Cyberthreats in a Quantum Computing-Enabled World

A Study of New Zealand's Role and Readiness

Nicole Girvan

A thesis submitted to Auckland University of Technology

in fulfilment of the requirements for the degree of

Doctor of Philosophy (PhD)

2024

School of Engineering, Computer and Mathematical Sciences

Declaration

“I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.”

Nicole Girvan

Acknowledgements

I would like to thank my supervision team, which includes Emeritus Professor Marilyn Waring, Dr Alastair Nisbet, and Professor Rhema Vaithianathan, for their support, wisdom, and ongoing encouragement.

Abstract

Quantum computing has the potential to impact geopolitical power balances, global economic stability, and national security. The exponentially increased power of a fault-tolerant large-scale quantum computer will threaten the security of existing cryptographic mechanisms that underpin safe online activity. Therefore, it is imperative that nations prepare for this emerging cyber risk. However, no literature currently describes how prepared New Zealand is to face quantum computing-enabled cyber threats.

This research aims to close this knowledge gap by investigating how prepared critical New Zealand organisations are to face quantum computing-enabled threats. It also explores the role the New Zealand Government should play in forming global policy on quantum technology's ethical and cybersecurity implications. Finally, this research aims to clarify the factors that will influence New Zealand's cybersecurity preparedness in a quantum-enabled landscape.

This qualitative study was undertaken through a lens of classical pragmatism. An interview method derived findings that reflected the lived experience of New Zealand cybersecurity and technology policy professionals and uncovered insufficient organisational preparation to address emerging quantum computing-enabled cyber threats. Document analysis found a growing global emphasis on developing quantum technology to ensure national sovereignty and security and highlighted the New Zealand Government's need to promote international collaboration in quantum technology.

The research describes global, national, and organisational readiness factors that may impact New Zealand's cybersecurity preparedness and provide actionable knowledge to prepare New Zealand for a quantum computing-enabled world.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes D'information
AWS	Amazon Web Services
CAKE	Code-based algorithm for key encapsulation
CIS	Center for Internet Security
CPT	Cumulative prospect theory
CQT	Centre for Quantum Technologies
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed denial of service
DOI	Diffusion of innovation
ECDH	elliptic-curve Diffie–Hellman
EIU	Economist Intelligence Unit
FOIS	Federal Office for Information Security
GCSB	Government Communications Security Bureau
GDPR	General Data Protection Regulation
HIRE	High impact rare event
IoT	Internet of things
IP	Intellectual property
ITR	Interviewee transcript review
LFT	Large, fault-tolerant
LMS	Leighton–Micali scheme
MOE	Ministry of Education
MSP	Managed service provider
NAS	National Academy of Sciences
NCSC	National Cyber Security Centre
NISQ	Noisy intermediate-scale quantum
NIST	National Institute of Standards and Technology
NQM	National Quantum Mission
NQSN	National quantum-safe network
NSA	National Security Agency
NSO	Nationally significant organisations
NZ	New Zealand

OTP	One time pad
PKI	Public key infrastructure
PQC	Post-quantum cryptography
QCCP	Quantum computing cyber security preparedness
QEP	Quantum Engineering Programme
QIS	Quantum information sciences
QKD	Quantum key distribution
QRAM	Quantum random access memory
RACI	Responsible, accountable, consulted, and informed
RTA	Reflexive thematic analysis
SEC	Securities and Exchange Commission
SIKE	Supersingular isogeny key exchange
SNDL	Store now, decrypt later
TLS	Transport layer security
UK	United Kingdom
UN	United Nations
US	United States
VPN	Virtual private networks
WEF	World Economic Forum
XMSS	eXtended Merkle signature scheme

Chapter 1: Introduction

"*Every thinker puts some portion of an apparently stable world in peril, and no one can wholly predict what will emerge in its place*". – John Dewey, Experience and Nature (1929, p. 222)

1.1 Background and Motivation

The New Zealand (NZ) Government's *2019 Cyber Security Strategy* acknowledges that international state-sponsored actors are targeting companies significant to NZ. Cybercriminals are taking advantage of vulnerabilities in technologies, policies, business processes, and human nature to steal information, glean profits, and damage the nation's economy (NZ Government, 2019). The ongoing and escalating nature of these cyber-attacks demonstrate that increasing NZ's cyber resilience is critical to maintaining a stable and thriving business ecosystem (Government Communications Security Bureau [GCSB], 2020). Unfortunately, emerging technologies such as quantum computing increasingly threaten the cybersecurity mechanisms fundamental to NZ's safety and security, such as cryptography to secure data communication (Mosca, 2018).

History has demonstrated that information technology developments have the power to disrupt global social, political, and economic structures (Dupont, 2013). These developments are typically referred to as "disruptive technology" and are characterised by their ability not just to improve existing technology incrementally but to define new products and services and make a lasting change in the landscape. Quantum technologies, broadly including quantum computing, quantum communications, and quantum sensing, belong to this group of highly disruptive emerging technologies. While many of the potential impacts that quantum technology may have on society are unknown, there is now wide acknowledgement that quantum computing will have serious implications for nations and organisations attempting to secure their digital environments (Atkinson, 2020; National Institute of Standards and Technology [NIST], 2020; Wilson, 2020).

The laws of quantum mechanics allow quantum computers to process large volumes of data exponentially faster than traditional classical computers. Often called quantum speedup, this increased computing power has many potentially beneficial uses; however, it can also be used for nefarious purposes and break the security mechanisms that underly many current cryptographic systems (Atkinson, 2020).

Cryptography is widely used to secure the confidentiality, integrity, and non-repudiation of information stored digitally and transmitted online. The cryptographic algorithms used to secure global internet communication rely on mathematical problems believed to be unsolvable with classical computing power. However, solving these otherwise intractable problems will become possible with quantum speedup, thereby rendering existing systems insecure and requiring new solutions to be implemented immediately (NIST, 2020).

There are significant engineering challenges yet to be solved by researchers before a large, practical, fault-tolerant quantum computer capable of quantum speedup is developed for commercial use. However, as nations and private organisations are heavily investing in quantum computing to accelerate the

development of these machines, many experts believe this goal may be achieved in the near to medium future (Mone, 2020; Mosca, 2018; Wilson, 2020).

Should a scenario unfold whereby a single country or private business develop the capability for quantum speedup, does not share this technology, and uses it for malicious purposes, all NZ businesses, regardless of scale or industry, could be negatively impacted. For example, even if one organisation has upgraded its systems to be resilient, a partner they rely on, such as a bank or supplier, may not be prepared, and collateral damage, such as business interruption or data theft, could be suffered. This rapidly evolving threat landscape is driving a need for a greater understanding of the complex factors involved in protecting NZ's critical assets (Carayannis et al., 2021; Ganin et al., 2020). However, despite the NZ Government acknowledging that "quantum computing is on the horizon" (NZ Government, 2019), there is no current information describing the cybersecurity preparedness of NZ businesses to operate in a quantum-enabled environment. Therefore, the rationale for completing this study is to fill this gap by adding to the knowledge base on cybersecurity risk management and the preparedness of NZ organisations to face emerging quantum cybersecurity threats.

1.1.1 Motivation

A career focused on assisting NZ businesses in responding to and recovering from cyber incidents provided the motivation to explore this topic. Watching the significant emotional, financial, and reputational damage that can result from even minor cyber incidents drove a desire to understand why organisations are still struggling to protect their systems despite the availability of a wide range of cybersecurity advice, technology, and frameworks. Seeing the ongoing suffering in this area also prompted concerns about how NZ organisations will combat the potentially even more sophisticated cyber threats from new technology.

As a technology professional, I know that the benefits and allure of new technology are clear, and the prospect of experiencing the transformative shifts in power that quantum computing may offer is exciting. However, first-hand experience watching NZ organisations fail to defend against current cyber threats has led to questions about whether society is rushing to embrace new advances without pausing sufficiently to examine the possible consequences of adopting new technology and allowing sufficient time to mitigate any negative impacts. Additionally, as a female working in technology with experience of unconscious bias, discrimination, and organisational cultures that do not support inclusivity, this research is conducted in the hope that society will embrace a new and more diverse technology culture as it adapts and transforms to accept new technology.

As a parent, maintaining a safe, open, and equitable online environment and ensuring the next generation can benefit from innovative technology without unnecessary risk feels crucial. However, nations and organisations are clearly struggling to combat increasing levels of cybercrime and data breaches, proving there are no simple answers to this problem. This challenge motivated me to explore the wider environment and the lived experiences of cyber security professionals in NZ to develop accurate and useful knowledge that may help further understand this ever-increasingly complex issue.

1.2 Significance of the Study

This research is significant as it will produce actionable knowledge on emerging threat preparedness for practical use in the NZ business landscape. Investigating the contributing factors to quantum cybersecurity preparedness in NZ will lead to a more thorough understanding of quantum-enabled cyber threats, thereby helping to close a gap in the current body of knowledge. Examining the NZ Government's role in global preparation for the cybersecurity threats posed by quantum technology will allow a greater understanding of how NZ might address these threats to ensure national and economic security. Insights and recommendations regarding specific policies and practices that NZ could adopt to combat these threats will be described, ultimately helping to minimise cyber risk and enable NZ's critical business assets to be protected in the future. It is also envisioned that the actionable knowledge derived from this study will guide NZ organisations in assessing emerging cybersecurity threats and planning preparedness activities.

1.3 Research Approach

This qualitative study was conducted through a lens of classical pragmatism. Classical pragmatism is primarily concerned with knowledge that has practical outcomes (Kelly & Cordeiro, 2020) and was, therefore, ideal for a study that aimed to contribute practical and relevant knowledge to the NZ landscape. A pragmatic and highly reflexive methodology was used to ensure actionable knowledge was produced that could inform professional practice on cybersecurity preparedness in a quantum computing-enabled world.

The following research questions were asked to address identified knowledge gaps around quantum cybersecurity threats and NZ's organisational preparedness to face these threats:

1. How prepared are NZ organisations to face quantum computing-enabled cyber threats?
    a. How aware of quantum computing cybersecurity threats are critical NZ organisations?
    b. If aware, how are NZ organisations currently planning for emerging quantum computing cybersecurity threats?
2. What role could the NZ Government play in global conversations and policy development focused on the cybersecurity and ethical implications of emerging quantum-enabled technology?
3. What factors will contribute to NZ's cyber threat preparedness in a quantum computing-enabled world?

Two methods were used to answer these research questions. Each method focused on deriving data for analysis using a reflexive thematic analysis (RTA) approach. Firstly, an interview method was developed to gain in-depth information concerning the lived experience of NZ professionals in the cybersecurity and emerging technology landscape. The first round of interviews was designed to identify current levels of organisational awareness and preparation for the cyber threats posed by quantum-enabled computing. The results demonstrated limited understanding of these threats and no preparation for these potential cyber threats.

The second round of interviews sought to understand the role the NZ Government may play when discussing global policy on managing quantum-enabled computing and its related ethical and cyber risks. The results described the need for the NZ Government to actively prioritise international collaboration and promote the values important to New Zealanders to ensure these are reflected in future quantum technology development and use.

Secondly, publicly available documents that described national and regional strategies and standpoints on quantum computing and cyber security were analysed. This analysis aimed to gain further insights into the factors contributing to NZ's cybersecurity preparedness in a quantum computing-enabled world and the role the NZ Government may play in governing this technology. The findings show the need for globally agreed principles to guide the development and use of quantum technology to ensure it evolves safely. The findings further emphasised the importance of NZ's voice on the international stage.

Based on the findings, practical guidance is outlined to assist NZ organisations in preparing for quantum computing-enabled cyber threats. Additionally, a high-level model that describes the key factors that will impact NZ's preparation for a quantum computing-enabled world is presented. The quantum computing cyber security preparedness (QCCP) model describes national, global, industry and organisational readiness factors and provides greater clarity around what cybersecurity may look like for NZ in a quantum computing-enabled world.

1.4 Thesis Structure

The thesis comprises seven chapters. This chapter introduced the thesis topic and discussed the background, origin, and current state of research on the topic. The motivation for undertaking this research was outlined, and the importance of this study was emphasised. The chapter then introduced the research philosophy, methodology, and methods used in this study to obtain the findings.

Chapter 2 presents a literature review covering several primary areas, including the current and emerging NZ cyber threat landscape, the evolution of quantum computing, the potential threats posed to cybersecurity as a result of quantum development, possible solutions to these threats, and the preparedness of nations, organisations, and society to face quantum computing enabled threats.

This chapter begins by outlining the evolving cyber threat landscape in NZ. It describes the grave national security and financial impacts of cyber-attacks in 2024 and explores concerns about how emerging technologies such as quantum-enabled computing may exacerbate these impacts and introduce further vulnerabilities into an already fragile landscape. The lack of research specifically focused on how this technology will impact NZ is highlighted.

Quantum computing development is then explored. The potential for quantum mechanical properties such as superposition to enable exponential computing power is explained; however, the literature highlights the need to overcome significant engineering challenges to produce a quantum computer capable of this power. Challenges in maintaining qubit entanglement, coherence, and error correction are explored, along with current research on quantum hardware, software, and algorithm development.

A review of literature that explores the threat quantum computing poses to algorithms commonly used in cryptographic systems to secure online communication and transactions is then presented. This review

describes how Shor's quantum algorithm is theoretically proven to break algorithms such as Rivest–Shamir–Adleman (RSA) and elliptic-curve Diffie–Hellman (ECDH), rendering them insecure. It additionally explains that Grover's quantum algorithm will reduce the security of algorithms such as the Advanced Encryption Standard (AES)-256, requiring changes to their implementation to remain secure. Finally, it emphasises that once a sufficiently large and fault-tolerant quantum computer that can run these algorithms is developed, it will be necessary to find new means to secure the global online environment.

Two critical areas of research that may present solutions to the cryptographic threats posed by quantum computers are then outlined. Firstly, the evolution of quantum-resistant cryptography, which includes code-based, hash-based, lattice-based, multivariate, and elliptic-curve-based algorithms that may be resistant to quantum computing, is investigated. While these solutions require more work to ensure they are operationally secure, a selection of these new quantum-resistant cryptographic schemes will likely be standardised for use in 2024. Secondly, the growing area of quantum cryptography, particularly the development and implementation of quantum key distribution (QKD) networks using fibre or free-space technologies, is explored. QKD is described as the only known future-proof post-quantum solution found to date, and as such, it has started to be commercialised globally. However, limitations such as cost and distance prevent it from being a widely accepted option to secure against quantum computers.

The review then presents a growing body of literature highlighting quantum-enabled technologies' potential geopolitical and ethical impacts. The body of knowledge in this area is immature, and more research is required to fully understand the broader cyber threats or ethical implications of quantum computing development, including how its use may be governed internationally.

Finally, the literature review describes existing research and cybersecurity frameworks that attempt to measure and guide the preparation of nations and organisations to face cyber threats. While available guidance is vast, it has weaknesses as most frameworks are too broad and not tailored for quantum technology.

Chapter 3 establishes the theoretical framework for this thesis. The diffusion of innovation and cumulative prospect theories are described as providing suitable frameworks to assist in interpreting the data derived from this study due to their successful history of use in technology research. Importantly, these theories also focus on understanding the adoption of technology and decision-making in conditions of uncertainty, such as those presented by emerging and not fully understood quantum technologies.

Chapter 4 identifies the main research questions and sub-questions this study aims to answer to address the gaps in the current body of knowledge. This chapter presents the overarching research philosophy of classical pragmatism and the qualitative, pragmatic, and reflexive methodological approach undertaken. Two data collection methods, interviews and document analysis, are presented, and an RTA data analysis approach is described. Finally, the management of quality and ethical considerations critical to this study is addressed.

Chapter 5 describes the findings obtained from both research methods. Firstly, the results of the interview method are presented, which describe a landscape in NZ of high cyber risk and varied cyber maturity. The findings also show a need to develop national cybersecurity and quantum technology capacity and highlight the importance of building trusted relationships and applying more strategic thought across the

emerging cybersecurity and technology area. This is followed by the findings from the document analysis, which discuss how many nations globally are developing quantum technology and ecosystems to protect digital sovereignty, national security, and economies and how this technology is also being developed to influence and protect online behavioural norms.

Chapter 6 analyses the findings from Chapter 5 and relates them to the main issues described in the literature review to answer the research questions. The chapter then describes the implications of the findings and presents recommendations for improving national and organisational preparation to address the cyber threats posed by quantum computing.

Chapter 7 concludes by summarising the findings, explaining limitations, and describing possible future research areas, which, if undertaken, could further advance the overall understanding of quantum computing-enabled cyber threat preparation in NZ.

Chapter 2: Literature Review

2.1 Introduction

This chapter reviews the relevant literature on quantum-enabled computing technologies and the cyber-threat environment they operate within. This review aims to outline the current understanding of quantum computing and the potential cyber threats it may pose and identify any gaps in the existing body of knowledge that warrant investigation. Critical issues in developing and securing quantum computing for use in the digital landscape in NZ are also presented.

The review comprises eight main sections. Section 2.2 discusses the general cyber threat environment in NZ, focusing on current literature that describes the current and emerging challenges faced when attempting to secure the digital landscape. Section 2.3 provides an overview of quantum computing research and development and includes literature investigating the challenges and limitations surrounding the technology. Section 2.4 focuses specifically on the threat posed to current cryptographic systems by the development of quantum computing, and Section 2.5 focuses specifically on current research and literature that considers potential solutions to this threat. Section 2.6 describes other less fully researched but critical areas where quantum computing may negatively impact society. This section covers literature exploring the geopolitical framing of emerging technologies and their potential ethical impacts on democracy, data sovereignty, and privacy. Section 2.7 investigates how nations globally, including NZ, are responding to the evolution of quantum technology and the potential threats it poses. Section 2.8 explores literature that attempts to determine the readiness of organisations and nations to combat threats in the cyber environment and includes literature that attempts to aid in preparation for quantum-enabled cyber threats. Finally, Section 2.9 concludes the literature review.

2.2 The Current and Emerging NZ Cyberthreat Landscape

Cyber-attacks that breach critical systems continue to threaten governments, organisations, and individuals globally and are predicted to grow in volume and impact (Organisation for Economic Co-operation and Development [OECD], 2023). NZ is not immune to this growing cyber threat landscape; however, a review of the available literature found limited academic research focused on investigating the NZ cyber threat environment. Achini and Ekundayo (2022) also highlight the lack of academic research on cyber security and cyber threats in NZ, explaining how most information is found in government white papers and industry reports.

