by highlighting additional exogenous impacts of QCC, particularly the environmental concerns, culture as an enabling factor for impacts and the amplification of known impacts of other technologies.

An overview of the total themes of impacts can be found in Figure 6.1. The themes that are exclusive to the interviews are highlighted in green, and the theme that is exclusive to the literature is highlighted in blue.

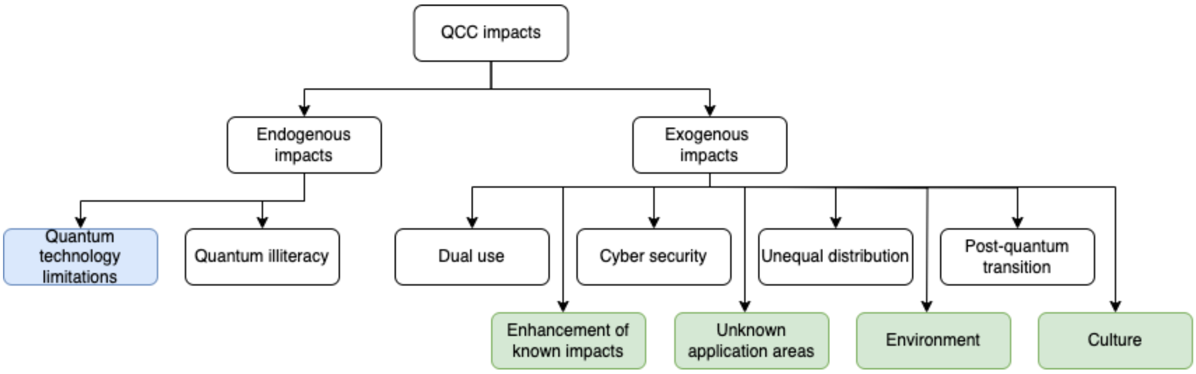


Figure 6.1: Complete overview of themes of impacts

Multiple categorisations of impacts and their respective themes were possible. The choice of making different distinctions of impacts in specific themes and labelling the themes as either exogenous or endogenous is based on making the findings actionable. This categorisation provides a clear overview of types of impacts anticipated within QCC applications in society. This way of portraying impacts addresses various dimensions by highlighting both specific impacts and providing a more high level overview of the general theme and origin of the impacts, being endogenous or exogenous. Moreover, this categorisation can be a valuable reference tool and provide a basis for policy advisers and managers to start and develop industry-specific roadmaps for mitigating the perceived impacts.

6.2. Ambiguity of QCC impacts

Although the distinction is made between endogenous and exogenous impacts, it should be stated that this distinction is not always binary, and impacts could be both endogenous and exogenous. This recognition that some impacts may portray attributes of both endogenous and exogenous origins adds a layer of complexity to the discussion of QCC impacts on society. To reiterate, the endogenous impacts stem from specific characteristics of quantum technology itself, while exogenous impacts stem from the application of the technology within a societal context. The distinction between exogenous and endogenous impacts provides a clear and useful framework for the categorisation of impacts. However, the outcomes might be more nuanced and interconnected.

To highlight this duality, the impact of quantum illiteracy is put forward. Quantum illiteracy is deliberately categorised as being an endogenous QCC impact. The reason for this categorisation is that the illiteracy stems from the complex nature of quantum physics and its attributes in the first place. This complexity causes a lack in understanding and thus an illiteracy on the topic. Moreover, the complexity in combination with the perceived illiteracy by society further causes a total illiteracy on QCC. However, quantum illiteracy can also be seen as a reaction of the application of the technology in a societal context, causing illiteracy to various stakeholders and individuals. This is further strengthened by the perceived illiteracy of society due to the framing of QCC. Hence, quantum illiteracy can be seen as both endogenous and exogenous.

When an impact possesses both endogenous and exogenous characteristics, it highlights that there is a dynamic interplay between quantum technology attributes and the societal applications of quantum technology. This means that effects cannot be solely attributed to either being originated from quantum attributes, or the societal application, but rather from the complex interaction between these two categories. This added layer of complexity highlights the reciprocal relation between technology and society. Technology shapes society, societal values and institutions. On the other hand, society also influences the development and deployment of technology. Thus the distinction of endogenous and exogenous is not always binary in essence, it however can play an important role in the effective identification and mitigation of the impacts. Hence, this study does make the distinction between endogenous impacts and exogenous impacts.

To continue, many found impacts portray an ambiguous picture of both positive- and negative aspects of QCC on society. It is noteworthy to comment on this and give some examples. QCC can cause several cyber security threats. On the other hand, it can also enhance cryptography and thus increase cyber security, making networks more secure and durable. This enhanced network security can then also cause negative impacts when criminals use the secured network for malicious activities without being caught by law enforcement. There is an interplay with positives and negatives, and society needs to decide what negatives it will allow. A knife can be very useful in the kitchen, however it can also be used for malicious ends. The question then arises whether a knife is a ’good’ or ’bad’ invention. Furthermore, QCC has the ability to enhance current technologies such as AI. This may bring unprecedented growth and innovation in various fields such as the medical world. However, it may also enhance the known negative impacts of such technologies, as is highlighted in the interviews.

6.3. Theoretical contribution

The insights of the results of the study will be discussed in this section. The focus of the literature is highlighted and compared with the data from the interviews. Furthermore, interrelations among impacts are discussed with an example, indicating that impacts are not independent.

6.3.1. Limited mitigation

Some scholars highlighted a specific security issue withing current cryptosystems and subsequently propose a quantum-resistant solution or scheme for a part of the issue (e.g., quantum permutation pad [100], blockchain-based system for Internet of Things security [101] and quantum walks-based encryption [92]). These solutions, identified within the literature, encompass a spectrum of protocols and algorithms designed to mitigate the weaknesses observed in existing cryptographic mechanisms. However, it is noteworthy to address that many of these proposed solutions are theoretical solutions only. Moreover, if the solutions are tested, it is often within controlled environments on virtual machines. Furthermore, these protocols and algorithms are predicated on theoretical models that usually rely on strong assumptions. This means that the translation from a laboratory setting to large-scale real-world implementations of such solutions portrays significant challenges and uncertainties that are currently not addressed. The effectiveness and feasibility of these provided solutions in practical scenarios remains uncertain and requires scrutiny and extended validation procedures.

6.3.2. Tunnel vision in anticipation: literature and interviews

The findings of the systematic literature review underscore the predominant focus on cyber security impacts of QCC. This suggests a notable disparity in the exploration of other potential negative impacts of QCC. The other themes of impacts are thus underexposed and under explored in the literature. This may indicate that the set of found identified impacts in the literature is non-exhaustive. The observed imbalance may come from multiple factors related to QCC developments. First, as the participants indicated in the interviews, this focus on cyber security might be because cyber security is the most concrete type of impact. You do not require expensive equipment to start working on the anticipation and effect of this impact on the firm, as it requires first an inventorisation of current cryptosystems in use and the vulnerabilities involved in a post-quantum sense. Second, cyber security poses strategic vulnerabilities to companies and governments. This may imply why most researchers and scholars cover this topic. In addition, the predominant focus on exogenous impacts of QCC from both the interviews and the literature suggests the emphasis on the anticipation of QCC and its interaction with society.

Although this focus is rational, it may pose several challenges and has some negative consequences. First, by only focusing and concentrating on cyber security impacts, scholars may overlook broader societal implications of QCC. For example, disruptions on the energy industry, supply chain industry and healthcare are underexposed. Neglecting these areas and the impacts of QCC in these industries, can lead to an incomplete view and limited understanding of holistic QCC impacts on society. Second, many impacts and values are merely mentioned by scholars, without in-depth explanations and discussion about their societal implications. Concerns about privacy, trust and the autonomy of individuals is often overlooked, indicating a lack of critical understanding of social and ethical implications of QCC impacts. Third, a focus mainly on cyber security impacts could lead to an inadequate preparedness for non-cyber security threats related to QCC that society may face. For example, financial instability and financial security may have profound consequences in society. Ignoring these aspects may leave society ill-prepared. Fourth, regulation requires profound and comprehensive research results in order to formulate and incorporate effective policies and regulations. A tunnel vision on cyber security impacts may steer regulatory frameworks towards an inadequate representation of broader challenges of QCC. This may leave society vulnerable to other consequences and it hinders adaptability of new and emerging technologies.