Burton (2013) explained how cybersecurity is a national security issue for NZ and how increasing cyber threats have implications for the nation's critical infrastructure, international partnerships, and military actions. Burton (2013) discussed how the relative geographic isolation of NZ, which typically influences national defence strategies, has become irrelevant in the cyber world, necessitating a new understanding of national defence. The NZ Government responded to this new security risk by increasing domestic cybersecurity capacity. For example, in 2011, The National Cyber Security Centre (NCSC) was opened as a part of the GCSB and an inaugural *National Cybersecurity Strategy* was created (New Zealand Government, 2011). However, Burton (2013) also highlighted how more research is required to develop effective cyber-attack deterrence in NZ, and this area of literature is still lacking.

In 2023, the NCSC described an increasingly complex cyberthreat landscape in NZ and a heightened determination from cybercriminal groups attempting to extort payment from NZ organisations. The availability of more effective cyber threat tools, compromised credentials, and growing vulnerabilities in public-facing cyberinfrastructure are all highlighted as factors enabling malicious actors to cause national-level harm to NZ (NCSC, 2023). Cyber-attack volumes in NZ are increasing yearly, and in 2022, the NCSC detected and disrupted over 250,000 malicious cyber incidents (NCSC, 2023). Asghar (2019) illustrated these growing threat volumes through the example of a small NZ regional district health board that reported facing 864,000 cyber-attacks per day. These attack volumes are described as putting vulnerable patients at risk.

Cyber-attacks also have a significant financial impact on NZ organisations. The amount of damage caused by cybercrime now exceeds that caused by theft, fire, or flood (Baker, 2021) and in 2022, CERTNZ reported the greatest quarterly loss from cyber-attacks to date of NZ$8.9 million (CERTNZ, 2022). However, due to limited visibility and reporting of attacks, this figure will likely be a fraction of the actual financial losses suffered by NZ organisations (Falkenmire, 2023). Several authors highlight how victims of cyber incidents rarely report them or share information describing how an attack occurred (Asghar, 2019; CERTNZ, 2022; Falkenmire, 2023; Garae et al., 2017). Garae et al. (2017) further describe how this lack of sharing not only impacts cyber incident statistics but also limits the ability of other organisations in NZ to utilise actual data to visualise attack patterns and learn from these attacks.

Business email compromise, ransomware, and supply chain exploitation were the most prevalent cyber-attack types seen impacting NZ organisations between 2019 and 2023 (Baker, 2021; NCSC, 2020, 2022, 2023). Aura Information Security (2021) surveyed NZ organisations and found that over half had experienced a ransomware attack in the previous 6 months. These figures are consistent with global reports suggesting that 66% of all organisations experienced ransomware in 2022 (Sophos, 2023) and further demonstrate how NZ is not immune to global trends in the cyber threat landscape.

Cyber-attacks are increasingly sophisticated and often target individual behaviours rather than software or systems (Falkenmire, 2023), suggesting the need for greater cybersecurity awareness in addition to greater technical defence measures. Unfortunately, Tirumala et al. (2016) found low cybersecurity awareness when surveying NZ students. The study describes how common cybersecurity terms and attack types are unfamiliar to NZ students and how they also have a low awareness of useful cybersecurity tools. The results of this study indicate that much greater effort is still required to lift general cybersecurity awareness levels in NZ.

The NZ Government acknowledges that state-sponsored actors pose an ongoing espionage threat to NZ organisations and continue to look for, identify, and exploit new weaknesses in NZ cyber defences. Foreign states may pose a risk to NZ by maliciously using technology to influence democracy covertly, interfere with international relationships, obtain access to sensitive information, and gain economic advantages by stealing technological and intellectual property (IP) (NZ Government, 2021). However, state-sponsored cyber activity is hard to identify and may go undetected. Additionally, even if detected, it is extremely challenging to attribute to specific nations or groups (NCSC, 2023). In 2022, the NCSC reported assisting in 316 incidents specifically targeting nationally significant organisations, with 28% of those suspected to be linked to state-sponsored activity (NCSC, 2023). In 2023, this level of state-sponsored activity rose to

34%, and the intensification of geostrategic competition is highlighted as one contributing factor to increasing state-sponsored cyber risk in NZ (Hampton, 2023).

The potential impact of emerging technologies on cyber security is now being widely investigated internationally due to the recognition that they may escalate existing cyber threat volumes, introduce new attack vectors, and increase the harmful impacts of cyber-attacks (North Atlantic Treaty Organization [NATO], 2023; Raban & Hauptman, 2018). Cyber-attacks fuelled by emerging technologies are predicted to become more disruptive and destructive. It is thought that malicious actors will increasingly use emerging technologies to target national democracies via election interference, espionage, critical infrastructure destruction, and misinformation campaigns (Hampton, 2019; Michael et al., 2020). NZ cyber professionals report also being increasingly concerned about the potential for these new technologies to introduce new vulnerabilities into the digital ecosystem (Murison, 2021).

Quantum technologies, which include quantum computing, communication, and sensing, are globally recognised as emerging technologies that will significantly impact cybersecurity and the global cyber threat landscape in the next decade. Raban and Hauptman (2018) and NATO (2023) describe how quantum technology may change the world and profoundly impact security by posing new threats from state and non-state actors to military and civilian society. In NZ, the Director General of the GCSB has stated that quantum computing will increase the potential scale and impact of cyber-attacks and that NZ will face growing insecurity in cyberspace due to this new technology (Hampton, 2019).

The NCSC (2023) warn that NZ organisations must be prepared to govern the use of emerging technologies and ensure that privacy and security risks associated with their adoption are managed. However, there is also a growing recognition that NZ cybersecurity infrastructure, including the people, processes and technology used to defend against cyber threats, is not keeping pace with rapid new technology and cyber threat developments (Murison, 2021).

While no research was found that specifically explores the impact of quantum computing on the NZ cyberthreat landscape, several studies may provide useful insights for the NZ Government and NZ organisations preparing to securely adopt this technology. The OECD (2023) included NZ in literature exploring the cybersecurity workforce in five countries, noting that NZ saw the greatest increase in demand for skilled cybersecurity practitioners in the last 5 years of all the nations surveyed. This research supplies a starting point for understanding the supply and demand for cyber skills essential to the safe adoption of new technology; however, further work is required to fully explore how the greater demand for skilled professionals may be met.

Younus et al. (2022) examined how cybersecurity structures influence the acceptance of new technology, such as bitcoin currency in NZ. Younus et al. concluded that effective cybersecurity has a significant beneficial impact on emerging technology acceptance and use. These results suggest that effective cybersecurity may be essential for quantum computing technologies to be readily adopted in the NZ landscape. Finally, Dizon and McHugh (2022) investigated the regulation of encryption in NZ, a critical cybersecurity tool. Dizon and McHugh outlined the existing laws regulating the development, use, and access to encryption, thereby providing a good foundation for considering any alteration in regulation

required to mitigate the impact of emerging technologies, such as quantum computing, on encryption technologies.

The studies outlined in this section each provide relevant insights into the existing cyber landscape; however, further investigation into the impact, defence, and readiness strategies for quantum computing must be undertaken in NZ to ensure organisations can securely adopt emerging quantum technologies and prevent further acceleration of NZ cyberthreat volumes.

2.3 Quantum Computing Overview

2.3.1 What is Quantum Computing?

Quantum mechanics is a subfield of physics aimed at describing the behaviour of atomic and subatomic particles. The underlying principles of quantum mechanics provide the basis for what is referred to as a new paradigm in computing—quantum computing. First proposed 40 years ago as a method to improve the computational modelling of quantum physical systems, quantum computing is the only currently known theoretical model that may offer exponential acceleration of today's computer systems (Grumbling & Horowitz, 2019).

Quantum computing is described as a new paradigm as it relies upon fundamentally different physical concepts than classical computing systems widely used today. These fundamental differences allow quantum computers to simultaneously consider various possible solutions to a problem, with the incorrect answers cancelling one another out and the correct answer being amplified (Byrd & Ding, 2023).

A classical computer uses binary digits or bits to represent values in its operations. Classical bits are deterministic; they only exist in known states of 0 or 1 (Kop et al., 2024a). Therefore, classical computer operations are determined by following sequentially coded 0s or 1s, which computer coding languages convert into bits. Computers then operate by using these bits on integrated circuits of billions of transistors (Grumbling & Horowitz, 2019).

In contrast, quantum computers use quantum bits or qubits for their operations. Qubits are probabilistic, as the value of a qubit is determined only after measurement by an observer. Further, a qubit differs from a traditional bit as it can represent the binary values of 0 and 1 and any combination of both 0 and 1 simultaneously (Kop et al., 2024a). This unique feature of quantum mechanics is called superposition and can be described using a coin toss analogy (Atkinson, 2020). The result of a classical coin toss can be either heads or tails, representing the binary nature of a classical bit. However, a quantum computer can be represented by spinning the coin on its side, becoming a combination of heads and tails or 0 and 1 at any given moment. This behaviour gives quantum computers the advantage of operating in exponentially more states in parallel than a classical computer and enables multiple calculations to be performed simultaneously on a series of stored values (Atkinson, 2020).

Table 1 describes the number of resulting states or outcomes possible for a classical versus quantum computer at any one time.

Table 1

The Number of Resulting States or Outcomes Possible for a Classical Versus Quantum Computer at any One Time

Number of bits or qubits	Number of possible states for a classical computer (bit)	Number of possible states for a quantum computer (qubit)
2	1 (out of 4 possibilities)	All 4 possibilities
3	1 (out of 8 possibilities)	All 8 possibilities
4	1 (out of 16 possibilities)	All 16 possibilities
5	1 (out of 32 possibilities)	All 32 possibilities

Superposition allows for significant performance improvements over a classical computer. A quantum computer built with 50 high-quality qubits may outperform today's fastest and largest classical supercomputers for some operations, including potentially enabling the ability to search vast databases at lightning speed, calculate the properties of complex molecules, and uncover the secrets of advanced chemical reactions (Conover, 2020). These abilities may lead to positive scientific advances, such as the discovery of life-saving medicines or energy-efficient industrial processes. However, this acceleration will not only enable scientific advances but also increase computing power for nefarious purposes such as cyber espionage, data theft and sabotage (Atkinson, 2020).

Researchers currently face constraints when attempting to harness the promised power of quantum computing. Therefore, a practical, fault-tolerant quantum computer built at a scale capable of achieving either the positive or the adverse outcomes described previously has not yet been developed commercially.

2.3.2 Quantum Computing Evolution

When first proposed, quantum computing was merely a theoretical concept as no one knew how to build one; however, recent developments in creating and controlling qubits have led to research and industry groups building small proof-of-concept computers (Grumbling & Horowitz, 2019). While forms of quantum technology, such as quantum sensors, are already used in both civilian and military applications (Arrow et al., 2023; Bova et al., 2021), the quantum computers built today are still arguably experimental systems with limited processing capability and small memories. They are essentially single-purpose quantum mechanical information processors designed to execute a single task. Additionally, they must integrate significant traditional computing structures to perform these tasks at the desired rate, indicating they are not likely to replace classical computers at any time soon, if ever (Hoefler et al., 2023; Bova, 2021).

In traditional computing, Moore's law (Moore, 1965) has enabled computer scaling to occur relatively predictably. Quantum computing, however, is not thought to be at the development point needed for Moore's laws to apply; therefore, how long it will take to scale a quantum computer large enough to be commercially useful cannot yet be predicted accurately (Mosca, 2018). Previous incorrect predictions demonstrate the difficulty in estimating quantum computing development. For example, IBM announced that the construction of fault-tolerant systems would be reached by 2016 due to rapid improvements in experimental quantum hardware; however, this did not come to fruition (Steffen et al., 2011). However,

many experts agree, that a universal quantum computer will be built in the near to medium future, enabling both the positive and potentially negative potential uses of quantum computational speed (Mone, 2020; Ten Holter et al., 2022; Wilson, 2020).

Several authors, including Devoret and Schoelkopf (2013), Grumbling and Horowitz (2019), and Atkinson (2020), have attempted to create frameworks designed to measure quantum computing's evolution. These frameworks acknowledge the impossibility of focusing on specific dates to predict progress and instead list significant milestones to be met on the journey. Yale University proposed a seven-step process for building a large-scale quantum computer, which, while not offering definitive time frames, can indicate what stage quantum development has reached (Devoret & Schoelkopf, 2013). Each stage in the process represented in Table 2 is interconnected, and advancement to the next stage requires mastery of the earlier stages.

Table 2

Stages of Building a Large-Scale Quantum Computer

Stage	Description
1	Operations on single physical qubits
2	Algorithms on multiple physical qubits
3	Quantum nondemolition measurements for error correction and control
4	Logical memory with a longer lifetime than physical qubits
5	Operations on single logical qubits
6	Algorithms on multiple logical qubits
7	Fault-tolerant quantum computation

Note. Adapted from "Superconducting Circuits for Quantum Information: An Outlook" by M. H. Devoret & R. J. Schoelkopf, 2013, *Science*, *339*(6124), 1169–1174. https://doi.org/10.1126/science.1231930

Literature suggests that stage 3 of this model has been reached and work is quickly progressing toward stage 4, which requires a logical qubit to be stored, via error correction, for a time significantly longer than the decoherence time of its physical qubit components (AbuGhanem & Eleuch, 2024). However, researchers further stress that the final stages will require significant engineering advancements that enable scaling fault-tolerant designs to produce quantum computing systems capable of general-purpose computing (Hoefler et al., 2023; Kjaergaard et al., 2020).

The National Academy of Sciences (NAS) presents a slightly different model whereby the starting milestone which already exists today is the small (tens of qubits) computer. This model then describes two stages expected to be achieved in the early 2020s—a gate-based quantum computer demonstrating quantum supremacy and implementing error correction. The last two milestones are a commercially useful quantum computer and a large (>1,000 qubit) fault-tolerant modular quantum computer. Estimates for fully achieving the last two milestones have not been attempted (Grumbling & Horowitz, 2019).

One significant milestone towards full-scale quantum computing highlighted in the NAS model is "quantum supremacy". The exact definition of quantum supremacy is debated in the literature (Pednault et al., 2019); however, it is generally accepted to mean the point at which a quantum computer can perform a calculation that no classical computer could complete in a reasonable timeframe (Debenedictis, 2020). In 2019,

Google researchers published the results of an experiment claiming to have achieved quantum supremacy using programmable superconducting circuits on a 53-qubit machine (Arute et al., 2019). Arute et al. claimed that the Sycamore quantum processor completed a single task in 200 seconds that would take a classical supercomputer 10,000 years to complete. This achievement, however, has been debated by Pednault et al. (2019), who believe the demonstrated task could, in fact, be simulated by a supercomputer in only two and a half days rather than 10,000 years.

Arute et al.'s (2019) announcement was closely followed by a publication from Zhong et al. (2020), who claimed to have surpassed Sycamore's speed using technology based on optical circuits. Zhong et al. described the successful development of a quantum processor capable of performing a single task 100 trillion times faster than a classical supercomputer.

Both quantum processors described in these claims were explicitly built for single tasks and operate using only a fraction of the one million qubits that may be needed for a general-purpose quantum computer. However, they herald the start of an era in which early quantum machines might be used for practical applications such as generating random numbers (Arute et al., 2019) and machine learning (Cong et al., 2019).

Achieving quantum supremacy is crucial as it proves that quantum computers can outperform classical machines and provides evidence that quantum speedup may be practically achieved in the "real world". Google are now further predicting that quantum computational power will start to grow at a double-exponential rate, and should the claims of quantum supremacy by either Arute et al. (2019) or Zhong et al. (2020) stand up under further scrutiny from the research community, consideration should be given to the possibility that quantum hardware development will start to follow an equivalent of Moore's law.

More recently, researchers are starting to look beyond the achievement of quantum supremacy and investigate the notion of "quantum advantage" or "quantum utility" (Herrmann et al., 2023). Hoefler et al. (2023) describe quantum advantage as the search for meaningful applications of quantum speedup, as opposed to the technical point in time milestone that quantum supremacy attempts to convey. Researchers believe that practical candidates for useful quantum speedup are likely to be solving small-data problems in chemistry and materials science with exponential speedup (Hoefler et al., 2023).

The body of literature discussing quantum computing progress does not appear to rely on any standard measuring or consistent reporting guidelines. If researchers developed standard benchmarks and widely adopted these, the comparison of achievements between quantum devices could be enabled. Benchmarked results could help clarify the steps required for full quantum computing enablement at a much more granular level. Creating a shared development roadmap would also minimise research overlap and encourage faster and more efficient progress.

2.3.3 Quantum Computing Challenges and Limitations

Significant engineering challenges have yet to be overcome to develop a practical machine capable of utilising quantum computing's increased computational power. It is particularly difficult to initialise a quantum system in a known state and perform operations on that state while ensuring the surrounding environment does not impact the result (Chatterjee et al., 2023).

Several essential conditions must be met to create a high-quality qubit and enable quantum operations. These conditions include ensuring qubit entanglement, gaining a high level of coherence, and sufficiently controlling the qubits to reduce error rates. However, currently, there is no leading qubit technology, and various physical systems are being explored in literature for use as qubits. These include using trapped ions (Ballance et al., 2016; Brandl et al., 2016; Moses et al., 2023; Tsuchimoto et al., 2024), photons (Vigliar et al., 2021; Qiang et al., 2018; Wang et al., 2016), spins in semiconductors (van der Heijden et al., 2018) and superconducting circuits (Chatterjee et al., 2023; Chen et al., 2014; Wendin, 2017). All of these techniques share common challenges when trying to meet the conditions necessary for quantum operations with no qubit technology currently deemed superior (Byrd & Ding, 2023).

2.3.3.1 Entanglement

All qubits in a system must be entangled to utilise the quantum computer's potentially larger problem space. Entangling all qubits allows an exponential increase in possible states with each qubit added to a system. This is achieved by correlating each qubit's state with the states of all the other qubits and linking them as if they were one entity, even when physically located on opposite ends of a chip (Byrd & Ding, 2023).

To create entanglement between nonadjacent qubits, they must be indirectly coupled through a chain of operations using intermediate qubits to facilitate the interaction. However, this process creates a challenge as it consumes many available qubits, thereby rendering the number of useful qubits in the quantum machine much lower than the actual physical number of qubits it possesses (Grumbling & Horowitz, 2019). Research is underway to develop quantum hardware that can preserve entanglement under varied conditions; however, as yet, the solutions presented still face challenges when attempting to scale systems and preserve entangled quantum states over distances (Bao et al., 2024; Cacciapuoti et al., 2020; Caleffi et al., 2020).

2.3.3.2 Coherence

Quantum computers require strong coherence to maintain a definite phase relationship between the waves (Lami, 2020). However, quantum computers differ from classical computers in that they have limited ability to handle small unwanted variations in the system, commonly described as noise. A qubit's extreme sensitivity to noise makes coherence hard to maintain.

Whilst a classical computer may encounter noise due to fluctuations in the electrical system, they are very effective at removing that noise and assigning the correct value of either 0 or 1. The data stored in classical bits is represented by magnetised areas consisting of many atoms. These plentiful atoms deliver built-in redundancy, making classical bits resilient to error (Conover, 2020).

In contrast, a qubit's ability to exist in superposition states makes overcoming noise and assigning a correct value to the operation more challenging. Qubits are made from fragile substances such as individual atoms, small bits of superconducting material and electrons trapped in silicon (Chatterjee et al., 2023). Errors are created as they interact with their environment and encounter electromagnetic fields, heat, or stray particles. If only one atom representing a qubit is jostled, the information being stored by that qubit is lost (Chatterjee et al., 2023). This ultimately leads to incorrect computations and a high error rate. Qubits, therefore, must be isolated from any outside interference (Krinner et al. 2022).

One solution for enhancing the stability of a qubit and, therefore, coherence is to keep qubits at a temperature near absolute zero or -459° Fahrenheit. Schoelkopf (2016) discovered that by using superconducting circuits and qubits built from materials that exhibit quantum properties when cooled and kept at very low temperatures, coherence could be increased by a factor of 10 every 3 years. IBM and Google are both using these superconducting circuits to build their prototype quantum machines (Byrd & Ding, 2023). While other researchers such as Esmaeilifar et al. (2020), Jing et al. (2020) and Ilyas et al. (2022) are investigating the use of alternative solutions such as anyon particles, it is thought that superconducting circuits will yield results first (Kjaergaard et al., 2020). However, maintaining systems that use superconducting circuits at near absolute zero introduces additional limitations for their practical use. Cooling units the size of a standard refrigerator are required for minimal quantum operations, rendering these systems impractical for any mobile applications (Byrd & Ding, 2023).

2.3.3.3 Qubits must be controlled in such a fashion that error rates are reasonable

Current literature recognises that without efficient error correction, it is unlikely that complex quantum problems will be solved (Chatterjee et al., 2023; Grumbling & Horowitz, 2019; Holmes et al., 2020). Errors can be corrected in quantum computers using algorithms; however, current error-correcting algorithms require an increased number of operations and additional qubits to perform corrective actions and produce a stable or logical qubit (Aleiner et al., 2023).

Error-correcting schemes in classical computers can be relatively simple. For example, a bit value of 1 may be copied three times, giving 111. If one of the bits is accidentally changed through error and 111 turns into 110, an error would be evident, as they are no longer the same. The majority value can then be used to determine which bit is incorrect and fix it (Chatterjee et al., 2023). Unfortunately, the unique properties of quantum mechanics do not allow similar schemes to work in a quantum computer. Firstly, the quantum no-cloning theorem states that it is impossible to copy or clone an arbitrary quantum state, and therefore, a qubit cannot be duplicated (Epstein, 2019). Secondly, any attempt to measure a qubit's state removes it from a superposition state and destroys its quantum properties (Wilson, 2020).

Quantum error-correcting schemes originate in research first proposed by Peter Shor in 1995 (Shor, 1995). These schemes combine multiple error-prone physical qubits into one reliable (or logical) qubit. This technique attempts to overcome the natural phenomenon known as decoherence, whereby quantum objects lose their quantum properties naturally through interactions with their surroundings (Krinner et al., 2022). Rather than measuring qubits, an error is measured by checking if the value of two qubits is the same without measuring either. However, as qubits cannot be copied, the error-correction schemes must store data redundantly over logical qubits, which introduces an additional challenge. As each logical qubit comprises multiple entangled physical qubits, a program requiring 10 logical qubits to run may need a quantum computer with hundreds of thousands of physical qubits to accommodate error correction. It is estimated that millions of physical qubits would be needed to run some complex quantum computations (Aleiner et al., 2023).

One early error-correction technique, termed surface codes, has been the basis for further recent development that separates qubits into different roles to perform various tasks (Bravyi & Kitaev, 1998). Surface codes are designed for qubits arranged in a 2D grid, such as how superconducting quantum computers are typically created. They work by dedicating some qubits to storing information and others to

ancilla tasks. In this solution, a logical qubit comprises both data qubits and ancilla qubits, allowing for error checking and correction without destroying any data stored in the data qubits. Kelly et al. (2015) released a simplified nine-qubit version of a surface code which was improved upon by Andersen et al. (2019), who have tackled the detection of not only simple bit-flip errors but secondary phase flip errors unique to the quantum environment. However, Andersen et al.'s solution can only detect errors, and correcting these is a problem yet to be solved. Both Krinner et al. (2022) and Aleiner et al. (2023) progress surface code research further and posit that their results demonstrate that achieving fault tolerant quantum computing is realistic.

Additional challenges to the theoretical surface code solution also exist. For it to be a practical error-correcting technique, it requires a 49-logical qubit quantum compute so it has not been widely tested (Conover, 2020). Additionally, the surface code technique requires stable original physical qubits that err less than 1% of the time to be effective. Current documented error rates for operations on systems containing five or more qubits are still at or above 3%, and to date, improved error rates have only been achieved in very small systems (Corcoles et al., 2020; Krinner et al., 2022).

A lack of efficient error correction is a significant limiting factor for quantum computing evolution. Currently, available fault-tolerant public quantum computers are small, and to achieve many of the tasks discussed, they must become much larger whilst simultaneously reducing error rates (Aleiner et al., 2023). At this stage, it can be concluded from the literature that an efficient solution to error correction, whilst getting closer, has not yet been found.

2.3.3.4 Hardware

Even if the conditions to create stable, high-quality qubits are met, further hardware challenges must be overcome to construct and operate a commercially viable fault-tolerant quantum computer. A quantum computer essentially consists of atoms and light. Quantum platforms can be built as optical systems using lasers or solid-state systems requiring microwaves to manipulate the qubits. However, both use fundamentally different hardware to classical computing systems (Chang et al., 2020).

Various companies are also choosing to develop different types of quantum computers, ensuring that no single hardware solution is currently standard. Large companies, including IBM, Google, Microsoft, and Fujitsu, are focused on developing universal quantum computers which aim to use gate operators to solve problems (Brooks, 2023a; Gibney, 2019; Nayak, 2023). Universal quantum computers require millions of logical qubits to operate, and as current architecture cannot scale to the number of qubits needed to achieve fault tolerance, it is not predicted that they will be commercially viable in the next decade (Brooks, 2023b).

The second type of quantum computer being developed is the noisy intermediate-scale quantum computer (NISQ). A NISQ may use hundreds of physical qubits that are not error-corrected, and researchers are exploring applications for NISQ use in quantum machine learning (Arya et al., 2023; Havlíček et al., 2019) and quantum chemistry (Arya et al., 2023; Kandala et al., 2019). Discovering useful calculations that are shallow enough to operate regardless of gate errors and decoherence is proving somewhat elusive; however, and the full potential of NISQ machines is currently unknown (Arya et al., 2023). Despite these challenges, the development of NISQ is acknowledged as an important milestone towards full quantum

computing, as the successful application of NISQs may encourage significant commercial funding and research (Grumbling & Horowitz, 2019).

The Defense Advanced Research Projects Agency (DARPA) is attempting to exploit quantum information processing before the development of full fault-tolerant quantum computers by utilising a hybrid method combining NISQs with classical computing systems (DARPA, 2023). DARPA's goals include developing scalable quantum systems and implementing a quantum optimisation algorithm on a NISQ device (Wilson, 2020). While the continued development of NISQ and hybrid systems will accelerate quantum use, whether these systems will offer any considerable advantages over classical supercomputers remains to be seen.

2.3.3.5 Quantum annealing

Another approach to building quantum computing hardware is seen in the evolution of quantum annealers. While not as powerful or flexible as a universal gate quantum computer, a stable quantum annealing processer is easy to build as it does not face the same challenge of maintaining qubit stability that universal gate systems have (Thapliyal & Humble, 2023).

Quantum annealing can be used to find the optimal solution for problems that involve many possible solutions by using quantum properties such as engagement, superposition, and quantum tunnelling. As annealing focuses on solving NP-hard problems, it is less impacted by noise than gate model quantum computing design. In quantum annealing, each state is represented as an energy level and simulated quickly to obtain the lowest energy state. The resulting lowest energy state is the most likely or optimal solution (Thapliyal & Humble, 2023).

The first superconducting circuit quantum annealing machine was built by D-Wave Systems in 2011, and subsequent research has shown practical, real-world use of quantum annealing in solving optimisation problems such as nurse scheduling (Ikeda et al., 2019) and satellite mission planning (Delilbasic et al., 2024). Ward and Bambos (2020) also used quantum annealing to combine deep-learning and quantum annealing's computational advantages to derive lung cancer diagnosis accurately and quickly from the x-rays of diseased lungs.

However, while quantum annealing performs better than classical computing, it has limited application and is typically used when the search space of a problem is discrete. Quantum annealers cannot execute all quantum algorithms as many are designed for gate-based universal quantum systems, and quantum annealers are not known to be polynomially equivalent to a universal quantum computer (Thapliyal & Humble, 2023).

The parallel development of multiple types of physical platforms, including varying encoding systems, is driving an emerging area of research focused on the interoperability of these systems. Guccione et al. (2020) have tackled one form of quantum system interoperability by creating an entanglement supporting protocol that allows quantum network nodes with different optical encoding to be connected. At this stage, the proposed protocol's success rate is not good enough for practical operations; however, it demonstrates promise that interoperability may be possible and leads the way for further research in this area.

Various parties, including the US (United States) National Security Agency (NSA), have launched academic programmes encouraging university research into quantum hardware development (NSA,

2020). However, as Wilson (2020) highlights, more recent progress in this area has been industry-led, and many hardware developments are now originating in the commercial sector. Literature on quantum hardware development also suggests that an industry-wide strategy to establish and support an engineering pathway for developing fault-tolerant universal quantum computers is still to be formed (Chang et al., 2020).

2.3.3.6 Software and control technologies

Programming a quantum computer requires software for translating abstract mathematical quantum algorithms into executable code, compilers to analyse the code, and support for optimising, debugging, and testing programs (Grumbling & Horowitz, 2019). Currently, many different software languages and tools are described in the literature. These include both functional languages that researchers believe are less error-prone, such as Quipper, Q#, Quafl and LIQul (Chong et al., 2017), and imperative languages, such as Scaffold and ProjectQ (Javadi-Abhari et al., 2014), which are being designed to be more resource-efficient for use on NISQs. This area of quantum development appears to be progressing quickly, with tools such as OpenQASM (Cross et al., 2022) and Forest (Rigetti, 2017) available for online use. As with quantum hardware, however, standards and benchmarks in this area are noticeably lacking (Byrd & Ding, 2023; Chang et al., 2020).

More research focus is also required in system integration software to progress quantum computers from theoretical research to engineering implementation. Technology to perform functions such as providing an optimal cryogenic environment, controlling qubit chips, and providing additional support features is still needed to close the gap between the theoretical and the practical (Serrano et al., 2023).

2.3.3.7 Debugging

Code is debugged on a classical computer by looking at the memory and snapshots of intermediate states. However, this form of debugging is not possible on a quantum machine as quantum states cannot be replicated, as any attempt to measure a quantum state collapses it and stops computation (Grumbling & Horowitz, 2019). Solutions described in the literature to address debugging in quantum software often use theorem provers and type checking to verify that programs correctly match algorithm specifications (Hung et al., 2019; Paykin et al., 2017; Ying et al., 2017). More recently, however, Huang and Martonosi (2019) addressed this problem by finding ways to debug quantum programs using information about the collapsed quantum states only. They report that using statistical tests to check quantum program assertions may be an effective method for future developers, opening a new direction for further research in this area. Additionally, researchers are now attempting to find ways to move away from manual debugging and adopt automated solutions (Pontolillo & Mousavi, 2024). It is clear however that more solutions and tools for debugging quantum software are still required (Di Matteo, 2024).

2.3.3.8 Converting classical data to a quantum state

There is no current method to convert large amounts of classical data to a quantum state. This conversion is a prerequisite for many quantum processing tasks such as collision finding, quantum searching, and quantum Fourier transforms to surpass classical approaches. Research in this area focuses on developing quantum random access memory (QRAM), a device that stores classical or quantum data and allows the

data to be queried with respect to the superposition of addresses (Park et al., 2019; Tabassum & Akter, 2023).

Givovenetti et al. (2008) first proposed a bucket brigade model for QRAM, which allowed the content of multiple data cells to be returned in superposition. However, early theoretical schemes like this and Elhoushi et al. (2011) relied upon routing elements that could introduce errors. Park et al. (2019) progressed research in this area by proposing a QRAM model based upon a quantum circuit model called flip-flop QRAM that does not rely on routing algorithms and, therefore, avoids the issues described in earlier schemes. Flip-flop QRAM is still just a theoretical model; however, and while research continues to progress in this area (de Veras et al., 2021), there are no practical implementations of QRAM research to date.

2.3.3.9 Quantum algorithms

The performance improvements that quantum computers can grant over classical computers depend on specialised quantum algorithms that can leverage the uniquely quantum features of interference and entanglement to find and output a classical result. Currently, less than 70 quantum algorithms are available online (Jordan, n.d.). These algorithms are built using completely different principles from classical computing algorithms, and most require a significant number of high-quality qubits to operate and error correction beyond what is currently available. These requirements render them impractical for current use. Until further quantum algorithms are created that can be used on non-error-corrected devices, the full potential processing power of quantum computers cannot be utilised.

Despite the limited number of useful developed quantum algorithms, several have already been created that can improve computational speed and, therefore, will significantly impact classical computing. The quantum algorithms that promise this quantum speedup rely upon three basic operating techniques: Hamiltonian simulation, quantum random walks, and quantum Fourier transform (Grumbling & Horowitz, 2019).

Hamiltonian simulation involves implementing time-evolution algorithms on gate-based quantum computers to simulate a quantum system's dynamics (Grumbling & Horowitz, 2019). If Hamiltonian simulations are implemented efficiently on a quantum computer, speedups for quantum chemistry and materials simulation could be enabled. Recently documented mathematical insights describe the achievement of significant reductions in the time required for computation using this technique (Ameri et al., 2023; Budinski, 2021; Gregory & Chiang, 2018; McArdle et al., 2020).

The quantum random walk probabilistically simulates progress in traversing terrain and is analogous to classical random walk methods (Xia et al., 2020). Grover's (1996) algorithm utilises quantum random walks to solve the problem of finding unique outputs to a given function that will result in a specific outcome, yielding a polynomial speedup over the fastest known classical approach. Practical uses for Grover's algorithm are currently being explored in the literature and are wide-ranging. They include low-light image enhancement (Dhara & Sen, 2018), pattern matching, data mining, machine learning (Cherif et al., 2023; Shrivastava et al., 2019) and in particular, quantum cryptography and cryptanalysis (Joshi et al., 2024; Jordan & Liu, 2019).

The Fourier transform is an operation that transforms a representation of a signal into a different representational form, such as turning a signal represented as time into a function of frequency (Grumbling & Horowitz, 2019). Two quantum algorithms that utilise the quantum Fourier transform could severely impact the computing world in the next decade. Created by Peter Shor, the algorithms factor large numbers and compute discrete logarithms exponentially faster than any classical algorithms available today (Shor, 1994). Shor's algorithms have generated renewed interest in quantum computing and serious concern amongst the security community because they solve problems at the core of the public key cryptosystems that currently protect much of the world's digital data (Mahmoud, 2023).

Peter Shor's algorithms give tangible proof that once the challenges of building practical quantum computing at scale have been conquered, this technology may impact several cryptographic algorithms currently in wide use. As a result, the security and privacy of data communications relying on these cryptosystems would be jeopardised (Wallden & Kashefi, 2019).

2.4 The Threat Posed to Secure Communications by Quantum Development

While the increase in computational power promised by quantum computers is desirable for many fields, applications that rely upon the computational complexity of mathematical operations to function, such as cryptography, could be negatively impacted by quantum development.

Cryptography is an indispensable tool widely used to protect information residing in computer systems and communicated across the internet. Albeit mainly hidden from the naked eye, cryptography underpins most transactions and interactions on the internet today. For example, every time online services such as PayPal and Facebook are used, or email is sent via applications such as Gmail, a secure online connection is established using hypertext transfer protocol secure (HTTPS). HTTPS provides website authentication and encrypts communications between a client and server, enabling a safe and secure online experience (Kiljan et al., 2017).

HTTPS connections rely on the use of public key infrastructure (PKI). PKI establishes a cryptographic key between two parties who wish to communicate and binds identity information to the keys to ensure the other party's identity using two critical security processes: key establishment and digital signatures. In summary, PKI helps satisfy the critical information security goals of confidentiality and non-repudiation using asymmetric cryptographic algorithms such as RSA, Diffie–Hellman (DH) and elliptic-curve (ECC) (Aydeger et al., 2024).

After PKI enables cryptographic key exchange, the data to be communicated is encrypted using symmetric cryptographic algorithms such as AES to ensure the message cannot be read by anyone other than the intended recipient (Cloud Security Alliance, 2018). The security of these internet connections is key to the modern economy. The PKI network enables an estimated 4.5 billion users to access the internet and transact in US$3 trillion dollars of retail e-commerce per year (The Quantum Economic Development Consortium, 2021). Secure PKI also enables online banking, intranets, virtual private networks (VPNs), and the remote maintenance of critical industrial infrastructure. Government and military organisations use PKI to authenticate access to secure networks and transmit highly sensitive information. PKI is also used in activities such as the remote inspection of nuclear weapon facilities to ensure they are operating correctly and have not been tampered with (Lindsay, 2020). If PKI connections are insecure, the user becomes

vulnerable to cybercrime, such as data theft and manipulation, malware injection, system tampering, or the hijacking of financial transactions.

Digital signatures are also currently used for practical security purposes, such as authenticating software updates. They commonly use RSA and ECC algorithms that rely on factoring large integers and the discrete-log problem to remain secure. If currently used digital signature schemes are broken, threats such as adversaries breaking software update keys and sending fake software updates containing malware become possible (Cloud Security Alliance, 2018).