In contrast with the literature review, the expert interviews provided a more balanced set of insights on exogenous QCC impacts. To highlight an example, the potential impact of a data deluge, in which quantum data requires more and sophisticated data centres, is the only impact that is mentioned in the literature where the environment is indirectly affected by QCC. On the contrary to the absence of real environmental impacts in the literature, the interviews provide a more elaborated view on environmental impacts by QCC. Several interviewees highlighted direct environmental impacts due to QCC and its inherent workings. In particular, the concern highlighted arises from the superconducting variant of quantum processors, which requires extreme cooling to near-absolute zero temperatures. Moreover, the energy-intensive nature of quantum computers in addition to the concurrent operation of multiple parallel quantum systems exacerbates these concerns. This results in serious negative environmental impacts. Furthermore, deploying and running post-quantum encryption algorithms throughout various systems in the current information infrastructure of countries requires an increased amount of computing power, further intensifying energy demands. Additionally, the construction of quantum computers will require special metals and the mining of such metals might cause a negative impact on the environment.

The recognition of a non-exhaustive set of impacts from the literature, in combination with the relative small sample size in this study, indicates that the total list of found negative impacts is incomplete. While the interviews provide valuable insights and perspectives from different stakeholders and experts, the sample size may not represent the viewpoints within the broader population. As such, the set of negative impacts derived from the interviews may be limited and may not be exhaustive either. The literature mentioned the impact of quantum technology limitations, while the interviews did not. The incompleteness of the found negative impacts underscores the importance of an iterative approach to studying QCC impacts on society. Future research could focus on an expanded scope, incorporate a larger sample size and engage with a broader range of stakeholders to get a more comprehensive understanding of QCC impacts.

6.3.3. Interrelations among impacts

One interesting observation is that several impacts have complex interrelations among each other. Instead of being isolated, a single impact can serve as a catalyst, allowing several other impacts to occur. This may cause a cascading effect of impacts within society. Moreover, this indicates that the found impacts are not all mutually exclusive.

To highlight an example, the identified cyber security impacts seem to form a hierarchy and dependency in which some impacts facilitate the occurrence of others. Most cyber security impacts stem from current cryptography vulnerabilities. These vulnerabilities enable the occurrence of various other negative impacts, such as breaches of sensitive data or the compromise of digital privacy. These breaches, in turn, may lead to a loss of public trust in digital technologies, and may undermine the confidence in the security of online transactions. Subsequently, this lack of trust can further exacerbate societal concerns and may potentially hinder the adoption of new digital technologies.

Moreover, the interrelations and overlap of impacts are also horizontal. An example is the theme of dual use impacts, portraying a military application of QCC in warfare domains. This dual use is partially facilitated by the cyber security applications of QCC and the integration of cyber security in the military. So although the themes are important to highlight and distinguish into categories, there is overlap throughout and the themes are not independent from each other.

The interconnectedness of societal impacts thus has profound implications for practical and managerial strategies. It highlights the importance of addressing and analysing the root cause, such as cryptography vulnerabilities, to mitigate these impacts. By understanding such relationships, stakeholders can develop approaches to safeguard societal values and mitigate negative impacts accordingly.

An illustrative depiction of the hierarchical structure of cyber security impacts can be seen in Figure 6.2. The cascading effects of cryptography vulnerabilities, portrayed in red as the rood cause, on societal values, portrayed in green, are highlighted here.

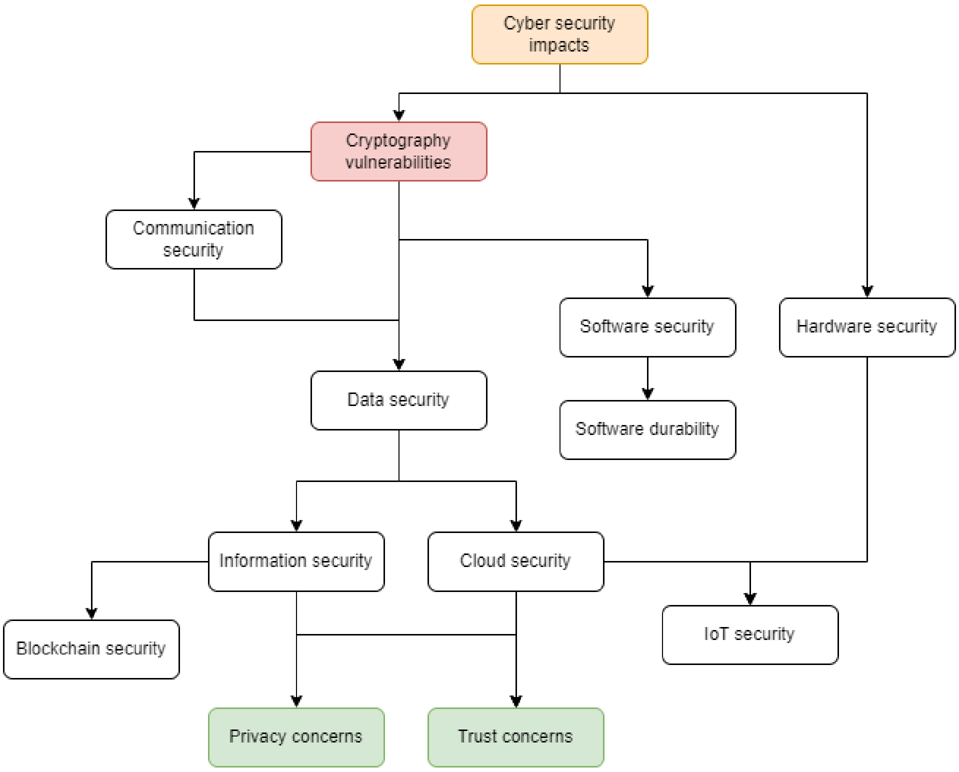


Figure 6.2: An overview of cyber security impacts and their relations

6.4. Practical and managerial implications

Even though the distinction between exogenous impacts and endogenous impacts looks trivial, it is not binary in essence. However, the distinction important to highlight here for a comprehensive understanding of the societal impacts of QCC. This distinction has several practical implications. First, it underscores the need for unique and tailored approaches in addressing and mitigating different types of impacts. For instance, solving the issue of opacity requires a different mitigation strategy in comparison with impacts linked to the dual use characteristic of QCC. The former may involve advancements in quantum memory technology, while the latter may involve regulatory frameworks and policies to govern the application of QCC within society. Second, the recognition of this distinction allows for a more nuanced understanding of the socio-technical advancements. Stakeholders can differentiate between negative impacts and positive impacts stemming from both the technology itself, and its application in society. Third, the distinction emphasises the complex interaction between technological innovation and societal application. It highlights the interplay of societal norms, values and governance frameworks shape the advancements of QCC, while QCC influences societal practices and institutions at play. It can thus guide the development of more precise policies in the mitigation of negative impacts.

6.4.1. QCC and its distinguishing features

A distinguishing feature of QCC impacts and impacts of other nascent technologies such as nanobiology and AI, is the fact that QCC requires a structural change in critical (digital) infrastructures society is revolved around currently. This structural change comes in the form of a transition into post-quantum systems to mitigate various cyber security concerns of current cryptosystems in use. This means that the current systems need to be made compatible with quantum systems. Moreover, this change has a time dimension linked to it. It is uncertain when a powerful enough quantum computer will be built that could break current cryptosystems. However, once such a computer comes into existence, the current systems need to be transitioned to mitigate the potential negative impacts. The current lack of standards and QCC security certifications makes this transition more difficult. Where the cyber security vulnerabilities may result in privacy violations and therefore a decreased public trust in digital systems, the introduction of standards and certifications may have positive effects with regards to privacy concerns and public trust. Moreover, as business processes may depend on legacy systems, in addition to processes not requiring quantum capabilities, there will be a situation in which both legacy systems and quantum systems work in parallel. This in turn is a novel problem, requiring different security measures and standards for a safe and sound infrastructure.

To continue, another distinguishing feature is the hybridisation of technologies. Current systems cannot be replaced altogether due to business processes running on various legacy systems and the dependability of the current critical information infrastructure. Moreover, it is not a given that quantum computers will replace classical computers entirely. On the contrary, as quantum computing is an expensive and resource-intensive technology, there will be a long-term phase in which both classical systems and quantum systems will run in parallel. This in term comes with several new challenges and uncertainties that need to be addressed and mitigated.