There is always a risk that creative new mathematical methods may break the cryptographic algorithms used today. Many organisations leak confidential data even with current robust PKI systems (Verizon, 2021); hence, no technical solution can be considered entirely secure. However, quantum computing introduces such an enormous paradigm shift in the underlying technology that new threats and attacks will become possible, and perhaps even trivial, to execute (Mahmoud, 2023). Functioning quantum computing at scale will have a devastating impact on several of the main cryptographic algorithms in use in 2024.

Algorithms that enable key exchange and secure communications globally rely on the assumption that certain mathematical problems are intractable. A widely used example is the “discrete-log problem on elliptic curves”. An instance of the discrete-log problem of size n bits can be solved using classical computing systems in 2n/2. Therefore, if an ECC key size is set at 256 bits, the best attack on this algorithm can uncover this key in 2 256/2, which would take a prohibitively long time today (Grumbling & Horowitz, 2019). Unfortunately, Peter Shor’s quantum computing-based integer factorisation algorithm can break all PKI systems that use RSA, elliptic-curve and Diffie–Hellman cryptography by providing an exponentially faster way to solve problems such as the discrete log (Ekerå, 2020).

Current estimates of how many physical qubits it will take to break RSA-2048 range significantly; however, it is thought that a quantum computer containing approximately 2,500 logical qubits may break ECC-256 or RSA-2048 in a few hours, as opposed to the quadrillions of years necessary for a classical computer to complete this task (Grumbling & Horowitz, 2019). This quantum speedup means that intercepting, tampering, or just reading most communication undertaken across the internet today would become trivial for any entity possessing quantum technology.

Although most research focuses on the threat posed to asymmetric algorithms by the development of quantum computing (Aydeger et al., 2024; Cavaliere et al., 2020; Mailloux et al., 2016; Wallden & Kashefi, 2019), symmetric algorithms used to encrypt ongoing communication streams will also be impacted (Aydeger et al., 2024). Current symmetric algorithms such as AES-GCM 128-bit are considered secure against brute force attacks because using the fastest existing classical computers would still require searching 2,128 possible keys and take approximately 10 trillion years to find the correct result. However, Grover’s quantum algorithm can reduce the computational cost of attacking symmetric key algorithms such as AES and identify this same key in 264 steps. It is difficult to determine how long this would take as it is unknown how long a quantum computer will take for each step; however, estimates place this at approximately 600 years (Grumbling & Horowitz, 2019). Therefore, although a group of quantum computers would be required to implement this attack, current literature recommends that a system using

AES with 128-bit keys will need to use AES with 256-bit keys to remain secure in a post-quantum computing world (Esmaeilifar et al., 2020).

Another common security function that utilises classical cryptography is the cryptographic hash. Hash functions take an arbitrarily long message and output a fixed message digest. They are used for practical security applications such as securing password databases. Currently, SHA-256 is the most common hash function and is used as the basis for most password management systems. It is not currently thought that Grover's quantum algorithm will threaten this system, as the time it would take to break SHA-256 using Grover's algorithm is still prohibitively long. However, should quantum error correction schemes improve significantly, this situation could change rapidly, and alternative solutions to secure information beyond password use may be necessary.

Each of the classical algorithms mentioned to date is known to be vulnerable to quantum computing attacks to some extent (Aydeger et al., 2024). Once a quantum computer that can operate tens of thousands of qubits is available, many of the commonly used algorithms summarised in Table 3 will become ineffective for securing any form of communication.

Table 3

The Impact of Quantum Algorithms on Current Cryptosystems

Cryptosystem	Impact	Comments	Notes
RSA	Broken by quantum computing (Shor's algorithm)	Shor's algorithm exponentially speeds up the factorising of large prime numbers. It solves discrete algorithms, thereby breaking the security of any systems based on the hardness of prime factorisation	Currently used in digital signatures and key establishment
Diffie–Hellman (ECDH)	Broken by quantum computing (Shor's algorithm)	Shor's algorithm exponentially speeds up the factorising of large prime numbers and solves discrete algorithms, thereby breaking the security of any systems based on the hardness of prime factorisation	Currently used in digital signatures, key establishment, key exchanges
Elliptic-curve (ECDSA, ECDH, ECC)	Broken by quantum computing (Shor's algorithm)	Shor's algorithm exponentially speeds up the factorising of large prime numbers and solves discrete algorithms, rendering the security of any systems based on the hardness of prime factorisation broken	Digital signatures and key exchanges
AES-256	Impacted by quantum computing (Grover's algorithm)	Larger key sizes need to be used to ensure security	Currently used for data encryption
SHA-256, SHA-3	Impacted by quantum computing	Larger output will be required	Hash function
Code-based	Not yet broken by quantum computing	Not known to be vulnerable to quantum computing at this stage	Introduced 1970s
Hash-based	Not yet broken by quantum computing	Not known to be vulnerable to quantum computing at this stage	Introduced 1970s

Lattice-based	Not yet broken by quantum computing	Not known to be vulnerable to quantum computing at this stage	Introduced 1990s
Multivariate	Not yet broken by quantum computing	Not known to be vulnerable to quantum computing at this stage	Introduced 1990s
One time pad	Proven unbreakable – perfect secrecy	The one time pad is immune to cryptanalysis and not vulnerable to quantum computing	

Sources. Mailloux et al. (2016); Grumbling and Horowitz (2019); NIST (2020).

In summary, should a quantum computer be developed that is sufficiently large, “fault-tolerant”, and universal, then the hard problems that current cryptographic algorithms rely on for their security may be solved efficiently, rendering these current cryptosystems insecure (Wallden & Kashefi, 2019). As the global economy requires trust to operate, it would likely grind to a halt should the cryptographic systems currently allowing secure and efficient ways to transact and communicate be broken (Atkinson, 2020).

2.5 Current Proposed Solutions

Quantum computing will provide the means to break the PKI that the internet currently relies upon, and therefore, solutions are being sought to avoid a situation where conducting any personal or commercial business online is threatened. Academics have been researching post-quantum cryptographic solutions for at least 20 years (Mosca, 2018), and therefore, mature theoretical options exist in the literature in 2024 that could provide feasible, practical solutions to the threat that quantum poses.

Much research is underway to find replacements for key exchange and digital signature schemes, as the threat to these from developed quantum computing algorithms seems most immanent. The body of literature dedicated to finding these solutions is divided between research investigating post-quantum cryptography (PQC) and research to advance quantum cryptography. The field of PQC looks to design efficient cryptosystems that cannot easily be broken by current or future quantum computing capabilities (Mailloux et al., 2016). It uses conventional cryptographic algorithms whose strength is not based on the mathematical problems of factoring or discrete algorithms. In contrast, quantum cryptography uses quantum technology for communication and computation to protect communications security (Cloud Security Alliance, 2018). Some authors also propose hybrid schemes combining classical with PQC or with quantum cryptography (Campagna & Crockett, 2020; Giron et al., 2023; Ricci et al., 2024).

2.5.1 Quantum-Resistant Cryptography

Public key cryptography is still possible in a world where attackers can access quantum computers, and many documented cryptographic systems are believed to be resistant to quantum attacks. These include hash-based systems, code-based systems, lattice-based systems, multivariate systems, and elliptic-curve isogenies (Mahmoud, 2023). Numerous cryptographic schemes based on these systems are currently being explored as candidates for standardisation and use in a post-quantum world (Mailloux et al., 2016).

2.5.1.1 Hash-based systems

Hash-based systems have been studied since they were first introduced in the 1970s, and their security and performance are well understood. These systems are relatively fast, and security relies on the one-

way function's ability to avoid collisions rather than the difficulty of number theory problems (Mailloux et al., 2016).

Hash-based schemes originated with the cryptographic systems of Lamport (1979) and Merkle (1989) signatures, combining a series of one-time-use signature key pairs into a single hash tree. As these systems have minimal security requirements and the flexibility to be used with any hash function, they have continued to evolve over the years (Butin, 2018). Two more recent variants, the Leighton–Micali scheme (LMS) and the eXtended Merkle signature scheme (XMSS), have been proposed for use by standards organisations and are widely accepted to be secure when used with a strong hash function (Hulsing et al., 2018; McGrew et al., 2019). However, LMS and XMSS still have limitations in that they are stateful schemes whereby a "state" must be kept for both signing and verification, leading to the need for more storage and solutions to synchronise states across devices (Sun et al., 2020).

Solutions such as state management and hybrid state approaches have been proposed to resolve the limitations inherent in stateful schemes (McGrew et al., 2016). More recently, advances in an alternative stateless hash-based signature called SPHINCS have also been made. SPHINCS has the benefit of not needing a signer to remember past signature history to be secure (Cloud Security Alliance, 2018); however, this trade-off comes with the price of increasing the signature size and signing time. Further work is underway to optimise this system and enhance the signing speed thereby reducing its limitations for practical use (Kim et al., 2024a; Sun et al., 2020).

Overall, most hash-based schemes have advantages, such as only needing small public key sizes and using existing efficient signing and verification algorithms; however, the signatures required are large. Additionally, hash-based systems are less than ideal as they generally severely limit the number of messages that may be securely signed using each private key or operate with single-use-only private keys (Cloud Security Alliance, 2018). While further development of these schemes is required, a compelling case exists for including them in post-quantum cryptographic portfolios.

2.5.1.2 Code-based (error correction) cryptosystems

Code-based cryptosystems use error-correction codes to generate public keys from private matrices while purposefully injecting errors. They rely on a decoding problem thought to be hard against quantum attacks (Tellez et al., 2019). Code-based systems are fast because the encryption and decryption algorithms have low complexity; however, their suitability and practicality are currently hindered by their need for relatively large key sizes. Public key requirements for these systems are millions of bits (Mailloux et al., 2016).

Recently developed code-based algorithms include the code-based algorithm for key encapsulation (CAKE) (Barreto et al., 2017). The CAKE scheme creates an authenticated key exchange protocol suitable for internet key exchange and provides a fast key generation process; however, this comes at the cost of even longer public keys.

Another code-based system, the McEliece with hidden Goppa codes, has been studied since 1978 and was widely believed to be resistant to attacks (Mailloux et al., 2016). As it also requires a lengthy key, researchers are currently attempting to evolve this system by modifying it to replace Goppa codes with other irregular codes (Carita & Kabetta, 2023; Hashemi & Hodtani, 2019). These developments have already successfully reduced the key length and continue to provide optimisation.

Attempts to crack McEliece public cryptography and uncover any weaknesses are also underway in parallel with its development. Zhu and Han (2020) believe they have recently demonstrated that it is vulnerable to a chosen-ciphertext attack, highlighting the risk inherent when implementing any new replacement cryptosystem and the need for ongoing cryptanalysis research.

2.5.1.3 Lattice-based cryptosystems

Lattice-based cryptosystems depend on solving complex mathematical problems similar to the classical algorithms under threat from quantum computing (Mailloux et al., 2016). Current literature reflects the high level of acceptance that lattice-based cryptography is gaining amongst post-quantum schemes, with its use demonstrated in a wide range of areas, including key exchange, digital signatures, homomorphic schemes, identity-based schemes, and symmetric encryption (Nejatollahi et al., 2019). Lattice-based systems fit well with existing IT infrastructure, making migration to these systems potentially easier than other proposed post-quantum cryptographic solutions.

Possible lattice-based solutions for key agreement include systems based upon learning with errors, such as Microsoft's FRODO scheme (Bos et al., 2016); ring learning with errors, such as the NewHope scheme (De Abiega-L'Eglisse et al., 2020); and module learning with errors, such as the Kyber scheme (Bavdekar et al., 2023).

Lattice-based digital signature algorithms that are potentially secure against quantum computing include learning with errors, such as TESLA (Butin, 2018), ring learning with errors, and module learning with errors, including the DILITHIUM scheme (Alkhulaifi & El-Alfy, 2020). Trapdoor lattices are also used to create effective signature schemes, such as NTRUSign and BLISS (Nejatollahi et al., 2019). NTRUSign schemes seem promising as they have relatively small key sizes, are computationally strong, and have performance enhancements over current systems such as RSA (Bavdekar et al., 2023).

Whilst lattice-based systems are promising, the current literature still neglects to address the need for agility, which is a practical requirement for implementing these schemes on varying platforms. Additionally, limited current research focuses on thwarting physical attacks on these systems, so further work is required to progress lattice-based schemes into robust solutions.

2.5.1.4 Multivariate cryptography

Multivariate cryptography relies on the difficulty of solving systems of multivariate polynomials over a finite field. Solving multivariate equations is considered difficult even for a quantum computer, and therefore, it is considered for quantum-resistant cryptography (Cloud Security Alliance, 2018).

Multivariate schemes exist for both symmetric and asymmetric cryptography. They provide fast arithmetic over small binary fields, resulting in low computational overhead for signature creation or encryption. However, multivariate public key sizes are substantial, which hinders their practical implementation and use (Cloud Security Alliance, 2018).

Multivariate digital signature algorithms include unbalanced oil and vinegar (Szepieniec & Preneel, 2020), rainbow (Le Van, 2019) and Multivariate Polynomial Public Key Digital Signature (MPPK KEM) (Kuang & Perepechaenko, 2022), which offer improvements to key size if slower key generation is acceptable. However, the provable security of these schemes remains uncertain (Butin, 2018; Sparkes, 2022), and a

practical key recovery attack that returned a secret key after an average of only 53 hours of computation time on a standard laptop was demonstrated against the rainbow signature scheme in 2022 (Sparkes, 2022).

2.5.1.5 Elliptic-curve isogenies

While standard ECC can be broken simply with a quantum computer, other elliptic-curve properties can be used to create quantum-resistant key agreement schemes, such as ECDH (Cloud Security Alliance, 2018). Using the mappings (isogenies) between different elliptic curves allows a quantum-resistant key exchange of supersingular elliptic curves to be built. Known as SIDH (supersingular isogeny elliptic-curve Diffie–Hellman) or SIKE (supersingular isogeny key exchange), one advantage of this scheme is that the key size required is similar to existing key size requirements for currently used Diffie–Hellman schemes (Qi & Chen, 2022). It is also relatively easy to upgrade systems that currently use ECC to this scheme as it uses some of the same computational elliptic-curve primitives used in standard ECC (Cloud Security Alliance, 2018).

Schemes based on ECDH and SIKE continue to be evolved (Qi & Chen, 2022) however; at this stage, isogeny schemes are still very new and have not stood the test of time. Further testing is needed to ensure the security of these solutions before digital signatures based on isogenies become trusted.

In summary, the advantages of quantum-resistant algorithms include characteristics such as being more computationally efficient than the existing public key algorithms used today and generally fitting well into existing IT infrastructure. However, most quantum-resistant algorithms discovered to date require significantly larger key sizes than current public key algorithms demand. This means that large volumes of data must be transferred to create keys and exchange digital signatures to establish a secure exchange (Cloud Security Alliance, 2018). Larger key sizes also mean a greater need for storage on a device, and many new devices, such as those making up the internet of things (IoT), are already struggling or unable to meet the resource demands (including storage) of current cryptographic schemes (Kumar et al., 2022). New research is starting to provide insights into the challenges and strategies for incorporating PQC into the IOT (Kumar., 2022; Fitzgibbon & Ottaviani, 2024); however, more work is required to determine how the suggested new schemes will work in IoT-embedded systems.

European and US standards organisations are investigating quantum-resistant cryptography with the aim of developing robust new algorithms for standardisation. Along with demonstrating quantum resistance, post-quantum cryptographic schemes are assessed for suitability using three criteria: computational speed; required key length; and private key lifetime (Mailloux et al., 2016).

NIST initiated a process in 2017 of reviewing and standardising potential quantum-resistant public key cryptographic algorithms with a view to having selected suitable options by 2022 and then standardising one or more for use in digital signatures, cryptographic key generation, and public key encryption by 2024 (NIST, 2020). The NIST selection process entered round three in 2020 after winnowing down 69 submitted candidates to just 15 for final consideration. This candidate group for standardisation contained algorithms based on various mathematical approaches, including code-based, lattice-based, multivariate, elliptic-curve isogenies, and hash-based algorithms (Moody et al., 2020).

In August 2024, NIST made a final selection and released three post-quantum encryption standards. Federal Information Processing Standards (FIPS) FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204 - Module-Lattice-Based Digital Signature Standard, and FIPS 205 - Stateless Hash-Based Digital Signature Standard (NIST, 2024a). These standards will become the primary tools for general encryption and protecting digital signatures once widely adopted.

FIPS 203 specifies the public-key cryptographic scheme chosen. The public-key encapsulation mechanism used in the standard is CRYSTALS-KYBER. Three digital signature schemes were also chosen: CRYSTALS-Dilithium, FALCON, and SPHINCS+ (NIST, 2024b). FIPS 204 specifies the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), which is derived from CRYSTALS-Dilithium (NIST, 2024c). Finally, FIPS 205 specifies the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), which is derived from SPHINCS+ (NIST, 2024d).

The side-channel attack described against the FALCON algorithm (Karabulut & Asyu, 2021) and the 2022 successful key recovery attack against the multivariate signature scheme rainbow (Sparkes, 2022), one of the three schemes to make it to the NIST competition finals, highlights how new attacks will continue to be discovered against these solutions. Therefore, the selection of various systems for standardisation consideration was intended to mitigate against the likely eventuality that one or more of these new and immature systems will be broken in future years (NIST, 2020).

It is also likely that future post-quantum cryptographic standards will continue to specify multiple algorithms for different applications, as the currently proposed quantum-resistant solutions have various implementation constraints. For example, large key sizes may be suitable for some applications but not others (Barker et al., 2020).

The new public key standards will protect sensitive government information even after the arrival of quantum computing; however, new standards for quantum-resistant cybersecurity algorithms are unlikely to remain static and will most likely be much more short-lived than previous pre-quantum algorithms that remained secure for decades. This is because they will be designed based on the currently limited known information on the possibilities of quantum computing and, therefore, will not protect against a rapid, continuously evolving threat landscape (Turner, 2022). NIST also clearly advises that the standardisation process is not complete, and further algorithms continue to be evaluated for potential standardisation that rely on different underlying mathematical systems than the algorithms already chosen (NIST, 2024a).

Standardisation processes can be lengthy; therefore, the use of hybrid key management schemes has been considered. A hybrid scheme may offer a level of quantum protection immediately without having to wait for the development of further standardised post-quantum cryptographic solutions.

One early example of a hybrid implementation is Google’s attempt to use an elliptic-curve key agreement and a ring learning with errors key agreement in the Google Chrome Canary browser (Braithwaite, 2016). A quantum-safe hybrid cypher suite is also being proposed for transport layer security (TLS) as part of the Internet Engineering Task Forces Transport Layer Security Working Group. It combines ECDH with SIKE as a hybrid key agreement method; however, this specification is still in draft form (Campagna & Crockett, 2020).