Furthermore, the capacity of QCC to enhance current technologies and amplify their known impacts makes QCC different from other nascent technologies. Unlike other technologies, QCC does not operate and evolve in isolation. It integrates with other technologies and augments the capabilities of these technologies, such as AI and cyber security protocols. This integration and augmentation leads to a scenario in which QCC introduces its own novel set of impacts, and on also amplifies and extends existing technological impacts. Particularly AI technology, as QCC can enhance the processing power and computational efficiency of AI systems, leading to more complex problem solving and processing of large amounts of data. However, this capability amplifies the potential negative societal impacts associated with AI, such as data privacy, algorithmic bias and the ethics of autonomous decision-making. Hence, QCC not only comes with its own set of new impacts, it enhances current known impacts of other technologies and influences the broader technological landscape. This interconnectedness indicates that it is important to study the role of QCC in amplifying the known impacts of other technologies. By understanding this interplay, policymakers, researchers and stakeholders can anticipate and mitigate these broader impacts.

6.4.2. A classification of QCC impacts

Based on Stirling's uncertainty matrix in figure 3.1 and the aforementioned definition of risk in section 3.2 and the previous sections, *risks* are not found in this study. The negative impacts all fall under a combination of uncertainty and ignorance, where some impacts also portray signs of ambiguities. The found impacts have characteristics of both uncertainty and ignorance for a couple reasons. First, there are some known probable aspects of the found impacts and at the same time many unknown possibilities. Second, many unknowns persist in the literature and among experts. As the interviews highlighted, there are unknown application areas of quantum computing, highlighting a state of ignorance. Moreover, as was argued by [48], uncertainty comes from complexity and the combination of uncertain outcomes and complex problems allow for ambiguity. Potential QCC impacts are also characterised by complexity. Both because of the often incomprehensible nature of quantum theory and the inter-dependencies of various actors involved in society. Moreover, the knowledge about outcomes is uncertain and it portrays different values to different stakeholders. Quantum communication can be seen as a means to safeguard national security in the eyes of the government, but it can be seen as a negative impact in the eyes of citizens with respect to autonomy, privacy and trust.

Following the categorisation of the found impacts in their respective themes, classifying the impacts may be of beneficial value to managers and policy advisers. Utilising the known classifications, further insights can be found on the distinction between QCC and other technologies. Moreover, a classification allows for a structured and systematic approach in interpreting and understanding these impacts. In this light, the discussed classifications of chapter 3.2 provided a limited overview of found QCC impacts. The categories do not cover all found impacts of this study. Some impacts can be classified accordingly, while others fall short within the provided explanations. This can be explained by the distinguishing features of QCC in comparison with other technologies. Therefore, a new classification framework is proposed and elucidated, combining the existing knowledge of classifications and the novel results and insights of this study:

- Unequal distribution of knowledge, power and wealth
- Privacy
- Trust
- Autonomy
- Sustainability
- Geopolitics and international relations
- Cyber security
- Dual use potential
- Technology limitations
- Organisational readiness
- Infrastructural fit

This framework is framed to not be limited to QCC specifically, but in a way that it can be used to assess new and emerging technologies in general. Noteworthy inclusions are the following. First, technology limitations portray specific limitations of an emerging technology that could form potential negative impacts on society. In assessing this, new standards need to be worked on in order to mitigate impacts. Second, organisational readiness highlights the need for assessing whether the organisation is ready to 1) incorporate the technology into its business processes, 2) have a capable workforce able to work with the technology, and 3) have the capacity to potentially protect the organisation from perceived threats of a new technology. Step 3 can mean that an organisation needs to have the capacity to migrate to new systems in anticipation of threats. Third, infrastructural fit emphasises the need to assess whether existing infrastructures, be it physical or digital, are compatible with the incumbent technology.

It should be noted that the classifications are not mutually exclusive. On the contrary, as is seen by the analysis of the found QCC impacts, different impacts may depend on each other and allow other impacts to occur. This means that some items in the framework may have overlapping impacts. This is recognised and yet it is deemed important to make the distinction between impacts in the different categories as the suitable mitigation strategy may be different. In the case of QCC, cyber security impacts may cause privacy and trust issues within society. Moreover, cyber security impacts also concern the dual use characteristic of technologies in a digital-driven world. The ethics of personal privacy are different with respect to the ethics of the military application of technology, and the mitigation of these impacts requires different types of strategies and it involves different stakeholders.

6.4.3. Culture as a confounding factor

The interviews indicated that company culture has a significant impact on the anticipation of cyber security threats. This role of company culture, and to a broader extent the culture of a country, plays a crucial role in the anticipation and mitigation of cyber security threats. This has negative impacts on how companies perceive, prioritise and respond to cyber security threats coming from QCC breakthroughs.

Company culture plays an important role in the agility of solutions. The mindset of a company to be proactive can significantly influence the ability to anticipate and mitigate these threats. The interviews indicated that many companies employ a short-term focus wherein long-term strategic considerations are often dismissed. This short-term vision can undermine mitigation efforts to establish cyber security frameworks and protocols, leaving organisations vulnerable to threats and vulnerabilities. Furthermore, this line of reasoning extents to governments and countries in general. When a country has cultural traits such as risk aversion and assertiveness, it can influence how governments and regulatory bodies collaborate and coordinate migration efforts. Countries with a bureaucratic culture may find it difficult to implement cyber security measures considering potential regulatory routes to take. This underscores the importance of company culture, national culture and the interplay between the two. Understanding and recognising cultural dynamics is therefore important for the development of effective mitigation strategies of QCC cyber security impacts.

Apart from responsiveness to cyber security threats, a company's cultural impacts extend to the lack of coordinated migration efforts and post-quantum transition initiatives in mitigating these threats. The presence of uncertainty with regards to the timing in which a powerful quantum computer will be built, allows for a sense of ambivalence among stakeholders. The critical question of when organisations need to be ready with their post-quantum migration is facilitated by this uncertainty. As Participant 2 mentioned, the prevailing sentiment of ”we have time enough” persists within society. This sentiment facilitates the absence of coordination and central authority in addressing the threats, resulting in a lack of investments in post-quantum systems. This delaying of investments and postponement of migration efforts creates a cycle of procrastination within organisations.

The migration is a costly and complex endeavour. Organisations that are dependent on traditional systems may be reluctant to adopt new post-quantum systems. This can come from a culture that prioritises stability over innovation. Furthermore, the lack of central authority and coordination at the national level heightens these challenges. The absence of clear frameworks, standards and policy may take away organisations' incentives to prioritise post-quantum transition. The decentralised decision-making, in addition to the absence of clear unified standards, results in a fragmented approach in which organisations work on the migration in isolation. This, in term, results in inefficiencies that drive up costs. Moreover, migration efforts are not a national concern, but an international effort in mitigating negative impacts. International collaboration and coordination is essential in critical sectors such as international payment traffic.

To continue, the current state of companies and their hesitancy in migration efforts may indicate a low organisational readiness level. Moreover, the problems and difficulties associated with quantum software engineering, and its fast-changing environment, make it difficult for companies to navigate through. Moreover, developing, implementing, testing and integrating quantum-resistant protocols into existing cryptographic protocols is challenging and requires specialised knowledge and skills that may be absent in the workforce of many organisations. This challenge may be further increased by the perceived quantum illiteracy due to QT being portrayed as being enigmatic and esoteric. Although QCC is a complex topic, stakeholders may believe the technology is too complicated to understand for non-experts. This perceived illiteracy in combination with misinformation about QCC facilitates uninformed stakeholders on the topic.

To address these challenges and foster organisational readiness on the topic of QCC and PQC adoption, a pragmatic approach is encouraged in which companies view QCC as a corporate resource with various benefits and opportunities, rather than a complex theoretical phenomenon. The potential negative impacts need to be highlighted to raise awareness. In this way, organisations can stimulate a more inclusive and attainable understanding among various stakeholders.

In addition, companies are advised to incorporate programs in which the workforce becomes familiar with basic use cases and workings of QCC to become familiar with the application in their respective industries. Incorporating such training programs and workshops can help employees and stakeholders to engage more efficiently and effectively with QCC opportunities and impacts. Furthermore, encouraging a culture of curiosity, continuous learning and open innovation can facilitate a proactive approach in dealing with challenges of QCC. Moreover, fostering cross-sectional collaboration and knowledge-sharing initiatives can allow technical experts and non-technical stakeholders to engage in informed decision-making procedures and the formation of strategy.

However, while culture can be seen as a factor in facilitating negative impacts, it should be noted that company culture can also be changed by the emerging technology itself. As QCC enfolds into society and portrays to be disruptive, it may require adjustments to incumbent cultures of organisations, as the ones suggested above. These adjustments and changes to the culture can facilitate the emergence of an entire new culture within the organisation. From the way employees engage new problems to the routines and interactions with other departments. Hence, technology and culture can have a reciprocal effect on each other and influence each other. This change of culture is thus an exogenous impact of the technology on the firm itself.