Another hybrid approach that may offer short-term protection would be to simply layer PQC on top of current classical cryptographic algorithms, effectively adding defence-in-depth. Research is continuing towards developing various valid hybrid schemes that enhance quantum resistance, and this area is starting to focus more on the practical application of these schemes (Ricci et al., 2024; Smyslov, 2024).

Post-quantum cryptographic schemes appear to be practical solutions to the near-term quantum threat. These schemes offer the first widely available form of defence against quantum-driven cryptanalysis, ensuring their use in post-quantum security strategy. Unfortunately, they are not proven perfectly secure and may be potentially broken by further quantum discoveries. Therefore, parallel research into another line of defence, quantum cryptography, is also well underway.

2.5.2 Quantum Cryptography

Quantum cryptography exploits quantum mechanical laws to achieve perfect secrecy in tasks such as QKD, quantum commitment, secure multiparty computation, and oblivious transfer (Mailloux et al., 2016). It achieves this using quantum mechanics to grow and distribute private key material that can be used with the OTP encryption algorithm (Ismail & Petruccione, 2018). One benefit of using a quantum channel is that information remains secure even if an eavesdropper is present, shifting the security basis away from mathematical complexities to a physical boundary defined by the laws of quantum mechanics (Ismail & Petruccione, 2018).

Quantum technology may enhance classical security via functions such as quantum random number generation, quantum fingerprinting, quantum digital signatures, or quantum private information retrieval (Broadbent & Schaffner, 2016). The available literature covers a vast array of contemporary research topics that are contributing to these functions in areas such as quantum secret sharing (Li et al., 2024; Senthoor & Sarvepalli, 2024; Qin et al., 2020; Shi, 2020), the authentication of quantum messages (Das et al., 2024; Nikolopoulos & Fischlin, 2020; Wen et al., 2019), quantum message encryption (Liang & Yang, 2020; Moody et al., 2020), quantum homomorphic encryption (Roman et al., 2024; Kolberg et al., 2020; Zhang et al., 2020), unclonable encryption (Kim et al., 2024b; Wu et al., 2020; Zhang et al., 2019) and quantum cryptanalysis (Mathews & Ajith, 2024; Lan et al., 2020; Truong et al., 2019). However, each field is immature, and only experimental prototype implementations of some systems have been achieved to date (Han et al., 2020; Mathews & Ajith, 2024; Tusun et al., 2019). Significant questions remain unanswered, such as which cryptographic functions can be achieved using quantum protocols, whether a classical computer will ever be able to delegate private quantum computation to a quantum server and ensure privacy and non-repudiation, how quantum-secure pseudorandom permutations can be constructed, and whether device-independent protocols are possible.

Quantum physics may provide a fundamentally secure form of encryption; however, the ability to hack these systems under real-world conditions has also been proven, for example, when noise or electrical static gets introduced into the system (NIST, 2023).

The most mature quantum cryptographic research area is focused on QKD (Wallden & Kashefi, 2019). In QKD, a combination of untrusted quantum channels and trusted/authenticated classical channels are used to establish a shared secret key between two parties separated by distance with information-theoretic security. The key bits are encoded as quantum data, which can be disturbed if observed by a third party

(Wallden & Kashefi, 2019). QKD is then combined with conventional symmetric cryptography for secure ongoing communication (Sahu et al., 2024). The advantage of QKD is that, unlike post-quantum cryptographic solutions, it does not rely upon any computation assumptions that may be broken in the future (Mosca, 2018).

QKD allows two geographically separated parties to grow unlimited amounts of secure keying material for use in OTP applications, but it requires a quantum channel to send quantum bits between these locations (Mosca, 2018). These links may consist of dedicated optical channels or free line-of-sight point-to-point connections (Mehic et al., 2021). At this stage in development, quantum channels are available over relatively short distances; however, successful examples of fibre and free-space implementations exist (Sahu et al., 2024).

Since 2005, global efforts have produced functioning QKD fibre optic networks (Elliott et al., 2005; Riedel et al., 2017; Wang et al., 2010; Wang et al., 2014). China is currently leading the practical implementation of QKD after developing a 2,000km link connecting Shanghai and Beijing and further metropolitan networks in Hefei and Jinan (Pan et al., 2020; Wang et al., 2014; Zhao, 2019). These achievements demonstrate the results that a collaborative approach can yield with contributors to these networks from the University of Science and Technology of China, the Chinese Government, and various commercial parties such as China Cable Television Network Co. and the Commercial Bank of China. The link connecting Shanghai and Beijing is believed to be ultra-secure, and the project to link other major Chinese cities is ongoing (Pan et al., 2020).

Whilst dedicated fibre optic channels are ideally suited as a medium for transmitting qubits, they are not always practical to implement and are beyond the budget of small research initiatives. Free space (non-fibre) point-to-point QKD channels can be implemented at a much lower cost; however, they are limited to clear line-of-sight terrain, and researchers have only developed these up to 144km in length to date (Avesani et al., 2021).

Successful free-space implementations have also led the way for space-orientated quantum technology using satellites. Satellite quantum technology is under investigation to increase the distance by which QKD can operate as optical signals between a satellite and the ground, which can travel much further than a terrestrial link, which suffers from transmission losses due to atmospheric scattering (Jennewein, 2018). China launched a quantum satellite, “Micius”, in 2017, demonstrating a successful satellite to ground QKD up to 1,200 kilometres (Mehic et al., 2021). As earth-orbiting satellites are the only known method of enabling global-range quantum communications, various research is underway to develop these links (Ntanos et al., 2024; Djordjevic, 2020; Jennewein, 2018). Djordjevic (2020) proposed a quantum network architecture based on satellites that could provide unprecedented security levels for future technology, such as the IoT and autonomous vehicles, when moved beyond the theoretical.

Implementing QKD involves utilising single photons as quantum data carriers; however, highly efficient single-photon sources are currently not reliable or commercially available. Promising research is underway that explores two potential single-photon sources: nitrogen-vacancy nanodiamonds and semiconductor nanocrystals, also known as quantum dots (Ismail & Petruccione, 2018). Research solutions that use quantum dots appear to be the most advanced, and much progress has been made by coupling quantum

dots with photonic nanostructures (Papylev et al., 2024; Uğurlu et al., 2020; Uppu et al., 2020). Generating this source of single photons has also been tackled by Ismail and Petruccione (2018), who made early advancements in this area by proposing a prototype single-photon source based on quantum entanglement that can be used in low-cost free-space quantum channels. Ismail and Petruccione (2018) purport that this source would give the quantum channel enhanced security and plug-and-play, enabling its easy use by researchers in the field. Easy and universally available quantum solutions such as this are required to develop quantum encryption further.

Practical QKD has some additional technical barriers and limitations. Systems using QKD must employ strict keying requirements to achieve adequate levels of data security. The symmetric key must be as long as the message that is being encrypted, it may never be reused, and it must be truly random. Additionally, QKD has relatively slow key generation rates (Mailloux et al., 2016). The lack of network repeaters also limits current quantum networks from directing traffic. Theoretical designs have been proposed in the literature for these (Lan et al., 2020; Munro & Nemoto, 2020; Seshadreesan et al., 2019); however, with existing technology, they cannot currently be developed (Mehic et al., 2021) and further advancements are required in this area to allow quantum networks to expand.

As the most tested application of quantum cryptography and the only known future-proof post-quantum solution to date, several vendors have already commercialised QKD (Mailloux et al., 2016). These commercial offerings only target a niche market of banking, government, and military at this stage, are not standardised and do not have to undertake any certification of their security (Mailloux et al., 2016). Standards bodies such as ETSI, IETF, and ITU-T are beginning to introduce draft QKD network guidelines (ETSI, 2023; IEEE Standards Association, 2022; IETF, 2021; ITU-T, 2020); however, these are still evolving and will need to be mature further to support QKD progress (Mehic et al., 2021).

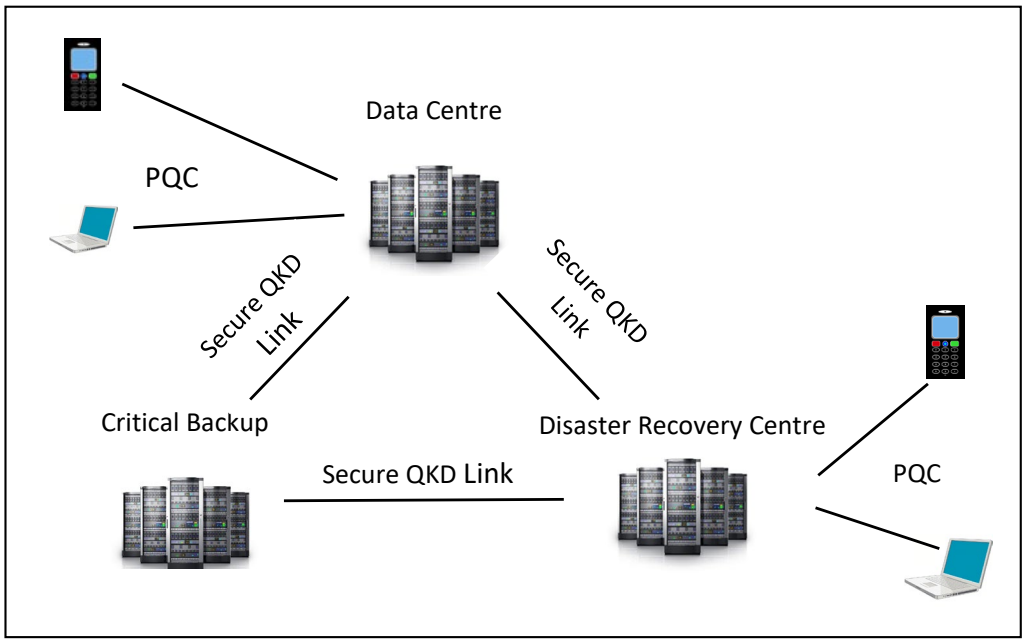
QKD has the advantage of being proven secure against future quantum developments; however, as described, it currently requires a dedicated point-to-point infrastructure and strict keying requirements, which limit its immediate practical implementation (Mailloux et al., 2016). However, with proven, albeit limited, commercial implementation in place and technology such as satellite quantum communication and quantum repeaters evolving, it seems likely that QKD will be enabled globally soon (Mehic et al., 2021).

As the challenges to implementing global QKD are still being solved, some researchers, such as Viksna et al. (2023), suggest a hybrid approach that combines quantum-resistant algorithms with QKD. In this scenario, the quantum-resistant algorithms may provide a solution that offers security at sufficient levels for current needs at a reasonable cost, whereas QKD will achieve long-term confidentiality but with high costs and disruption. An example of how this hybrid solution may deliver “good enough” protection includes using quantum-resistant algorithms to create signatures based on hash functions, along with QKD based key establishment to obtain a set of cryptographically unbreakable keys in a public key environment (Viksna et al., 2023).

Another example of a possible hybrid architecture is shown in Figure 1, which demonstrates how combining post-quantum cryptographic solutions with QKD may be used to secure a wider network.

Figure 1

Example Hybrid PQC and QKD Network Architecture



Hybrid designs such as those described may offer a pragmatic, near-term secure solution; however, these have not yet been practically demonstrated.

2.6 Other Potential Cyber and Ethical Implications of Quantum Technology

Along with the known threat to cryptography, the evolution of quantum computing may pose several additional, albeit less well-understood, challenges in the cyber landscape.

Authors such as Coenen et al. (2022), Roberson et al. (2021) and Possati (2023) describe how disruptive technologies such as quantum computing can create risks to the stability of globally contested areas such as space, air, sea, and cyberspace. This instability may lead to geopolitical power shifts and may interfere with and erode existing democratic processes.

Literature also describes how the evolution of quantum computing may also exacerbate current inequalities seen in the digital landscape. For example, it may contribute to marginalising minorities, further eroding privacy, accelerating climate change, and when combined with additional emerging advanced technologies such as artificial intelligence (AI), change the collective psyche of society by influencing thought (Charlet & King, 2020; Kavanagh, 2021; Roberson, 2023; Vermaas, 2017). While some of these threats are not unique to quantum computing, researchers believe it could accelerate and enhance these threats well beyond our current understanding of them (Possati, 2023; Manning, 2020).

The development of quantum computing has clear implications for national security. Anyone accessing large-scale general-purpose quantum computing will have a significant signals intelligence advantage, including the ability to decrypt most pre-quantum encrypted data. Additionally, as classical computing is now an essential component driving almost every industry, any advances in quantum computing will significantly change many industries and may enable economic advantages through complex financial market modelling and precision risk management (Hosseini et al., 2023). Current literature suggests that the ability of nations to innovate, adapt, and protect against emerging technologies such as quantum computing will determine their geopolitical and economic strength moving forward (Rim, 2023). However,

the goal of being prepared to protect a nation against the threat that quantum computing may pose to a secure digital economy will be more challenging to overcome for some nations than others.

Quantum technology is very specialised, and building and maintaining a quantum infrastructure requires a stable government, a reliable power grid, roading infrastructure, and a highly educated population (Wallden & Kashefi, 2019). The number of entities capable of building this technology is limited to those with the significant wealth required to invest in necessary components such as shielded facilities, supercooling technology, rare materials, and intellectual capital. A valid concern expressed by several authors is that poorer nations will not have the ability to build quantum-safe cryptography into all facets of their economy (Manning, 2020; Wallden & Kashefi, 2019; World Economic Forum [WEF], 2022b). This inability may leave them even more vulnerable on the global stage, as they may be more susceptible to attacks such as the compromise and alteration of all records from their bank accounts or government reports. Researchers have also highlighted how the efforts to weaponise quantum have already begun. Der Derian and Wendt (2020) cite information leaked by Edward Snowden that discusses the US national security imperative to research quantum computing and conduct surveillance on nations and corporate powers pursuing quantum communication technology. Manning (2020), Kavanagh (2021), and Burton and Christou (2021) all describe how quantum technology is being used in military applications to revolutionise warfare with potential unintended consequences.

The pace of quantum technology development is unlikely to be linear or evenly distributed, and development may come in bursts as each new technology is commercialised. Currently, clearly documented global pockets of concentrated venture capital and scientific research give select countries and regions an obvious advantage. This geographic divide in innovation is likely to continue, and authors such as Roberson et al. (2021), de Wolf (2017), Vermaas (2017) and Der Derian and Wendt (2020) believe this may portend a technology-driven hierarchy among nations. This is of concern as it will reinforce and increase inequality within and between nations and exacerbate the current digital divide. The potential power chasm between those with quantum computing and those without could also play out in the private arena. Should a private company develop quantum computing before anyone else, it may be able to dominate an industry, gain access to all trade secrets, and supply quantum power to the highest bidder, even if that entity uses it in ways detrimental to others (Manning, 2020).

There is a growing body of literature discussing quantum and emerging technology's influence on geopolitics due to the recognition that emerging technologies may have the power to change the global power balance. Johnson (2019) and GESDA (2022) believe the recent increased defence spending in emerging and disruptive technologies demonstrates an acceleration in the trend for digital technologies to change the character of conflict and the strategic political landscape and describe how it is becoming challenging to predict the future of geopolitics due to emerging digital technologies such as quantum computing. GESDA (2022) describes how traditional theories on international relations have tended to assume and be based upon the notion of "states" and several powerful states, but this does not remain strictly true in the digital world where any group of people with access to transformative capabilities may use these to forward their own agendas.

Overall, the recent body of literature suggests that current global politics seem to indicate increasing geopolitical competition and the unravelling of legacy economic and political institutions and agreements

(Farrand & Carrapico, 2022; Lee et al., 2024; Roberson et al., 2021; Trager, 2022). GESDA (2022) explains that while elements of multilateralism and state cooperation are still apparent, greater polarisation is being seen globally on global security and leadership issues, creating a complex geopolitical environment.

As quantum computing could drive a large geopolitical power imbalance, authors such as Atkinson (2020) and Johnson (2019) explored how this scenario may be mitigated to avoid harm. One suggestion is to regulate the use of quantum computers in a way that is similar to how nuclear power is regulated. One example of how regulation could be developed is ensuring all quantum computers are owned and operated by government entities and only allowing private companies closely monitored access. Another quite different strategy may be to increase global access to quantum computing by requiring all private quantum computers to save some capacity for computations submitted via the public cloud. Finally, supporting all nations to switch to quantum-resistant cryptography must be a priority if maintaining global economic stability and equity is of concern (NIST, 2024e).

A related and growing area of research is the general regulation of “big technology” or private technology companies. As Lindman et al. (2023) and Manning (2020) described, a small collection of US and Chinese-based firms, including Facebook, Google, Apple, Amazon, Microsoft, Alibaba, Baidu, and Tencent, arguably dominate the global technology sector. This situation leads to questions such as who should determine the ownership, use or sharing of data and whether monopoly practices could distort innovation. These issues are also reflected in the quantum technology discourse, where there is significant concern that quantum development will only focus on use cases for profit rather than societal good (GESDA, 2022). The current literature is calling for a common approach to regulating Big Tech to ensure policy issues are addressed at a global level as well as a national one (Lindman et al., 2023; Manning, 2020), and the outcome of this debate will heavily impact quantum computing as the development of quantum technology is dominated by big technology companies in the private sector.

Coenen et al. (2022) argue that further examination of the factors that could influence the ability of quantum computing to change geopolitics or impede the democratic potentials of a quantum-enabled world is necessary. One such factor is the language used to frame the quantum technology discourse. Currently, the language used to discuss and describe quantum technology leans heavily on notions of competition, battle, and supremacy, with quantum technology capability increasingly being referred to as a tool that may frame geopolitical power moving into the next century (Liman & Weber, 2023). To demonstrate this rhetoric, Coenen et al. (2022) cite how French President Emmanuel Macron frames quantum technology as a scientific battle for dominance in stating, “We are aware of the Chinese and American competition but – today we have the recipe for success and for being among the top players in this battle” (p.2). Other researchers, such as Burton and Christou (2021), also highlight the negative impact this framing may have on society’s true understanding of the topic.

Some literary discourse is centred around the concept of “quantum supremacy” and the appropriateness of the use of terms such as “supremacy” due to associations with colonialism, imperialism and the anglophone contexts that surround it (Palacios-Berraquero et al., 2019; Roberson et al., 2021; Wiesner, 2017). Quantum supremacy designates a threshold event in quantum computing evolution whereby a quantum computer efficiently solves a problem not feasible by classical computing; however, the

associations of the term “supremacy” with ideas of imperialism, colonialism and White supremacy have led to authors suggesting it be replaced (Roberson et al., 2021).