6.5. Preliminary mitigation strategies and recommendations

Now that the found impacts are listed and categorised, and a classification of impacts is given, the next steps are taking action in order to mitigate the negative impacts and take advantage of the positive impacts of QCC. In this section, an initial, preliminary set of mitigation strategies is given on a subset of the found impacts.

Security audits

The profound cyber security impacts of QCC extend beyond the technical vulnerabilities to consequences on privacy and trust as human values. To try and counter and mitigate these impacts, companies should start to conduct regular security audits. QCC is changing and developing fast. Hence, the impact on current systems may change overnight. Conducting security audits helps companies check whether the security measures in place are still effective in mitigating the evolving threat posed by QCC. Moreover, by regularly assessing the current cycber security posture, companies can identify vulnerabilities in their systems and take proactive countermeasures to address them before exploitation by malicious users occurs. This involves not only assessing the technical robustness and security of the systems, but also evaluating whether organisational policies, employee training programs and incident response protocols are still effective in relation to QCC threats.

Agility in response

As new vulnerabilities and attack vectors come to light, companies are advised to remain agile and responsive in their security efforts. This agility requires investments in research and development departments, or the inclusion of third parties in collaboration with cyber security experts. Organisations should focus on facilitating an assertive culture, allowing for anticipation of impacts and long-term strategy. Fostering an open innovation culture can allow for stakeholder engagement and informed decision-making on QCC anticipation and strategy. Participation in information-sharing networks in order to stay up-to-date with the latest developments is also advised. In this light, a collaboration with a university department could help foster this. Moreover, companies should prioritise transparency with stakeholders regarding the cyber security practices and measures. Having an open conversation about handling and protecting data results in trust among partners, customers and the public, especially when companies deal with sensitive, private information.

Awareness and education

To counter quantum illiteracy at companies, the following mitigation strategy can be used. First awareness needs to be created among staff members, management and relevant stakeholders. QCC is an emerging technology with various positive impacts and opportunities, however, it may also bring about negative impacts. Moreover, training programs and lectures should be organised and developed to teach staff and stakeholders about QCC. This does not necessarily involve delving into quantum physics, but a mere explanation that QCC is a technology that has both positive and negative implications to companies.

An example lecture program may include:

- An introduction to emerging technologies and their characteristics
- Quantum technology as a tool to accomplish tasks in society
- The negative consequences and potential harm

These topics are essential because emerging technologies share characteristics and they show patterns of diffusion throughout society. These patterns can also be found within QCC. With this, stakeholders can have a more realistic and nuanced view on QCC. Highlighting then the positive and negative impacts is essential to give the stakeholders a complete view of positives and negatives of the technology so that they can form their own opinion on the matter.

This program could be given in a seminar form in which a seminar takes place once a week for three weeks long, encompassing these topics to give stakeholders more knowledge on the topic, with the goal of eliminating the perceived quantum illiteracy. A lecture should not take more than one hour. Afterwards, the audience can ask questions and raise concerns they may have.

Global mandates and regulations

The European Union AI act, proposed by the European Commission, is the first attempt to regulate the usage of AI systems in society. It gives a comprehensive regulatory framework for AI technologies in the EU to facilitate responsible development and deployment of AI technologies [104]. With QCC still in its early stages, a similar regulatory framework could guide the development of QCC and facilitate a responsible deployment of the technology. In comparison with the AI act, utilising the formed categorisation of this study, in addition to the proposed classification framework of QCC impacts, a regulatory framework can be formed on the usage of QCC. It is advised for policymakers to focus on the distinguishing features of QCC in relation to other nascent technologies. Moreover, a board can be formed in order to oversee the enforcement of the regulations their implementations. This board can be coordinate with governments, central banks and other national supervisory authorities to ensure compliance with the regulations.

6.6. Limitations

Several limitations have been identified in this study. First, this study was carried out by one person. This means that the collection and interpretation of data, both from the systematic literature review and the semi-structured expert interviews, could be subjective and pose bias problems. This can be solved by performing the coding process of the interviews with two or more people to allow for peer reviewing. The coding process in that case is done individually after which the codes and themes are compared. Even though this takes more time, it would counter bias problems in future research. This however is not within the given time-frame of the study, and would require more resources.

Second, the sample size for the interviews is eight. Even though there is a limited amount of experts on the field of QCC, it is still a relatively small sample size. A small sample size may not represent the broader population of the study. This may result in a limited generalisability of the findings. However, this was countered to an extent by including a diverse set of participants ranging from academia, the government and the industry. Moreover, the interviews were an addition to the systematic literature review, in order to gain more insights into the potential negative impacts of QCC on society.

Third, to continue on the interviews, the sample was limited to experts in the Netherlands only. This presents a geographical limitation and may result in a regional bias in which the given perspectives are limited to anticipated impacts present locally. The problem of overgeneralising findings based on a small sample size is recognised and it is thus advised that future research will perform similar studies on a variety of different industry fields, including multiple stakeholders. However, the research employed a mixed-research strategy. The systematic literature review in combination with the semi-structured interviews does allow for generalising and comparing the academic literature with expert opinions from society. Moreover, it would be interesting to see workshop studies conducted on this topic, allowing participants to discuss among each other on QCC impacts.

Fourth, the sole focus on Scopus as a research database could exclude other relevant literature. As the literature review was systematically carried out, grey literature from various sources was not included in this study. Although this increases reproducibility of the study, this may also imply that a great deal of known knowledge is not covered by this study. Hence, the list of found impacts may not be exhaustive. It is advised that future research will include other search engines such as Web of Science and analyse grey literature on the topic of societal QCC impacts.

6.7. Future research

QCC is an emerging topic and its impacts on society are found to be underexplored in the literature. Moreover, this underexposure of impacts within the literature poses ample opportunities for future research directions. Some preliminary research directions are proposed here to deal with anticipated impacts, and get a deeper understanding of these impacts.

A continuation of this study

The results of this study show that the focus of current literature is predominantly on cyber security impacts. Moreover, the relative small sample size of the participants may have also resulted in a limited set of impacts from the interviews. This indicates that there is more room for researchers to conduct a similar research on the societal impacts of QCC, utilising different research methods. Future research could focus on exploring specific impacts that received less attention in existing literature. For example, investigating environmental impacts of QCC could give insights into energy consumption, resource utilisation and the carbon footprint associated with quantum computing. Different stakeholders from the defense industry could be interviewed to further investigate the dual use potential of QCC. Moreover, workshops could be organised among experts in society to allow discussions on impacts. There are many directions to take as the literature is still scarce. Examples of research questions could be:

- What are potential environmental impacts of quantum computing?
- What are the ethical implications of dual use scenarios in QCC?
- How can policymakers promote innovation while safeguarding against potential misuse of QCC?

QCC impacts per industry sector

This study has focused on the societal impacts of QCC. However, impacts may differ significantly across different industry sectors. By zooming in on specific industries and conducting sector-specific evaluations, researchers can gain a more comprehensive understanding of how QCC technologies are reshaping various sectors and uncover more nuanced insights that may not be apparent at a broader societal level. Multiple industry-specific experts could be interviewed followed by workshops to form theory. Examples of research questions could be:

- What are potential impacts of QCC on the financial sector?
- What are potential impacts of QCC on the defence industry?
- What are potential impacts of QCC on the supply chain industry?

Economic impact analysis

Several found impacts may impose significant socioeconomic disruptions. One notable example is the potential of job displacement resulting from the improved automation by means of quantum computing. While quantum computing can promise enhanced efficiency for corporations and driving innovation across industries, the unequal accessibility and potential workforce disruptions might necessitate further examination and measures to mitigate these effects on firms.

Furthermore, the unequal distribution of the technology and the high cost involved regarding R&D of QCC means that some companies can form monopolies around QCC and its services in certain industries. Additionally, the aggressive race to the acquisition of patents can may further facilitate this concentration of power and influence among a select group of companies. Potential research questions may be:

- How does the adoption of quantum computing technologies affect employment dynamics across various industries, and what strategies can be implemented to mitigate potential job displacement?
- What ethical considerations arise from the automation potential of quantum computing, and how can ethical frameworks be developed to guide responsible deployment and use of quantum technologies in the workplace?
- What role do patent policies and intellectual property rights play in shaping the landscape of quantum technology development?

Mitigation and prevention of negative impacts

Following the identified negative impacts of QCC on society, the next step in research is to formulate targeted mitigation strategies top address these identified impacts. A deeper exploration into feasible and effective mitigation approaches is needed. While preventing impacts entirely may be challenging given the complex nature of QCC in society, proactive mitigation efforts can help minimise the negative consequences. Examples of research questions are the following:

- What mitigation strategies can be developed in the prevention of negative environmental impacts of QCC?
- What is the role of regulatory frameworks in mitigating potential negative impacts?
- What is the role of collaboration in impact prevention?

Standardisation and post-quantum transition

The standardisation efforts of NIST take a long time. Moreover, the transition to post-quantum systems is portrayed to be a challenging and costly endeavour. This is largely due to the compatibility issues with existing information infrastructures, and the dependency on legacy systems. Furthermore, the lack of collaboration fosters this difficulty. Researching how post-quantum systems can be integrated into current structures would be an interesting study. Moreover, researchers can focus on the development of a generalisable framework for the adoption and integration of post-quantum systems into their current infrastructure. Potential research questions are:

- How can organisations effectively assess the readiness of their existing infrastructures for the integration of post-quantum cryptography?
- How can constrained IoT-devices be modified to run resource-intensive post-quantum cryptography?
- What are the governance mechanisms and best-practices for managing the transition into post-quantum systems?

QCC and open innovation strategies

Open innovation in the development and anticipation of QCC is currently overshadowed by the competition surrounding QCC. This focus on competition results in a narrow view regarding standardisation and transition efforts, and this leads to neglecting responsible innovation efforts and prolongs the transition to post-quantum systems. Open innovation focuses on external expertise and resources to expand internal capabilities. How this might effect the post-quantum transition could be an interesting research topic. Possible research questions could be:

- What are the barriers and challenges hindering the adoption of open innovation practices in QCC?
- What are the potential benefits of adopting open innovation practices in the QCC domain?
- How can open innovation practices be integrated into the transition to post-quantum systems?
- What role do institutions, regulations and policy play in facilitating open innovation in QCC?

7 Conclusion

Emerging and breakthrough technologies may bring both societal disruptions and numerous benefits to companies. These technologies can also introduce ethical dilemmas and societal problems, as is seen in previous historical introductions of technology within society. This highlights the Collingridge Dilemma in which it is stated that controlling the technology becomes more difficult with time when the technology matures, whereas it is easier to steer in the beginning while knowledge about the potential impacts remains limited.

This study has shown that the topic of societal impacts related to quantum technology remains relatively under explored. This study presents a systematic literature review and categorisation of found impacts of quantum computing and communication (QCC) on society. Moreover, this systematic review is followed by semi-structured expert interviews from the industry to try and give a holistic overview of QCC impacts, and see whether the literature is complete in this regard. While many impacts are found in the literature, it remains largely focused on the cyber security implications of QCC, indicating a tunnel vision in anticipation. The interviews shed light on different types of impacts, such as environmental impacts, proving a mismatch between what the industry thinks and what the literature mentions. The combination of both the systematic literature review and the interviews answers the main research question: ”What are potential negative impacts of quantum computing and communication on society?”.

QCC impacts are complex and they have consequences on individuals, companies, the environment and the government, encompassing total society. At the micro-level, impacts on individuals related to privacy, trust and autonomy emerge. Firms are faced by the need to change and adapt their strategies, technologies and workforce skills to remain competitive and anticipate on QCC impacts. Environmental considerations emerge when the demand for energy increases for quantum computing, impacting carbon footprints and increased resource consumption. Furthermore, governments face challenges around the regulations of QCC on top of the geopolitical considerations and national security concerns.

The found impacts exhibit interrelations among each other, indicating that the impacts are not mutually exclusive. One impact may cause several other impacts, potentially leading to a cascading effect within society. Moreover, many impacts tend to be characterised by ambiguity, in which one impact can be seen as both positive, or negative.

Following the identification of QCC impacts and their categorisation, a new classification is presented as a general framework for policy advisers and managers in the context of QCC and society. This framework utilises known classifications and the distinguishing features of QCC impacts elicited from the literature and interviews. The framework is made to be generic in order to allow its use to be more general and outside of QCC domains.

Utilising the knowledge on the impacts, a preliminary set of mitigation strategies and recommendations is given. First security audits are recommended to companies in order to follow the cyber security developments and see whether current security measures are still effective. Second, companies are advised to be agile and foster an open innovation culture. Collaboration and transparency with stakeholders results in trust among partners and informed decision-making. Third, to counter illiteracy at companies, it is advised that organisations should incorporate learning programs for their workforce and relevant stakeholders. Fourth, recommendations are given to policymakers to start working on a regulatory framework. Furthermore, limitations of the study are recognised and highlighted. Moreover, a set of future research recommendations is given. There remain ample research opportunities in this relatively under explored domain.

With the identification and discussion of QCC impacts, and the presented classification, this study aims to have a positive impact on society. Policy advisers and managers can use this framework in the anticipation of new technologies in which impacts can be classified and ranked according to the users and their respective industries. Moreover, this work aims to address the Collingridge Dilemma and foster Technology Assessment by providing insights into the negative impacts at an early stage of QCC development and deployment. A collaboration among government, academia, industry and civil society may have the potential to bring insights and poses an opportunity to allow society to capitalise on the positive impacts of QCC, while minimising its negative impacts.

References

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *nature*, vol. 464, no. 7285, pp. 45–53, 2010.

[2] M. Lanzagorta, *Quantum radar*. Morgan & Claypool Publishers, 2012, vol. 5.

[3] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation," *Reviews of Modern Physics*, vol. 86, no. 1, p. 153, 2014.

[4] M. Kop, "Quantum-ELSPI: A Novel Field of Research," *Digital Society*, vol. 2, no. 2, Aug. 2023, ISSN: 2731-4650. DOI: `10.1007/s44206-023-00050-6`.

[5] N. M. Neumann, M. P. Van Heesch, F. Phillipson, and A. A. Smallegange, "Quantum Computing for Military Applications," in *2021 International Conference on Military Communication and Information Systems, ICMCIS 2021*, Institute of Electrical and Electronics Engineers Inc., May 2021, ISBN: 9781665445863. DOI: `10.1109/ICMCIS52405.2021.9486419`.

[6] J. Forge, "A note on the definition of "dual use"," *Science and Engineering Ethics*, vol. 16, pp. 111–118, 2010.

[7] P. Inglesant, M. Jirotka, and M. Hartswood, "Responsible innovation in quantum technologies applied to defence and national security," *NQIT (Networked Quantum Information Technologies)*, 2018.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[9] E. Milanov, "The rsa algorithm," *RSA laboratories*, pp. 1–11, 2009.

[10] A. Montanaro, "Quantum algorithms: An overview," *npj Quantum Information*, vol. 2, no. 1, pp. 1–8, 2016.

[11] A. Acín, I. Bloch, H. Buhrman, *et al.*, "The quantum technologies roadmap: A european community view," *New Journal of Physics*, vol. 20, no. 8, p. 080 201, 2018.

[12] V. Dunjko, J. M. Taylor, and H. J. Briegel, "Quantum-enhanced machine learning," *Physical review letters*, vol. 117, no. 13, p. 130 501, 2016.

[13] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, "Improvement of frequency standards with quantum entanglement," *Physical Review Letters*, vol. 79, no. 20, p. 3865, 1997.

[14] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nature photonics*, vol. 5, no. 4, pp. 222–229, 2011.

[15] J. Stilgoe, R. Owen, and P. Macnaghten, "Developing a framework for responsible innovation," *Research Policy*, vol. 42, no. 9, pp. 1568–1580, 2013, ISSN: 0048-7333. DOI: `https://doi.org/10.1016/j.respol.2013.05.008`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0048733313000930`.

[16] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[17] S. Saunders, "Are quantum particles objects?" *Analysis*, vol. 66, no. 1, pp. 52–63, 2006.

[18] E. Schrödinger, "Discussion of probability relations between separated systems," in *Mathematical Proceedings of the Cambridge Philosophical Society*, Cambridge University Press, vol. 31, 1935, pp. 555–563.

[19] F. Schumann, C. Winkler, and J. Kirschner, "Spooky long-distance effect or entanglement?,"

[20] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.

[21] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Reviews of modern physics*, vol. 81, no. 2, p. 865, 2009.

[22] P. Busch, T. Heinonen, and P. Lahti, “Heisenberg’s uncertainty principle,” *Physics reports*, vol. 452, no. 6, pp. 155–176, 2007.