A shift in language from "quantum supremacy" to "quantum advantage" has gained traction since these concerns were raised with the term “quantum advantage” seen as a more inclusive alternative that represents the broader idea that quantum computers should provide a significant benefit without implying dominance or exclusion. As a result, many researchers and industry bodies have now adopted this term (IBM, n.d.; Hoefler et al., 2023). Others disagree, however, highlighting that changing the name itself will not change the ideological values that make quantum supremacy an appealing target to achieve and to incite competition between organisations and nations (Coenen et al., 2022). These contradictions highlight that sufficient research to explore the impact the language of quantum technology has on societal beliefs and actions is yet to be undertaken. However, the foundational research does suggest that more caution be applied in the framing, language, and articulation of terms when forming policy agendas, roadmaps, and technical standards in this field, as the way we talk about quantum technology will set expectations and may influence reactions and responses to the topic (Coenen et al., 2022).

Some authors believe that more technology-driven change will occur in the next 20 years than at any other time in human history (Charlet & King, 2020). This change, driven by converging technologies such as AI, big data, biotechnology, IoT, nanoengineering, robotics and quantum computing, may have profound ramifications in our social, geopolitical, and economic landscapes (Manning, 2020). Therefore, additional but minimally explored ethical and security concerns exist when discussing quantum computing, including questions such as how free speech, individual privacy, or data sovereignty is maintained in a world where governments or large private institutions with quantum computing can decrypt all communications and utilise enhanced search algorithms for data mining.

Chen (2020) argues that technology has enabled the death of privacy by aggregating data and giving power to those who hold that data. In doing so, it has also marginalised some minorities and exacerbated existing inequalities. This view is supported by Kukutai et al. (2020), who investigated the erosion of data sovereignty and privacy in NZ. The researchers discuss how NZ data colonialism is characterised by the role of private corporations extracting and controlling data for economic benefit and is supported by the underlying technology. Citing how state and private organisations routinely use CCTV, GPS, wearable devices, and social media to track and monitor groups and individuals in NZ without requiring active consent or providing the ability to opt-out, the researchers illustrate the erosion of data privacy and sovereignty. Kukutai et al. suggest that NZ must consider new ways to think about and structurally support individual data privacy, highlighting the possible use of Māori data sovereignty principles developed by Te Mana Raraunga (Kukutai et al., 2020), which describe an ethical and inclusive approach to data ecosystems for the collective good.

While still unclear, the evolution of quantum computing may also impact the ability of NZ to address data colonialism and contribute to further erosion of data sovereignty. Quantum computing could enhance data privacy issues, and its rapid adoption may leave little time for NZ to address the existing structural ways of thinking about data sovereignty and design a future that reflects all cultural views of data and digital sovereignty. Therefore, if data sovereignty and cultural inclusivity are important to New Zealanders, further examining how quantum computing is used will be necessary.

Another concern highlighted in recent literature is the potential for quantum computing combined with AI to impact democracy due to enabling government surveillance technology (Gangwar et al., 2022) and increasing general cyber risk (Axon et al., 2020). AI has already been used as a mechanism to enhance authoritarianism (Kavanagh, 2021; Manning, 2020), with facial recognition and big-data digital monitoring being used for social control in countries such as China. Quantum computing could enormously impact deep-learning AI by making it exponentially more powerful (Nivelkar & Bhirud, 2021; Possati, 2023; Valdez & Melin, 2023), exacerbating these current concerns.

Other risks related to the development of AI in cybersecurity include the development of autonomous malicious software. By learning from contextual information, AI can find and target vulnerabilities or mimic trusted systems, effectively evading detection to maximise damage (Manning, 2020). It is believed that quantum computing will enhance these AI abilities as the benefits of running machine learning and search algorithms on quantum computers, such as the ability to solve problems with smaller datasets, have been well-documented for years (Vermaas, 2017; Ying et al., 2017). Additionally, the possibilities of quantum speedup for machine learning are already being demonstrated (GESDA, 2022; Manning, 2020; Nivelkar & Bhirud, 2021). The synergy of emerging technologies such as AI, big data, and quantum computing may exponentially change the cyber conflict landscape and increase the volume, severity, and novelty of all cyber risks. Continued research is required to understand these impacts and find ways to mitigate them fully.

Finally, the role quantum computers may play in many other troubling issues, such as weaponised social media, misinformation, and distributed denial of service (DDoS) or malware attacks, is yet to be explored or understood. Some researchers focused on the ethical threats of emerging technology have chosen to exclude quantum computing from the scope of their studies for reasons such as accessibility, uncertainty, and the view that it is an infrastructural technology only (Quach et al., 2022); however, as the issues described previously are seen to be already causing harm and threatening social cohesion (Manning, 2020) the positive or negative role quantum computing will play in these issues is a gap that warrants further attention.

The complex ethical and moral issues outlined in this section suggest that the transition to a world with quantum computing is not straightforward, and governments may need to take a leading role in guiding the introduction of this technology. However, at this stage, only conceptual legal or policy-based frameworks have emerged to support the governing of quantum technologies, which is a gap that requires careful consideration (Possati, 2023; Johnson et al., 2020).

Current literature recognises the limited, disparate, and imperfect structures that exist globally to govern technology and the global digital landscape (Charlet & King, 2020; Johnson, 2019; Possati, 2023) and many authors agree that new standards, codes of conduct, and standards for using emerging technologies are required to avoid a situation of decreased global stability (Charlet & King, 2020; Genus & Stirling, 2018; Johnson, 2019; Roberson et al., 2021; Trager, 2022). For example, quantum computing could potentially disrupt global economic commerce, which relies on transparent, open scientific, academic, and commercial global data flows; however, as highlighted by Manning (2020), no common global framework outlines trade rules for governing electronic commerce. The World Trade Organization has agreements covering many services and some IP rights; however, these only offer a partial framework with numerous gaps in the

digital governance of the current environment. Trager (2022) also emphasises how new challenges arising from emerging technology are not yet addressed in any comprehensive fashion.

The literature describes how several, not entirely compatible, digital regimes seem to be evolving globally, with China, the EU, and the US all taking different data privacy approaches and countries such as China and Russia claiming a doctrine of “internet sovereignty” (Beattie, 2018). While there is debate on the practicalities of global technology regulation and frameworks and acknowledgement that it is unclear how new rules and codes of conduct are created in the emerging technology landscape (Manning, 2020), many authors are arguing for minimum standards for emerging technology to be agreed globally to avoid the evolution of even greater conflicting digital regimes (Charlet & King, 2020; Genus & Stirling, 2018; Roberson et al., 2021; Trager, 2022).

In response to widespread ethical concerns in technology development, research into “Responsible Innovation” (RI) has started to flourish (Boenink and Kudina, 2020; Randles et al., 2024; Roberson, 2023). Originating to address advancements in fields like nanotechnology (Fisher & Rip, 2013), RI aims to anticipate and address societal impacts before technologies become entrenched (Inglesant et al., 2021). It is an approach that integrates ethical foresight, societal engagement, and proactive governance into the development of emerging technologies and has evolved through various applications, including artificial intelligence, robotics, and more recently quantum computing (Inglesant et al., 2021).

Researchers are now advocating for robust RI frameworks to guide quantum computing's development responsibly by balancing innovation with societal accountability and inclusivity (Ten Holter et al., 2022). Some studies are taking this research even further by exploring specific challenges in operationalising RI (Randles et al., 2024; Ten Holter et al., 2023), and developing frameworks that aim to provide actionable steps for embedding ethics into specific quantum areas such as research and development (Kop et al., 2024a; Kop et al. 2024b) and quantum education (Arrow et al. 2023).

The emphasis of the current research in this area is on proactive and interdisciplinary approaches to quantum ethics (Kop et al., 2024a). This demonstrates good progress toward shaping an equitable and socially responsive quantum future; however, continued work is required to overcome the wide-ranging and unique (Possati, 2023) ethical challenges that quantum technology poses.

2.7 Global Response to the Quantum Technology Evolution

Globally, many governments appear to be taking the quantum technology threat seriously and are working to prepare for a post-quantum computing world (Mone, 2020). The rise of investment in quantum technologies has been called “the second quantum revolution”, and a so-called quantum “space race” is currently underway to determine which nations will succeed in producing fully functioning quantum computers first (Johnson, 2019).

Advancements in quantum technology, alongside progress in fields such as artificial intelligence, robotics, the Internet of Things (IoT), and nanotechnology, are set to propel the Fourth Industrial Revolution at an exponential pace. It is thought that global leaders in this domain will experience profound and transformative impacts from investing in quantum technology that include bolstering industrial capabilities, generating employment opportunities, and enhancing economic growth and national security (WEF,

2024b). Therefore, it is prudent to review the investment and actions of the leading nations in quantum technology to identify the level of response underway globally. Exact investment figures are debated; however, it is thought that seventeen countries to date have launched quantum technology programmes that range from million to billion-dollar investments (WEF, 2024a).

2.7.1.1 China

China has been aggressively pursuing research and development in quantum communication since 2006. The exact public funding amounts for quantum information systems research in China are unknown; however, researchers estimate China has committed up to US$17 billion to quantum advancement with plans in place for immediate, medium, and long-term initiatives (Chang et al., 2022; Jakob, 2023; McKinsey & Company, 2023; Swayne, 2023; WEF, 2024b). This investment has yielded results for China, enabling it to place the first quantum satellite in space and declare the achievement of quantum supremacy (Grobman, 2020). This investment also appears to be growing a thriving quantum ecosystem, with over 30 quantum technology companies thought to be actively operating in China (Jakob, 2023). The Chinese Government is also reported to have spent approximately US$11.4 billion building the National Laboratory for Quantum Information Sciences based in Hefei, which will further support quantum innovation and national defence initiatives (Jakob, 2023; Johnson, 2019).

By 2030, China aims to expand its quantum communication infrastructure, develop a prototype of a practical quantum computer, and construct a practical quantum simulator. China's 14th 5-year policy plan, released in 2021, declares quantum technology a key pillar of Chinese technical sovereignty. With state funding estimated to comprise over 50% of the world's public spending on quantum computing, China may be leading the field in quantum evolution (Center for Security and Emerging Technology, 2021; Jakob, 2023).

2.7.1.2 US

As early as 2015, the NSA announced the need for national security systems to start preparing for the current PKI cryptography to be replaced with quantum-resistant cryptographic solutions, and the US Government purportedly invested approximately US$249 million in quantum information sciences in the subsequent 5 years (Chang et al., 2022). However, this was a significantly lower amount than geopolitical rivals China, and whilst the US has traditionally led capability in signals intelligence and national secrets protection, experts such as Grobman (2020) believe the large gap between the US and Chinese investment may have led to a significant disadvantage for the US in signals intelligence.

The US fiscal 2021 budget request included increased funding for future industries, including quantum information sciences (QIS), with US$210 million for the National Science Foundation and US$237 million for the Department of Energy for Quantum Research (The White House, 2023). US$25 million was also proposed to build a quantum internet connecting 17 national labs (Metz, 2020). These 2021 investment levels demonstrated a fivefold increase in quantum investment since 2017 and were purportedly driven partly by the concern that rival nations will gain a quantum advantage over the US, putting national security at risk (Lindsay, 2020).

In 2022, the WEF estimated the total US public investment in quantum technologies had increased to approximately US$1.2 billion (WEF, 2022a), and in 2024, researchers once again significantly lifted this

estimated total to approximately US$3.75 billion (McKinsey & Company, 2023; Swayne, 2023; WEF, 2024); however, these figures are debated as some public initiatives in this area are unlikely to be disclosed due to national security concerns. Despite the growing level of public investment, the estimated total amounts are still lower than those seen in China and the EU, and private investment is thought to be driving many of the advancements in quantum technology in the US (McKinsey & Company, 2023).

2.7.1.3 EU

The EU launched the US$1.1 billion EU Quantum Flagship Programme in 2018 (European Quantum Flagship, 2020). Lasting for 10 years, the programme aims to unite scientists and research institutes across the EU and accelerate the commercialisation of QIS research. The programme was formed after EU scientists highlighted the need for a large-scale initiative to compete with competing global research teams to corner the quantum technology market. They also cited protecting national security as a key driver for the investment (Blau, 2017).

Levels of investment in quantum development increased significantly in the EU between 2021 and 2023, signalling that the EU intends to become a world leader in quantum innovation. It is now estimated that the EU has now committed approximately US$8.4 billion total in quantum computing (McKinsey & Company, 2023; WEF, 2022a), and in 2023, a European Declaration on Quantum Technologies was signed that aims to make the EU the “quantum valley” of the world and outlines the highest level of public funding for quantum technologies in the world (European Commission, 2023).

2.7.1.4 Japan

Japan was an early leader in quantum technology, demonstrating the world’s first superconducting qubit in 1999 (Nature Research, 2024). The Japanese Government planned to invest approximately US$276 million in quantum research in 2020 (Oshikawa, 2019); however, this public investment has significantly increased to an estimated total of US$1.8 billion (McKinsey & Company, 2023).

Japan aims to produce 100-qubit quantum machines by 2030 and more powerful machines by 2039, signalling its intent to catch up with China and the US in the race to build general-purpose quantum machines. To achieve these goals, the Japanese Government launched a quantum research and development programme named “Moonshot,” intending to create a fault-tolerant universal quantum computer by 2050 (Cabinet Office, Government of Japan, n.d.; Nature Research, 2024).

2.7.1.5 UK

The UK committed US$2.7 billion to develop quantum technologies in the UK from 2024–2034 (Department for Science, Innovation and Technology [DSIT], 2023b) and the WEF estimate this has increased to US$4.3 billion in 2024 (WEF, 2024b). The UK’s National Quantum Strategy outlines initiatives to support quantum technologies in the UK across quantum computing, sensing, timing, imaging, and communications. Research hubs, including universities partnering with industry and government organisations, were created to focus on specialised areas of quantum technology, including secure communications (Kaur, 2023), and the UK have focused on five areas of quantum ecosystem development, including stimulating market opportunities and applications in the UK, enabling a strong

foundation of capability in the UK, creating a skilled UK workforce, creating the right regulatory context, and maximising benefit to the UK with international cooperation (DSIT, 2023a).

Quantum technologies are recognised as one of the UK Government's five critical technologies as outlined in the UK Science and Technology Framework (DSIT, 2023b). Some of the planned initiatives include a competition to develop quantum computing hardware prototypes funded by The UK Research and Innovation Technology Missions Fund and the UK's National Quantum Computing Centre and a project to accelerate the use of quantum computing in government by the Quantum Catalyst Fund (HPCWire, 2024).

2.7.1.6 The Netherlands

In 2019, the Netherlands published a National Agenda of Quantum Technologies. Focusing on the four main ecosystem development areas of human capital, market creation and infrastructure, research and innovation, and societal dialogue on quantum technology, it aims to place the Netherlands as a world leader in this area (Quantum Delta Nederland, 2019).

Approximately US$147 million has been invested in the Delf University of Technology's quantum technology institute, and in 2021, the Netherlands Government announced an additional investment of approximately US$684 million in quantum computing research and development (Ferranti, 2021).

The Netherlands continues to advance research collaboration via the quantum technology research institute QuTech, which is a collaboration between the Delft University of Technology and the Netherlands Organisation for Applied Scientific Research (QuTech, 2024) and the WEF estimate they have now invested up to US1 billion on quantum initiatives (WEF, 2024b).

2.7.1.7 Germany

Germany introduced a framework to bring quantum technologies to market in 2018. They allocated approximately US$705 million to this programme, which encompassed many of the themes seen in other global programmes, such as informing the German population about quantum technology and ensuring the security and autonomy of Europe in a new quantum environment. An additional approximately US$2.2 billion was committed in 2020 to support progress (Kaur, 2023).

In 2023, Germany is believed to have committed approximately US$2.7 billion to its quantum strategy (Swayne, 2023). The German Government's *Action Plan for Quantum Technologies* aims to establish Germany as a world leader in quantum technologies and focuses on bringing quantum technologies into practical use, driving targeted technology development in quantum computing, and creating a strong quantum ecosystem (QBN, 2023).

2.7.1.8 Russia

In 2019, Russia committed to spending approximately US$663 million on basic and applied quantum research. Quantum computing and quantum communications, along with their enabling technologies, were described as the key focus for the research laboratories (Kaur, 2023).

Quantum research programmes have been in place in Russia since 2015 at the Lebedev Physical Institute of the Russian Academy of Sciences and the Russian Quantum Center (RQC) (RQC, 2024). Russia has already developed a 20-qubit quantum computer as part of a roadmap on quantum computations and has

announced an aim to make a 50-qubit computer by the end of 2024 (TASS, 2023). The Russian Government also announced it would invest US$790 million in quantum computing research from 2021–2026, indicating greater aspirations to lead in this technology (Swayne, 2024b).

2.7.1.9 South Korea

The South Korean Government have described a goal to launch a 20-bit quantum cloud service by 2024, a 50-qubit quantum cloud service by 2026, and a 1000-qubit service by 2032 (Ji-Seop & Kim, 2024). The South Korean Government have already invested approximately US$40 million to develop core quantum technology and around US$12 million towards developing next-generation supporting technologies (Venegas-Gomez, 2020). A plan to collaborate with the Netherlands to operate an Advanced Semiconductor Academy and advance research in advanced quantum-supporting technologies is designed to secure South Korea's global position in strategic technologies and total investment in quantum is expected to be around US$2.35 billion by 2024 (Swayne, 2024a; WEF, 2024b).

2.7.1.10 Australia

Federal funding has provided over US$98.5 million for developing quantum technologies in Australia to date. In 2017, two early quantum-focused centres of excellence were established, the first at Monash University and the second at the University of Melbourne. Further to these research centres of excellence, the Centre for Excellence for Quantum Computation and Communication Technology was created and has worked to raise the public profile of quantum technology in Australia significantly (Centre for Excellence for Quantum Computation and Communication Technology, 2024).

Australia launched a National Quantum Strategy in 2023, centred around five themes: research, development, investment and the use of quantum technologies; developing a quantum computing workforce; access to quantum infrastructure; standards that support national interests; and an ethical quantum ecosystem (Department of Industry, Science and Resources [DSIR], 2023). In 2023, the Australian Government also committed approximately US$40 million to assist organisations in integrating quantum technology into their businesses and the WEF estimate a total public sector quantum investment of approximately US$599 million to date (WEF, 2024b).

2.7.1.11 Singapore

The WEF (2024) estimates that Singapore has announced at least US$138 million of government funding for quantum initiatives. Singapore has launched three quantum initiatives since 2020 as part of its National Quantum Engineering Programme (QEP) and has committed approximately US$17.5 million towards these to date (Kurohi, 2022). Firstly, Singapore has invested in creating a National Quantum-Safe Network (NQSN) (Infocomm Media Development Authority, 2023). The NQSN aims to deploy commercial quantum-safe technologies for government agencies to trial and support organisations in adopting quantum-safe technologies (National Quantum-Safe Network Singapore, n.d.).

Secondly, Singapore's Deputy Prime Minister Heng Swee Keat announced the creation of the National Quantum Computing Hub in 2022, which combines expertise and resources from Singapore's Centre for Quantum Technologies (CQT) and other institutions. CQT has already published over 2,000 scientific papers and trained over 60 doctoral students in quantum science (Kaur, 2023). Additional funding is

intended to drive further research and ultimately allow the hub to host Singapore's first quantum computer (Quantum Engineering Programme Singapore, 2022). Finally, the National Quantum Fabless Foundry was created to develop quantum computing components and materials (Institute of Materials Research and Engineering, 2023).

2.7.1.12 India

India's Indian Institute of Science (IiSc) has a dedicated quantum technology research area that investigates single-photon sources and detectors for quantum communications, photonic quantum networks, and quantum sensors (IiSc, n.d.). A National Mission on Quantum Technologies and Applications was launched in 2020 with an initial investment of approximately US$1 billion (Kaur, 2023). In 2023, India's Department of Science and Technology announced a further investment of approximately US$740 million for its National Quantum Mission (NQM) (Department of Science and Technology, 2024). The NQM's objectives are to explore the application of quantum technologies in quantum computing, quantum sensing, and quantum materials and devices, with the aim of being internationally competitive in this area.

2.7.1.13 Israel

Google's research centre in Tel Aviv is actively researching quantum computing, and the government indicated in 2018 that it would assign US$390 million to a 6-year national quantum science and technology programme (WEF, 2024b). In 2022, The Israeli Innovation Authority and the Defense Ministry further announced an investment of US$62 million to establish a national quantum research centre and develop Israel's first quantum computer (Ben-David & Toi Staff, 2022).

2.7.1.14 France

France has committed over US$2.2 billion of public funds to quantum research (WEF, 2024b). In 2020, France launched a national strategy for quantum technologies that focuses on developing quantum computing, quantum sensing, and quantum cryptographic and communication solutions (Government of France, 2023). Strategic recommendations for their 2020 plan included delivering a tailored economic strategy, establishing effective governance, deploying cutting-edge quantum computing infrastructure, and launching an ambitious technological development programme. France also aims to develop at least two quantum computers with 128 logical bits by 2030 (Swayne, 2024b).

2.7.1.15 NZ's response to the quantum threat

While not investing at the levels seen by China, the EU, Japan, and the US, NZ has invested approximately US$36 million in quantum technologies to date (WEF, 2024b). This public funding has enabled the establishment and ongoing research of the Dodd–Walls Centre of Research Excellence, which focuses on quantum optics, photonics, and precision atomic physics (Dodd–Walls Centre, 2022).

In 2022, the NZ Government updated the New Zealand Information Security Manual v3.5 to include guidance on the impact of quantum computing on cryptographic algorithms (GCSB, 2022b) and in 2023, the Director General of the GCSB announced that NZ was working alongside overseas partners to counter the threat that quantum computing will pose to cryptographic systems globally (Hampton, 2023).

Despite the challenges of building a working quantum system, the efforts being directed into this area globally suggest that at least one, if not more, nation-states will further develop this technology. Therefore, all countries must plan for a time when increased quantum computing is a reality.

2.8 Preparedness for a Post-Quantum World

2.8.1 Response Timing

Various experts agree that organisations need to plan now for their systems to be resilient to upcoming quantum attacks (Grumbling & Horowitz, 2019; Mone, 2020; NIST, 2024e; Wallden & Kashefi, 2019). However, quantifying this threat and the urgency around which it must be addressed is difficult as the threat remains theoretical. This difficulty has led to a perceived and likely actual level of inertia from organisations, with one global survey indicating that only 40% of those surveyed were currently working to future-proof data and systems against the quantum threat (DigiCert, 2019).

Delaying any move to cryptographic algorithms that can resist quantum attacks poses risks and may lead to contemporary real-world implications. For example, as security can be broken retrospectively, an attacker could start to capture ciphertext (encrypted communications) and key establishment data sent today and break this later using a quantum computer (NIST, 2024e). Another risk posed by not immediately addressing the quantum threat is that information digitally signed today may not be trustworthy as soon as a quantum computer is available. An attacker could change the digital signature or repudiate ever signing or sending information earlier signed with non-quantum-resistant signatures (Mone, 2020). Additionally, large-scale products manufactured today, such as automobiles, power plants and trains, rely on embedded devices that will likely still operate beyond the time quantum computers become a reality, placing them at risk (Mone, 2020).

Mosca (2018), Wallden and Kashefi (2019), and NIST (2024e) all attempted to define the threat quantum computing poses to individual organisations by describing the critical factors an organisation must consider when planning quantum-resilient information systems. These factors include the time remaining before quantum computers break current security protocols, the length of time a business requires their information to be protected, and the time it will take to migrate to any new solution.

Firstly, to determine how imminent the quantum threat may be to all organisations and how hastily they need to start responding, the time remaining before quantum computers break the currently deployed PKI should be considered. Research has estimated a 16.67% chance that quantum systems will break RSA-2048 encryption before 2027 and a 50.00% chance that it will be broken by 2032 (Mosca, 2018). These estimates were made after considering when the design of a fault-tolerant scalable qubit may be achieved, how many physical qubits will be required to break RSA-2048, and how long it might take to scale the design to a size sufficient to break RSA-2048. Whilst these timeframes are estimates only, prudence suggests that cybersecurity professionals should not expect it to be any further than 10 years away and should plan accordingly (NIST, 2024e).

Secondly, the urgency around transitioning to quantum-safe systems partially depends on how long an organisation is required to keep the information they hold or send secure and, therefore, how long they require their current cryptographic keys to remain secure (Grumbling & Horowitz, 2019). This duration will

differ between organisations, as health information, trade secrets, or national security information may require a secure shelf life of 100 years or more, whereas systems that only use real-time security may have a secure shelf life of 0. For example, the US Department of Defence protects sensitive information for a minimum of 25 years (US Department of Defense, 2016). Therefore, if a stable quantum computer becomes available within the next 25 years, any information they are attempting to secure today using classical cryptosystems may not be secure for this minimum specified period. In contrast, if a business has short-lived security requirements, it may be able to wait longer to transition to a post-quantum solution (Mailloux et al., 2016).

Finally, deploying a set of new tools or new quantum-safe cybersecurity mechanisms is not instantaneous; therefore, migration time must be considered when businesses plan to protect themselves from future threats. Migration time could differ from 1 hour to implement a simple auto-update to more than 10 years for an untested brand-new public key encryption system that needs industry standards agreed upon by many stakeholders (Mosca, 2018).

Developing and implementing new crypto security systems involves numerous steps, such as:

- Vetting and agreeing on standards
- Converting standards into multiple computer languages
- Developing hardware and code libraries
- Incorporating new standards into all new and existing products
- Re-encrypting existing data with the higher standards
- Re-issuing public key certificates
- Testing the compatibility of the new standards with all existing applications, servers, and browsers
- Updating a wide range of documentation, including security procedures
- Maintaining existing cryptographic systems until all consumers and businesses have updated their systems (Atkinson, 2020).

History has shown that undertaking these steps and changing existing cryptographic systems is not fast. For example, the announcement to increase the RSA key size from 1024–2048 bits took a minimum of 10 years to be widely implemented, and transitioning from RSA to elliptic-curve solutions took a similar period (NIST, 2024e). Additionally, the SHA-1 cryptographic hash has been known to be insecure since 2004, and yet, in 2020, it was still in use in servers and browsers that did not support SHA-256 (Grumbling & Horowitz, 2019).

Many IT systems are not designed to support rapid changes to cryptographic primitives and algorithms without significantly altering the overall infrastructure. Therefore, any changes to cryptographic mechanisms and processes currently being used may involve extensive manual effort (Barker et al., 2020).

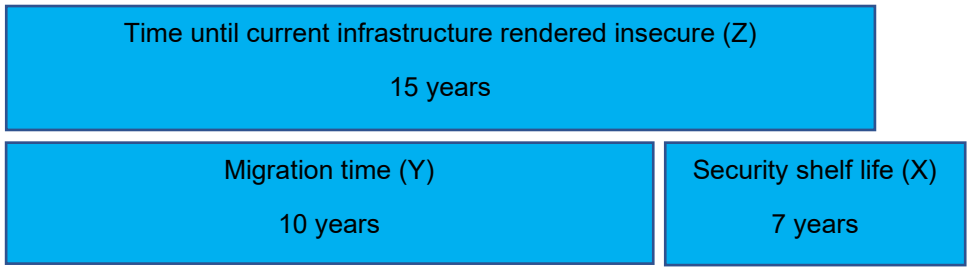
Additionally, cryptographic algorithms often cannot be replaced until all system components are ready to process the replacement. This means it can be incredibly disruptive and time-consuming as introducing new algorithms often necessitates protocol updates, schemes, and infrastructure.

Based on previous experience, experts believe a transition to quantum-resistant cryptography could take at least 10 years and possibly up to 20 years (Grumbling & Horowitz, 2019; NIST, 2024e). Some researchers even suggest that deploying the significant changes required to accommodate quantum computing may require a complete rebuild of the internet ecosystem (Inglesant et al., 2018).

Once an organisation identifies a value for each of the three components, the required timing for a transition to quantum-safe systems can be calculated. This calculation is shown in Figure 2, whereby X = the time needed for information to remain secure (assuming data is protected from today); Y = the time needed for migration (including design, build and implementation of new infrastructure); and Z = the time it will take for a quantum computer sufficiently capable of breaking existing systems to become available. The risk is highest if $X + Y > Z$.

Figure 2

Required Timing for Transition to Quantum-Safe Systems



Note. Adapted from "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" by M. Mosca, 2018, *IEEE Security & Privacy, Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723. Copyright 2018 IEEE.

Figure 2 portrays a hypothetical scenario whereby a quantum computer becomes available in 15 years, the needed security shelf life of an organisation's data is 7 years (a typical legal retention period in business), and migration is estimated to take 10 years. This migration period assumes that NIST standardises a quantum-safe algorithm by 2024 and leaves an optimistic 6 years for full implementation, an ambitious goal, as history shows. In this scenario, it is clear that sensitive data will be placed at risk for some time with no effective protection mechanisms available, even if work to replace these systems begins immediately. Whilst these timeframes are estimates, they are probable and may even be conservative. NAS believe that if a fault-tolerant quantum computer with 2,500 logical qubits is built anytime in the next 25 years, then it is inevitable that some data will be compromised (Grumbling & Horowitz, 2019).

2.8.2 Implementation of Quantum-Safe Solutions

Whilst much literature focuses on the development of cryptographic systems capable of thwarting the threat that quantum computing poses to PKI, the study of how these solutions may be practically implemented is far less mature (Mone, 2020). Critical guidance for organisations is still largely missing from the literature, and this gap requires urgent attention. NIST has only just begun to publish high-level considerations for planning the transition to a post-quantum world. Further guidance is not expected until after the first quantum-resistant algorithms are adopted (NIST, 2024e).

Complementing the NIST's post-quantum cybersecurity standardisation exercise is a project driven by the US Government's National Cybersecurity Centre of Excellence. This project is intended to initiate the development of practices that will guide migration from the current public key algorithms to suitable replacements. Initial activities include funding the creation of automated discovery tools to assist in identifying where and how PKI algorithms are currently used in hardware, operating systems, firmware, applications, protocols, cryptographic libraries, cloud data centres and beyond, and prioritising the migration of legacy algorithms based on risk management methodology (NIST, 2021). The overall outcome of this project is to publish a NIST Cybersecurity Practice Guide as a Special Publication 1800 series, which will outline specific practical steps for implementation. However, this guide is some time away; therefore, the NIST recommends that organisations immediately create plans for this transition based on current information.

Barker et al. (2020) and NIST (2024e) suggest that readiness steps can be undertaken while the quantum-safe algorithm standardisation process is underway. These steps include developing architectural guidelines for post-quantum versions of critical protocols and raising awareness of the upcoming need to change protocols and algorithms. However, the current literature does not indicate clear accountability or timeframes for these activities, which is concerning as this work will likely require the global cooperation of many entities to be successful.

There are also steps that individual organisations can undertake immediately to prepare for a post-quantum world. These include conducting an initial discovery process to uncover where public key encryption is employed within the organisation and how it is used. NIST (2020) highlight potentially important characteristics for a business to identify when attempting to understand the requirements for any migration or implementation of post-quantum cryptographic solutions, such as:

- Current hardware and software limits for future key and signature sizes
- Thresholds for latency and throughput
- Current cryptographic negotiation protocols
- Current key establishment protocols
- The level in the stack where cryptographic processes take place
- How cryptographic processes are currently involved
- Current cryptographic suppliers used for hardware, software, and processes
- Current key and certificate sources
- Current legal and contractual requirements
- Any IP impacts of a transition
- Level of information sensitivity

This list provides a valuable starting point; however, it is high-level, likely incomplete, and requires relevant skills and knowledge to undertake. Unfortunately, the IT security community currently lacks skills and knowledge around post-quantum cybersecurity solutions such as quantum-safe cryptography and QKD (Greinert et al., 2023). A survey of IT professionals undertaken overseas in 2019 by the Cloud Security Alliance indicated that 60% of respondents were aware of the risk that quantum technology poses to secure communication; however, 70% were unaware of solutions available to address this risk, and less than half (40%) had plans to future-proof their systems (Cloud Security Alliance, 2019). Similar research conducted across the US, Japan, and Germany by DigiCert added to these findings by highlighting the current confusion around quantum computing. Only 63% of their respondents were aware of the correct definition of PQC (DigiCert, 2019).

Along with the IT security community, key business leaders and decision-makers must also understand the threat that quantum computing poses to incorporate quantum computing into risk management plans and allocate sufficient budget and resources to address this challenge promptly. IT resources require

senior-level support to acknowledge the impact that a powerful quantum computer will have on current secure cryptographic schemes, explore alternate technology solutions, and plan to build organisational capability in quantum computing (Chang et al., 2020; Cloud Security Alliance, 2019).

The lack of research around the practical implementation of quantum-safe solutions suggests that the security and business community may be waiting until an organisation such as NIST standardises all paths forward. This approach may be unwise, as regardless of which algorithms are ultimately standardised, nations and businesses must be ready to adapt and implement an alternative to classical systems quickly. No research has yet been conducted exploring the awareness or preparedness of NZ and NZ organisations to face cybersecurity threats in a post-quantum world. However, governments and standards bodies have significant work ahead to educate, develop clear guidelines, and pave the way towards safe communications for the future. Further research on preparedness will help determine the steps necessary to ensure that countries, business ecosystems, and individuals are ready for the significant changes ahead.

2.8.3 Assessing Preparedness

Previous major technological advancements, such as the widespread adoption of the internet or cloud computing, have prompted many research studies that attempt to assess readiness for change (Aripin et al., 2020; Hashim et al., 2020; Holm & Goduscheit, 2020; Wang et al., 2017). Research on analysing whether an entity is prepared to protect itself against the changing cyber threat landscape these technological advancements pose is growing; however, studies looking at quantum computing preparedness are scarce.

There are currently numerous cybersecurity readiness, preparedness, and maturity frameworks and models published by industry bodies that purport to assist businesses in managing cybersecurity risk by describing readiness activities, best practices, and suggested measurements. Some of the most widely used are described in Table 4. Each industry-developed framework is similar, and they overlap by containing many of the same cybersecurity controls. All provide a good starting point for organisational cybersecurity improvement.

Table 4

Contemporary Industry Cybersecurity Frameworks

Name	Description
NIST Cybersecurity Framework (CSF)	The NIST CSF was first published in 2014 and updated in 2018. It is arguably one of the most respected and adopted cybersecurity frameworks (Better Business Bureau, 2017). Freely available and highly comprehensive, both governments and industries recommend that this framework be adopted in organisations to manage cybersecurity risk (Financial Markets Authority, 2019). This framework structures cybersecurity into the five core areas of identify, protect, detect, respond, and recover (NIST, 2018a).
NIST Special Publication (SP) 800 series	Publications in the NIST 800 series contain more detailed technical guidance than the NIST CSF. The series was developed to support the privacy and security needs of US Federal Government information systems; however, it can be voluntarily adopted wider (NIST, 2018b).
International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC) 27000 series	The ISO 27000 series of cybersecurity guidelines are intended to be used by organisations to strengthen their cybersecurity posture and consist of more than a dozen different standards. Certification against the ISO 27000 standards is possible and is one reason why a company may adopt this system (ISO/IEC, 2018).
Center for Internet Security (CIS) Controls	The CIS controls are a recommended set of actions designed to protect organisations and data from known attack vectors. The controls differ from other models in that they strongly recommend prioritising recommended actions based on an organisation's size and resources (CIS, 2021).
ISACA CMMI Cybersecurity Platform	The ISACA CMMI Cybersecurity Platform focuses on building cybersecurity resiliency using a risk-based solution to measure cyber maturity against globally accepted industry standards (ISACA, 2021).

Despite their widespread availability, criticism has been directed at the industry frameworks and models described to date due to their complexity in implementation and the need for organisations to change business processes to accommodate them (Aliyu et al., 2020a). Due to the imperfect nature of these models and the lack of a single global standard to assess and plan cyber maturity, there is also an abundance of other models and frameworks proposed in the literature, such as, the information security focus area maturity model (Van Steenbergen et al., 2010); the cloud security capability maturity model (Ngoc & Hoang, 2017); the national initiative for cybersecurity education capability maturity model (Curtis et al., 2015), and the systems security engineering capability maturity model (Drivas et al., 2020). The sheer volume of cybersecurity models highlights the confusing and complex nature of this area.