[23] R. Ortt, “Quantum technology,” *Stichting Toekomstbeeld der Techniek*, 2020.

[24] N. Gisin and R. Thew, “Quantum communication,” *Nature photonics*, vol. 1, no. 3, pp. 165–171, 2007.

[25] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, eaam9288, 2018.

[26] C. H. Bennett and D. P. DiVincenzo, “Quantum information and computation,” *nature*, vol. 404, no. 6775, pp. 247–255, 2000.

[27] D. P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschritte der Physik: Progress of Physics*, vol. 48, no. 9-11, pp. 771–783, 2000.

[28] R. P. Feynman *et al.*, “Simulating physics with computers,” *Int. j. Theor. phys*, vol. 21, no. 6/7, 1982.

[29] V. Bužek, R. Derka, and S. Massar, “Optimal quantum clocks,” *Physical review letters*, vol. 82, no. 10, p. 2207, 1999.

[30] A. Peres, “Measurement of time by quantum clocks,” *American Journal of Physics*, vol. 48, no. 7, pp. 552–557, 1980.

[31] A. Genus and A. Stirling, “Collingridge and the dilemma of control: Towards responsible and accountable innovation,” *Research policy*, vol. 47, no. 1, pp. 61–69, 2018.

[32] A. Stirling, “Keep it complex,” *Nature*, vol. 468, no. 7327, pp. 1029–1031, 2010.

[33] M. V. Hayes, “On the epistemology of risk: Language, logic and social science,” *Social science & medicine*, vol. 35, no. 4, pp. 401–407, 1992.

[34] ISO., *Risk Management: Vocabulary*. ISO, 2009.

[35] Iso., “Risk management–principles and guidelines,” *International Organization for Standardization, Geneva, Switzerland*, 2009.

[36] F. H. Knight, *Risk, uncertainty and profit*. Houghton Mifflin, 1921, vol. 31.

[37] S. O. Hansson, “From the casino to the jungle: Dealing with uncertainty in technological risk management,” *Synthese*, vol. 168, no. 3, pp. 423–432, 2009.

[38] H. Hoffmann-Riem and B. Wynne, “In risk assessment, one has to admit ignorance,” *Nature*, vol. 416, no. 6877, pp. 123–123, 2002.

[39] S. O. Hansson, “How to perform an ethical risk analysis (era),” *Risk Analysis*, vol. 38, no. 9, pp. 1820–1829, 2018.

[40] D. Banta, “What is technology assessment?” *International journal of technology assessment in health care*, vol. 25, no. S1, pp. 7–9, 2009.

[41] A. Grunwald and M. Achternbosch, “Technology assessment and approaches to early engagement,” in *Early engagement and new technologies: Opening up the laboratory*, Springer, 2013, pp. 15–34.

[42] A. Grunwald, “Technology assessment: Concepts and methods,” in *Philosophy of technology and engineering sciences*, Elsevier, 2009, pp. 1103–1146.

[43] J. Schot and A. Rip, “The past and future of constructive technology assessment,” *Technological forecasting and social change*, vol. 54, no. 2-3, pp. 251–268, 1997.

[44] J. Durant, “Participatory technology assessment and the democratic model of the public understanding of science,” *science and Public Policy*, vol. 26, no. 5, pp. 313–319, 1999.

[45] A. W. Russell, F. M. Vanclay, and H. J. Aslin, “Technology assessment in social context: The case for a new framework for assessing and shaping technological developments,” *Impact Assessment and Project Appraisal*, vol. 28, no. 2, pp. 109–116, 2010.

[46] D. H. Guston and D. Sarewitz, “Real-time technology assessment,” *Technology in Society*, vol. 24, no. 1, pp. 93–109, 2002, American Perspectives on Science and Technology Policy, ISSN: 0160-791X. DOI: https://doi.org/10.1016/S0160-791X(01)00047-1. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X01000471.

[47] E. Palm and S. O. Hansson, “The case for ethical technology assessment (eta),” *Technological forecasting and social change*, vol. 73, no. 5, pp. 543–558, 2006.

[48] M. B. Van Asselt and O. Renn, “Risk governance,” *Journal of risk research*, vol. 14, no. 4, pp. 431–449, 2011.

[49] B. Taebi, J. H. Kwakkel, and C. Kermisch, “Governing climate risks in the face of normative uncertainties,” *Wiley Interdisciplinary Reviews: Climate Change*, vol. 11, no. 5, e666, 2020.

[50] N. Doorn and S. O. Hansson, “Should probabilistic design replace safety factors?” *Philosophy & Technology*, vol. 24, pp. 151–168, 2011.

[51] S. O. Hansson, “Risk and safety in technology,” in *Philosophy of technology and engineering sciences*, Elsevier, 2009, pp. 1069–1102.

[52] D. Wright, “A framework for the ethical impact assessment of information technology,” *Ethics and information technology*, vol. 13, pp. 199–226, 2011.

[53] M. J. Page, D. Moher, P. M. Bossuyt, *et al.*, “Prisma 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews,” *BMJ*, vol. 372, 2021. DOI: 10.1136/bmj.n160. eprint: https://www.bmj.com/content/372/bmj.n160.full.pdf. [Online]. Available: https://www.bmj.com/content/372/bmj.n160.

[54] R. Pranckutė, “Web of science (wos) and scopus: The titans of bibliographic information in today’s academic world,” *Publications*, vol. 9, no. 1, p. 12, 2021.

[55] K. L. Barriball and A. While, “Collecting data using a semi-structured interview: A discussion paper,” *Journal of Advanced Nursing-Institutional Subscription*, vol. 19, no. 2, pp. 328–335, 1994.

[56] P. Voigt and A. Von dem Bussche, “The eu general data protection regulation (gdpr),” *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[57] I. Etikan, S. A. Musa, R. S. Alkassim, *et al.*, “Comparison of convenience sampling and purposive sampling,” *American journal of theoretical and applied statistics*, vol. 5, no. 1, pp. 1–4, 2016.

[58] M. K. Salazar, “Interviewer bias: How it affects survey research,” *Aaohn Journal*, vol. 38, no. 12, pp. 567–572, 1990.

[59] M. B. Miles and A. M. Huberman, *Qualitative data analysis: An expanded sourcebook*. sage, 1994.

[60] C. McMullin, “Transcription and qualitative methods: Implications for third sector research,” *VOLUNTAS: International journal of voluntary and nonprofit organizations*, vol. 34, no. 1, pp. 140–153, 2023.

[61] A. Castleberry and A. Nolen, “Thematic analysis of qualitative research data: Is it as easy as it sounds?” *Currents in pharmacy teaching and learning*, vol. 10, no. 6, pp. 807–815, 2018.

[62] L. Possati, “Ethics of quantum computing: An outline,” *Philosophy and Technology*, vol. 36, no. 3, 2023, cited By 0. DOI: 10.1007/s13347-023-00651-6. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85164305182&doi=10.1007%2fs13347-023-00651-6&partnerID=40&md5=1af00566891b74d27c77b1f0370f2f44.

[63] M. Krelina, “Quantum technology for military applications,” *EPJ Quantum Technology*, vol. 8, no. 1, 2021, cited By 38. DOI: 10.1140/epjqt/s40507-021-00113-y. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118701398&doi=10.1140%2fepjqt%2fs40507-021-00113-y&partnerID=40&md5=5c3087e120373cfdceb04d8261cdb86a.

[64] K. Svozil, “Quantum hocus-pocus,” *Ethics in Science and Environmental Politics*, vol. 16, no. 1, pp. 25–30, 2016, cited By 10. DOI: 10.3354/esep00171. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015872810&doi=10.3354%2fesep00171&partnerID=40&md5=a61e601fd038df3be8fe2c16292873ec.

[65] A. Meda, I. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, “Quantum key distribution security threat: The backflash light case,” cited By 2, vol. 10674, 2018. DOI: 10.1117/12.2307704. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051181268&doi=10.1117%2f12.2307704&partnerID=40&md5=b761493f863e3b348357b250590e5d1f.

[66] J. Brito, D. López, A. Aguado, *et al.*, “Quantum services architecture in softwarized infrastructures,” cited By 1, vol. 2019-July, 2019. DOI: 10.1109/ICTON.2019.8840400. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073055743&doi=10.1109%2fICTON.2019.8840400&partnerID=40&md5=6142f51da47c981a24b29a19d4d9845a.

[67] P. Inglesant, C. Ten Holter, M. Jirotka, and R. Williams, “Asleep at the wheel? responsible innovation in quantum computing,” *Technology Analysis and Strategic Management*, vol. 33, no. 11, pp. 1364–1376, 2021, cited By 11. DOI: 10.1080/09537325.2021.1988557. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118152245&doi=10.1080%2f09537325.2021.1988557&partnerID=40&md5=c260970efdd4a52cf89b469e3349cbb7.

[68] G. Moody, V. Sorger, D. Blumenthal, *et al.*, “2022 roadmap on integrated quantum photonics,” *JPhys Photonics*, vol. 4, no. 1, 2022, cited By 138. DOI: 10.1088/2515-7647/ac1ef4. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85125773756&doi=10.1088%2f2515-7647%2fac1ef4&partnerID=40&md5=5021ba06ce00927972822a400cd9151c.

[69] S. Chowdhury, A. Covic, R. Acharya, S. Dupee, F. Ganji, and D. Forte, “Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions,” *Journal of Cryptographic Engineering*, 2021, cited By 5. DOI: 10.1007/s13389-021-00255-w. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100110511&doi=10.1007%2fs13389-021-00255-w&partnerID=40&md5=b9589e26a7288eed5ca294b81b7358fc.

[70] F. Smith, “Quantum technology hype and national security,” *Security Dialogue*, vol. 51, no. 5, pp. 499–516, 2020, cited By 21. DOI: 10.1177/0967010620904922. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85079462229&doi=10.1177%2f0967010620904922&partnerID=40&md5=b16fbcdc07431010117836143c2ddf65.

[71] P. Vermaas, “The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable,” *Ethics and Information Technology*, vol. 19, no. 4, pp. 241–246, 2017, cited By 21. DOI: 10.1007/s10676-017-9429-1. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85025687824&doi=10.1007%2fs10676-017-9429-1&partnerID=40&md5=f8c81aa706d82c86fa03b13b3296e667.

[72] Z. Seskir, S. Umbrello, C. Coenen, and P. Vermaas, “Democratization of quantum technologies,” *Quantum Science and Technology*, vol. 8, no. 2, 2023, cited By 4. DOI: 10.1088/2058-9565/acb6ae. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85148043325&doi=10.1088%2f2058-9565%2facb6ae&partnerID=40&md5=d5c76f3d89168dc560b8a1c50b5953a6.

[73] G. Peterssen, “Quantum technology impact: The necessary workforce for developing quantum software,” cited By 6, vol. 2561, 2020, pp. 6–22. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081644195&partnerID=40&md5=20866c56198a1bdad60a3cd7cdcdec09.

[74] J. Hevia Oliver, “Requirements for quantum software platforms,” cited By 1, vol. 2705, 2020, pp. 20–26. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85095976940&partnerID=40&md5=08d0819f264736c0a46f2bc1961a3e4c.

[75] G. Hernández González and C. Paradela, “Quantum agile development framework,” *Communications in Computer and Information Science*, vol. 1266 CCIS, pp. 284–291, 2020, cited By 3. DOI: 10.1007/978-3-030-58793-2_23. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091159756&doi=10.1007%2f978-3-030-58793-2_23&partnerID=40&md5=294f0ddff7443fb2cf7c2b93132dca52.

[76] L. Jiménez-Navajas, R. Pérez-Castillo, and M. Piattini, “Reverse engineering of quantum programs toward kdm models,” *Communications in Computer and Information Science*, vol. 1266 CCIS, pp. 249–262, 2020, cited By 7. DOI: 10.1007/978-3-030-58793-2_20. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091164745&doi=10.1007%2f978-3-030-58793-2_20&partnerID=40&md5=973c846a0ca583c4e67d4be08a9b0345.

[77] M. Kumar, “Post-quantum cryptography algorithm’s standardization and performance analysis,” *Array*, vol. 15, 2022, cited By 10. DOI: 10.1016/j.array.2022.100242. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136500675&doi=10.1016%2fj.array.2022.100242&partnerID=40&md5=a5ce2278c77729ef3b125055de499356.

[78] G. Yalamuri, P. Honnavalli, and S. Eswaran, “A review of the present cryptographic arsenal to deal with post-quantum threats,” cited By 2, vol. 215, 2022, pp. 834–845. DOI: 10.1016/j.procs.2022.12.086. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85163790389&doi=10.1016%2fj.procs.2022.12.086&partnerID=40&md5=48555d6a5b0b9f38a0a403da6bbaa447.

[79] H. Alyami, M. Nadeem, W. Alosaimi, *et al.*, “Analyzing the data of software security life-span: Quantum computing era,” *Intelligent Automation and Soft Computing*, vol. 31, no. 2, pp. 707–716, 2022, cited By 5. DOI: 10.32604/iasc.2022.020780. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116202948&doi=10.32604%2fiasc.2022.020780&partnerID=40&md5=09c868f2f93bc31cad5c3d086d3f85c1.

[80] M. Kaiiali, S. Sezer, and A. Khalid, “Cloud computing in the quantum era,” cited By 6, vol. 2019-January, 2019. DOI: 10.1109/CNS44998.2019.8952589. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078348371&doi=10.1109%2fCNS44998.2019.8952589&partnerID=40&md5=f64b8123567e8809294a86499aa9ae57.

[81] G. Pradel and C. Mitchell, “Post-quantum certificates for electronic travel documents,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12580 LNCS, pp. 56–73, 2020, cited By 4. DOI: 10.1007/978-3-030-66504-3_4. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85120530093&doi=10.1007%2f978-3-030-66504-3_4&partnerID=40&md5=49e1a6e061a6f28bcaeb82d9da2539ef.

[82] M. Krelina, “The prospect of quantum technologies in space for defence and security,” *Space Policy*, vol. 65, 2023, cited By 1. DOI: 10.1016/j.spacepol.2023.101563. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85163292906&doi=10.1016%2fj.spacepol.2023.101563&partnerID=40&md5=f60aa51f1b8790a2162f5553e94dd4d0.

[83] A. Covic, S. Chowdhury, R. Acharya, F. Ganji, and D. Forte, *Post-quantum hardware security: Physical security in classic vs. quantumworlds*. 2021, pp. 199–227, cited By 0. DOI: 10.1007/978-3-030-64448-2_8. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85148979822&doi=10.1007%2f978-3-030-64448-2_8&partnerID=40&md5=23f57a6c8e9bceef7d026df3738a05b6.

[84] R. Brandmeier, J.-A. Heye, and C. Woywod, “Future development of quantum computing and its relevance to nato,” *Connections*, vol. 20, no. 2, pp. 89–109, 2021, cited By 2. DOI: 10.11610/Connections.20.2.08. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85128354016&doi=10.11610%2fConnections.20.2.08&partnerID=40&md5=a1634cd999b64eb865d728f97fb9b946.

[85] A. Purohit, M. Kaur, Z. Seskir, M. Posner, and A. Venegas-Gomez, “Building a quantum-ready ecosystem,” *IET Quantum Communication*, 2023, cited By 0. DOI: 10.1049/qtc2.12072. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85170514192&doi=10.1049%2fqtc2.12072&partnerID=40&md5=62b87cbcab8df6f601a554b9e150b471.

[86] A. Bashirpour Bonab, M. Fedele, V. Formisano, and I. Rudko, “In complexity we trust: A systematic literature review of urban quantum technologies,” *Technological Forecasting and Social Change*, vol. 194, 2023, cited By 1. DOI: 10.1016/j.techfore.2023.122642. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85160724774&doi=10.1016%2fj.techfore.2023.122642&partnerID=40&md5=61e10a8fb0c35897c2d5439e4bfcf22c.

[87] I. García-Cobo and H. Menéndez, “Designing large quantum key distribution networks via medoid-based algorithms,” *Future Generation Computer Systems*, vol. 115, pp. 814–824, 2021, cited By 4. DOI: 10.1016/j.future.2020.09.037. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092909488&doi=10.1016%2fj.future.2020.09.037&partnerID=40&md5=101ea3bfb5fa98711d770a48062ce92a.

[88] M. Turlington, L. Sattler, D. Pacella, J. Gamble, and M. Toy, *Quantum Computing and Its Impact*. 2021, pp. 435–449, cited By 1. DOI: 10.1007/978-3-030-81961-3_16. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85159032210&doi=10.1007%2f978-3-030-81961-3_16&partnerID=40&md5=eb66e39c465c5ee74489a6a80367b0d1.

[89] X. Zhang, F. Wu, W. Yao, W. Wang, and Z. Zheng, “Post-quantum blockchain over lattice,” *Computers, Materials and Continua*, vol. 63, no. 2, pp. 845–859, 2020, cited By 11. DOI: 10.32604/cmc.2020.08008. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091180739&doi=10.32604%2fcmc.2020.08008&partnerID=40&md5=847bfed668b34080f2e0e7683949d508.

[90] Z. Jemihin, S. Tan, and G.-C. Chung, “Attribute-based encryption in securing big data from post-quantum perspective: A survey,” *Cryptography*, vol. 6, no. 3, 2022, cited By 5. DOI: 10.3390/cryptography6030040. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138628186&doi=10.3390%2fcryptography6030040&partnerID=40&md5=a208cc2c3ecec3d02faa8a91cf01b3bc.

[91] M. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, “A review of quantum cybersecurity: Threats, risks and opportunities,” cited By 11, 2022. DOI: 10.1109/ICAIC53980.2022.9896970. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136911796&doi=10.1109%2fICAIC53980.2022.9896970&partnerID=40&md5=eae91bc3257764ab7f4d4d128b4da80a.

[92] A. El-Latif, A. Iliyasu, and B. Abd-El-atty, “An efficient visually meaningful quantum walks-based encryption scheme for secure data transmission on iot and smart applications,” *Mathematics*, vol. 9, no. 23, 2021, cited By 5. DOI: 10.3390/math9233131. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85121313303&doi=10.3390%2fmath9233131&partnerID=40&md5=5fda984d9aeb7e86d6ff669e1d14de6d.

[93] C. Ten Holter, P. Inglesant, and M. Jirotka, “Reading the road: Challenges and opportunities on the path to responsible innovation in quantum computing,” *Technology Analysis and Strategic Management*, vol. 35, no. 7, pp. 844–856, 2023, cited By 10. DOI: 10.1080/09537325.2021.1988070. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85116468350&doi=10.1080%2f09537325.2021.1988070&partnerID=40&md5=0cc92c30230e6f0c08bcd67fd2700677.

[94] R. Romaniuk, “European quantum strategy – global and local consequences,” *International Journal of Electronics and Telecommunications*, vol. 69, no. 1, pp. 199–206, 2023, cited By 0. DOI: 10.24425/ijet.2023.144351. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152599521&doi=10.24425%2fijet.2023.144351&partnerID=40&md5=04213074f15adcb2aca5717168d8aae7.

[95] M. Kop, M. Aboy, and T. Minssen, “Intellectual property in quantum computing and market power: A theoretical discussion and empirical analysis,” *Journal of Intellectual Property Law and Practice*, vol. 17, no. 8, pp. 613–628, 2022, cited By 4. DOI: 10.1093/jiplp/jpac060. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136645979&doi=10.1093%2fjiplp%2fjpac060&partnerID=40&md5=0e327e1eb8a8b02ed0f0e5933fa90ffd.

[96] M. Hasanovic, C. Panayiotou, D. Silberman, P. Stimers, and C. Merzbacher, “Quantum technician skills and competencies for the emerging quantum 2.0 industry,” *Optical Engineering*, vol. 61, no. 8, 2022, cited By 10. DOI: 10.1117/1.OE.61.8.081803. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85140465203&doi=10.1117%2f1.OE.61.8.081803&partnerID=40&md5=9d344ebe92248291123523ba0590f2b2.

[97] A. Majot and R. Yampolskiy, “Global catastrophic risk and security implications of quantum computers,” *Futures*, vol. 72, pp. 17–26, 2014, cited By 19. DOI: 10.1016/j.futures.2015.02.006. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84953637757&doi=10.1016%2fj.futures.2015.02.006&partnerID=40&md5=d91a5dd9030d218fccb5555947f4fa0c.

[98] A. Petrenko, S. Petrenko, K. Makoveichuk, A. Olifirov, and H. Krachunov, “Security threat model based on analysis of foreign national quantum programs,” cited By 1, vol. 3057, 2021, pp. 11–25. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85122836962&partnerID=40&md5=c03f8343afcd08e71a33950ec48c2957.

[99] A. Iftemi, A. Cernian, and M. Moisescu, “Quantum computing applications and impact for cyber physical systems,” cited By 0, 2023, pp. 377–382. DOI: 10.1109/CSCS59211.2023.00066. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85170206632&doi=10.1109%2fCSCS59211.2023.00066&partnerID=40&md5=10edfce14cc9cd22abdc938be587c95e.

[100] R. Kuang and M. Barbeau, “Quantum permutation pad for universal quantum-safe cryptography,” *Quantum Information Processing*, vol. 21, no. 6, 2022, cited By 10. DOI: 10.1007/s11128-022-03557-y. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85131940109&doi=10.1007%2fs11128-022-03557-y&partnerID=40&md5=59b55bb48ff878397ecd25d801c2b2b1.

[101] H. Yi, “A secure blockchain system for internet of vehicles based on 6g-enabled network in box,” *Computer Communications*, vol. 186, pp. 45–50, 2022, cited By 6. DOI: 10.1016/j.comcom.2022.01.007. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85123743294&doi=10.1016%2fj.comcom.2022.01.007&partnerID=40&md5=dbbcb334b2bbfeb691ef8d6e9425d67e.

[102] R. Shah, “The conventional security of cloud computing and the growing threat to quantum computing,” cited By 0, 2022. DOI: 10.1109/GCAT55367.2022.9972028. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85145442226&doi=10.1109%2fGCAT55367.2022.9972028&partnerID=40&md5=3ee65645ddf65c698c96cf4d648b6025.

[103] S. Bickley, H. Chan, S. Schmidt, and B. Torgler, “Quantum-sapiens: The quantum bases for human expertise, knowledge, and problem-solving,” *Technology Analysis and Strategic Management*, vol. 33, no. 11, pp. 1290–1302, 2021, cited By 12. DOI: 10.1080/09537325.2021.1921137. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105356604&doi=10.1080%2f09537325.2021.1921137&partnerID=40&md5=62fe6447002cdcaed12b4a905f2eb15b.

[104] T. Madiega, “Artificial intelligence act,” *European Parliament: European Parliamentary Research Service*, 2021.

A

Human Resource Ethics

The informed consent form for the qualitative interviews can be found below.

Consent form quantum research

Dear participant, you are being invited to participate in a research study titled "An exploration of societal impacts of quantum technology". This study is being done by Cemal Dikmen, a master student at the Technology, Policy and Management faculty from the TU Delft, and as a graduation internship at EY. This work will aid in the completion of my master thesis in Management of Technology, anticipated to be finished by the end of February 2024.

The purpose of this research study is to gain insights into potential negative impacts of quantum computing and communication (QCC) on society and will take you approximately 30 minutes to complete. This study aims to interview experts in different aspects of society: academia, governmental bodies and the business world. I have found and created a list of known potential negative impacts from the academic literature. I will be asking you to highlight potential negative impacts of QCC that are known to you. Moreover, we will discuss these impacts and potential mitigation strategies. The data gathered during the interviews will be compared to the found potential negative impacts. With this, we can see whether the academic literature lacks behind and propose further research directions for scholars. Furthermore, having a comprehensive and holistic view of potential negative impacts may provide policy makers, academic scholars and managers a framework to guide their decision-making processes to innovate responsibly. The insights you provide on QCC impacts will be summarized and sent back to you before it is going to be used (as aggregated data and anonymous quotes) in the report, to counter misinterpretation.

As with any online activity the risk of a breach is always possible. To the best of our ability your answers in this study will remain confidential. All personal data (such as name and email address) will only be visible to me and to my direct TU Delft supervisors and is stored safely on the TU Delft One Drive to remain fully GDPR compliant. This data will not be used in the report. For the internal and external validity of the research, the job title/position and general industry (government, banking sector etc.) will be mentioned in the set of interviewees (in the appendix of the report). The interviews will be recorded in order to make the transcribing process more efficient. The recordings will be stored on the TU Delft One Drive and will only be accessible by me and my direct TU Delft supervisors. The transcripts will be stored on the TU Delft One Drive to elicit mentioned potential negative QCC impacts. After the master thesis is completed, all the data will be deleted within two years. The two-year window is in place to reuse the data to allow for a potential publication of the research on the topic of QCC impacts, as this may allow other researchers to get more insights into potential QCC impacts on society and accelerate responsible quantum innovation. You will remain anonymous in all the potential output. Should we want to use the data for any other purpose, such as education, we will reach out to get your consent first.

Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any questions. You have the right to request access to your data and the right to request deletion of your data at any time.

Signature

______________________________ ______________________________ _________
Name of participant Signature Date