Drivas et al. (2020), Miron and Muita (2014), and Akinsanya et al. (2020) all investigated multiple different contemporary cybersecurity models, and each concluded that the explored models all required a level of customisation for practical use and that none fully addressed the unique scenarios and contexts under study. Further criticism of these models focused on the high-level nature of the guidance they offer and the inability of any models to support complex environments and emerging technology (Drivas et al., 2020). As Carayannis et al. (2021) described, most of the existing cybersecurity, maturity, and resilience frameworks are based on assessing the current threat environment and acceptable organisational risk level to determine action. Generally, the models look at minimum compliance measures and do not address

the emerging threat landscape (Aliyu et al., 2020). Therefore, these models and processes are insufficient to evaluate cybersecurity preparedness for an emerging and unclear threat such as quantum computing.

Researchers have attempted to address the gaps in these various frameworks by building on them and combining them into new models for practical use in various industries. For example, Chapman and Reithel (2020) chose relevant areas from several NIST core functional areas and combined these with controls in the CIS control set to create the practice and awareness cybersecurity readiness model. Almuhammadi and Alsaleh (2017) looked at gaps in the NIST CSF by comparing it to other standards, such as ISO/ISEC 27001, and proposed a new model to fill these called the information security maturity model, and both Drivas et al. (2020) and Aliyu et al. (2020) proposed new cybersecurity maturity frameworks to incorporate and integrate new regulatory requirements such as the general data protection regulations and NIST directives 2016/1148. These studies successfully investigated cybersecurity preparedness in specific environments; however, the applicability of any models to be applied beyond their initial scope is unclear.

Many studies describe how the successful adoption of technology can be premised on an organisation's state of electronic readiness (e-readiness) (Fathian et al., 2008; Kamanghad et al., 2019; Uzoka, 2008; Wibowo et al., 2020). E-readiness is a widely used concept in information technology research and is defined as "the ability of a firm to successfully adopt, use and benefit from information technologies" (Fathian et al., 2008, p. 578). In the cybersecurity landscape, e-readiness relates to adapting and using technologies to protect against cyber threats and is typically broken down into the sub-categories of people, governance, and technology. Skilled and knowledgeable resources at all levels of an organisation are described as necessary for a cyber-aware culture that contributes positively to protecting a business from cyber threats (Wibowo et al., 2020). Governance, such as implementing appropriate cybersecurity policy, technical change management systems and security ownership, has also been proven to impact cybersecurity readiness (NCSC, 2019), and Mosca (2018) and NIST (2020) each outline the necessity of agile technology for responding to cyber threats in the post-quantum world.

Studies conducted by Kurnia et al. (2009) and Eilts (2020) sought to understand the technology readiness of small and medium-sized enterprises by exploring the relationship of variables contributing to overall readiness, such as industry readiness, organisational attitudes, technical controls, and national readiness. Whilst successfully describing and ranking the readiness variables under investigation, these studies found that different technologies have different correlations with the variables described.

Rather than researching technology readiness, Sumner (2009) investigated organisational preparedness to address specific information security threats. Sumner's (2009) study determined the level of preparedness by surveying the number of protection mechanisms employed by an organisation to address 12 specific information technology threats. This research clearly showed that levels of preparedness differed when individual threats were considered, making it difficult to estimate overall cybersecurity preparedness.

The results described by Sumner (2009), Kurnia et al. (2009) and Eilts (2020) all suggest that applying a broad and holistic model of readiness may not be as effective as defining readiness for each specific technology or threat. Kademeteme and Twinomurinzi (2019) and Bharadwaj et al. (2013) both highlighted that the rapid pace of emerging technologies creates difficulties when attempting to address preparedness,

and Molla and Licker (2005) and Ogunyemi and Johnston (2012) additionally argue that developing a unifying theory or framework to investigate all emerging technologies is challenging.

Recognising that preparedness assessment may be more effective when completed for each unique technology, Ogunyemi and Johnston (2012) investigated the readiness of South African businesses to adopt cloud computing. Variables describing national e-readiness, organisational preparedness, industrial relationships, internal resistance, and external influence were assessed to determine their relationship to readiness. The study concluded that all variables were significant; however, national e-readiness and industrial relationships were highly significant.

The importance of industry partners and relationships was also represented in studies by Nghihalwa and Shava (2018), who undertook a study to assess the Namibian Government's readiness for cloud computing. A combination of online questionnaires and policy reviews revealed that vendor commitment and expertise in cloud technologies were crucial to adopting this emerging technology. How industry readiness and relationships with supply chain partners contribute to cybersecurity maturity is also highlighted in studies such as Lees et al. (2018), who found that excessive trust and reliance on third parties potentially lowered cyber resilience when investigating cybersecurity in multinational corporations. Additionally, Ogunyemi and Johnston (2012) and Kurnia et al. (2009) found that industry relationships strongly influenced whether an emerging technology was accepted within an organisation.

National e-readiness is also highlighted in various studies as necessary for businesses to operate successfully in the global economy (Bahuguna et al., 2019; Ogunyemi & Johnston, 2012). The Economist Intelligence Unit (EIU) defines national e-readiness as "a measure of the quality of a country's information and communication technology infrastructure and the ability of its consumers, businesses, and governments to use information technology to their benefit" (EIU, 2008, p.1). Early studies by Kurnia et al. (2009) and Molla and Licker (2005) did not find national e-readiness to be a significant factor driving organisational readiness to adopt e-commerce. However, Ogunyemi and Johnston (2012) found that it was highly significant when investigating emerging server virtualisation technology adoption. Therefore, a suitable level of national e-readiness may allow businesses to deploy the emerging technology required to operate and defend against threats in a post-quantum world; however, the contrasting results demonstrate that further investigation is required.

Another critical national measure considered in current literature is national cyber readiness. National cyber readiness differs from national e-readiness, as it focuses on a nation's ability to protect itself from technological threats rather than its ability to benefit from technology use. The Potomac Institute for Policy Studies developed the cyber readiness index 2.0 to define what "cyber ready" means for a country. The index describes seven essential elements to assess a country's maturity and level of preparedness for certain cybersecurity risks. These elements are national strategy, incident response, electronic crime and law enforcement, research and development investment, diplomacy and trade, information sharing, and defence (Potomac Institute for Policy Studies, 2015). The importance of national cyber readiness factors to cybersecurity maturity was confirmed by Bahuguna et al. (2019), who identified legal and regulatory measures and policy measures as critical to enabling business cybersecurity maturity when assessing the cybersecurity maturity of Indian organisations. Bahuguna et al. concluded that the government could use policy intervention and regulation to influence and improve the cyber maturity of Indian businesses.

It has been argued that frameworks should be created specifically for the technology being investigated due to the difficulties of defining a unified theory to support all types of technology innovation (Molla & Licker, 2005). Additionally, the review of current literature highlighted a lack of frameworks that fully support the investigation of cybersecurity preparedness for specific emerging technologies such as quantum computing (Ogunyemi & Johnston, 2012). To date, no literature has proposed or validated the conceptual construct of quantum-computing cybersecurity preparedness. Therefore, this study aims to develop a high-level model to describe quantum-computing cybersecurity preparedness for the NZ landscape.

2.9 Conclusion

Chapter 2 provided an overview of prior research on quantum computing and uncovered a significant body of knowledge describing the potential development and application of this emerging technology. A growing amount of material on the potential cyber threats that quantum computing may pose, and the potential solutions to combat these threats, was also found. However, gaps in our understanding of this area were also revealed. The literature review discovered that research or knowledge describing the impact quantum computing may have on the NZ cyber threat landscape is absent. Additionally, limited investigation has been conducted around NZ organisational awareness and preparedness to face these potential impacts. There is also limited awareness of how governments globally, including the NZ Government, will address the potential cyber threats that this emerging technology will pose and finally, a full understanding of all the factors required to prepare for a quantum computing-enabled cyber threat landscape is unclear.

Section 2.2 explored the current and emerging cyber threat environment in NZ. Growing levels of cyber-attacks and their significant impacts on NZ organisations were described. This section posited that emerging technology such as quantum computing might escalate and exacerbate an already high-risk cyber threat environment in NZ and presented researchers' concerns around this.

Section 2.3 focused on an overview of quantum computing. The technology was defined and the unique features of quantum superposition that may enable quantum computing to increase computing power for some applications exponentially were explored. Literature that describes the technical evolution of quantum computing and discusses the challenges and limitations around current engineering approaches was included. A lack of development standards in this area was highlighted.

Research that focuses on solving existing challenges in coherence, entanglement, error correction, data conversion, software, and quantum algorithms was presented. Several types of quantum computers currently under development highlight that there is no standard in quantum computing hardware. Overall, this section demonstrated that while significant engineering challenges are still yet to be overcome to develop a large-scale fault-tolerant quantum computer that can provide quantum speedup, steady progress is being made towards this goal.

Section 2.4 investigated the threat posed to secure communication by the development of quantum computing. A comprehensive body of research confirms the impact of quantum computing on the cryptographic algorithms commonly used to secure digital communications and online transactions. This section described how developing a full-scale fault-tolerant quantum computer capable of running Shor's and Grover's quantum algorithms will render cryptographic algorithms such as RSA, ECDH, ECDSA, ECDH, and ECC insecure. These algorithms are currently used in digital signatures, key establishment,

and exchange processes in the PKI. Research describing the less severe but significant impact quantum computing would have on symmetric hash and data encryption algorithms such as AES-256 and SHA-256 was presented.

Proposed solutions to the threat that quantum computers pose to these currently used cryptographic algorithms were explored in Section 2.5. The research into solutions can be divided into two focus areas: quantum-resistant cryptography and quantum cryptography.

In Section 2.5.1, quantum-resistant cryptographic options were investigated, including the use of new hash-based, code-based, lattice-based, multivariate, and elliptic-curve isogeny-based cryptosystems. The advantages of these new systems include computational efficiency and potential security against quantum computing; however, most require significantly larger key sizes, making them unsuitable for all architectures. Additionally, the review highlighted how these new cryptosystems are operationally unproven. In Section 2.5.2, solutions dependent on quantum cryptography were explored. The literature in this area describes how quantum cryptography is still in its infancy and requires more research before implementations can fully utilise the security inherent in quantum mechanics. QKD networking was presented as the most mature application of quantum cryptography, having already been implemented and commercialised globally. However, limitations to this technology, such as distance restrictions and the expense of implementation, were also uncovered in the literature.

Section 2.6 focused on literature investigating further potential cyber threats and ethical implications of quantum technology. The literature describes how quantum computing has clear implications for national security, and concerns around the ability of quantum computing technology to upset existing geopolitical power balances and exacerbate the digital divide were explored. Initial findings in a new area of research exploring the discourse and language of quantum computing and how it may negatively influence society's response to quantum technology were reviewed. The literature in this section recognises that quantum computing will exacerbate many current cyber threats when combined with other disruptive technologies such as AI; however, it also highlights gaps in our understanding of its potential impacts on existing cyber threats such as data privacy, DDoS, disinformation, and malware attacks. Finally, literature exploring the need to govern quantum technologies globally was investigated, highlighting a disparate and imperfect global governance landscape that requires further work.

Section 2.7 presented material that describes how nations are responding to the evolution of quantum computing and its potential cyber threats concluding that significant investment is being made in this area worldwide. Section 2.8 explored research into preparedness for quantum computing which describes the necessity of taking action immediately to prepare for any potential threats. High-level preparation guidance available in the literature, including preliminary steps that would assist an organisation in preparing for quantum-safe algorithms and systems was presented. However, this section also highlighted the limited research on the practical implementation of quantum-safe systems.

Literature describing numerous frameworks supporting organisations in assessing and improving cyber security were also reviewed. Gaps in the existing frameworks were described, including the lack of emerging technology coverage. The need to build frameworks and assess cyber security preparedness for specific technologies such as quantum computing was established.

The literature review highlights that limited investigation has been conducted around the impact quantum computing may have on the NZ cyber threat environment and how current threat awareness and preparation levels are unknown. The concept of post-quantum cybersecurity preparedness is also not well-defined by the current body of knowledge, and therefore, this study aims to investigate quantum cybersecurity awareness and preparedness in NZ organisations to close this gap.

The literature review also described how quantum computing may present a national security risk, exacerbate the existing global cyber threat landscape, increase the digital divide, and change global power balances. Global governance mechanisms may be required to mitigate these impacts on society; however, there is no research describing the NZ Government's role in this process. Therefore, this study will investigate the role the NZ Government could play in global discussion and policy formation in this area.

Chapter 3 focuses on identifying a research approach to investigate the awareness and preparedness of NZ organisations to face quantum computing threats and clarify the factors that will influence quantum cybersecurity preparedness in NZ. An appropriate method to research the level of organisational awareness and preparation for quantum cyber threats, along with a method to investigate the NZ Government's role in forming quantum technology policy on the global stage will be formed.

Chapter 3: Theoretical Framing

Information technology researchers have used various theoretical frameworks when attempting to explore and explain concepts such as technology adoption and readiness for new technology. Frameworks considered for use in this study included the theory of reasoned actions (Fishbein & Ajzen, 1975), theory of planned behaviour (Ajzen, 1991), emerging IT framework (Cegielski et al., 2005), technology acceptance model (Davis et al., 1989), the theory of acceptance and use of technology (Venkatesh et al., 2003), and theory of diffusion of innovation (DOI) (Rogers, 2003).

As addressing post-quantum cybersecurity requires executive decision-making, theoretical frameworks that describe decision-making were also reviewed for suitability. These included the status quo bias theory (Kim & Kankanhalli, 2009; Samuelson & Zeckhauser, 1988), cognitive dissonance theory (Akerlof & Dickens, 1982), self-perception theory (Bem, 1972), and cumulative prospect theory (Tversky & Kahneman, 1992).

While each of the theories considered has a long history of use, several were found less suitable for this study as they rely upon assessing specific technology usage variables. For example, the technology acceptance model measures “ease of use”, and the emerging IT framework requires specific information about the technology under study to complete the assessment. As this study focused on future quantum technologies that are still evolving and not within general reach, theories relying on knowledge gained when using the technology were discarded. Additionally, theories such as the self-perception theory, the theory of reasoned action, and the theory of planned behaviour were ultimately not chosen due to the sheer number of revisions made to them since their conception that rendered their purpose and application in answering the research questions in this study unclear.

The literature review showed that investigating cybersecurity preparedness for a post-quantum world requires understanding technological, environmental, organisational, and individual cognitive factors that may contribute to decision-making in an uncertain climate. Therefore, these issues will be examined through the lens of DOI and cumulative prospect theories to support this research. Both theories have a history of successful use within the information technology research landscape and most closely attempt to explain the conditions under which NZ businesses may need to address post-quantum cybersecurity, namely those of uncertainty and risk. The theories outlined in this section will be used as a lens to think about the topics explored and as an interpretive lens through which to view the data during analysis.

3.1 Theory of Diffusion of Innovation

Organisations may need to adopt emerging technologies quickly to face the cybersecurity threats that widespread quantum computing will pose. Therefore, it is vital to consider the issues surrounding the organisational adoption of emerging technologies. The DOI theory developed by Rogers (2003) provides insights into this area by describing how innovation diffusion occurs at a holistic level. DOI outlines a sequential diffusion process consisting of five steps whereby knowledge and awareness of the innovation are gained first, followed by the formation of a negative or positive opinion towards the innovation, a decision to adopt or reject the innovation, the implementation, and finally, a decision reinforcement (Rogers, 2003).

The current body of literature contains many examples of information technology researchers using DOI with a strong emphasis on explaining the technological (IT capability and infrastructure) and organisational (support level, human resources, and financial resources) contexts benefitting or inhibiting technology adoption (Ching et al., 2020; Mabad et al., 2021; Min et al., 2019; Ogunyemi & Johnston, 2012). These studies differ significantly in context, focusing on phenomena such as developing countries, SME e-business, and individual mobile applications. However, the findings of each study confirm that continuing to operate in a fast-changing business environment successfully is dependent on significant technological innovation and that DOI theory can be used to analyse potential barriers to this process and drive a deeper understanding of the contributing factors in each unique context.

Rogers' (2003) DOI theory may help understand the necessary technological and organisational prerequisites for adopting post-quantum cybersecurity technology measures, for example, describing the need to gain knowledge about a new cybersecurity tool or threat as the first step in the adoption process before taking any further action. The DOI theory may also help interpret the maturity level of NZ businesses regarding their preparedness to address cybersecurity threats in a post-quantum world by looking at which step in the DOI process NZ businesses are currently addressing. Early studies that adopted DOI theory as a sole primary lens were criticised by authors such as Chang (2010), who believed that DOI theory does not address environmental factors well. As the literature review describes the importance of third-party suppliers and partner relationships to cybersecurity preparedness, theories that take a relational view of the environment and consider the characteristics of these relationships are critical to addressing preparedness. Further limitations of DOI theory were highlighted by Iles et al. (2017) in a study aiming to understand the adoption process of national security technology. Iles et al. recognised that DOI theory does not deeply consider the decision reasoning process involved in any innovation adoption. The approach thereby combines factors from DOI theory with elements from persuasion literature to overcome this limitation and offer recommendations to motivate the adoption of a security tool for enhancing national security.

DOI theory may assist in providing a theoretical framework for adopting post-quantum cybersecurity technologies; however, it is important to look beyond this theory alone due to its limitations. In this study, DOI theory is supplemented with the additional lens of cumulative prospect theory.

3.2 Cumulative Prospect Theory

Cumulative prospect theory (CPT) was developed by Tversky and Kahneman (1981) in response to research that found that people exhibit patterns of preference that did not conform with the leading decision-making theory at the time—the expected utility theory (Tversky & Kahneman, 1981). The original theory evolved to encompass the ideas of status quo bias and patterns of risk aversion with CPT, providing a philosophical framework to explain how decision-making occurs under risk in many information technology research studies (Eilts, 2020; Kim & Kankanhalli, 2009; Lee & Joshi, 2017; Polites & Karahanna, 2013).

CPT aims to describe how decisions are made under conditions of risk by offering insights into how the incorrect framing of a situation can lead to non-optimal decision-making. The framing effect refers to a perspective bias that occurs when a decision-maker evaluates options presented to them using either

negative or positive semantics. For example, it describes how any difference between options in a decision will “loom larger” when framed as a disadvantage of one option versus the advantage of the other option (Tversky & Kahneman, 1981).

As cybersecurity preparedness is essentially a risk management tool, understanding how decisions are made under conditions of risk, such as those presented by widespread quantum computing, is warranted. CPT was used to analyse the framing effect on organisational decision-making in early research conducted by Bazerman (1984), who concluded that organisations tended to be “risk-averse” when situations were framed positively and “risk-seeking” when framed negatively. Eilts (2020) used CPT in more recent information security research to highlight the negative consequences of decisions based on framed circumstances. For example, when maintaining the status quo is justified by the decision-maker, even when they are aware of a significant or imminent threat.

The theoretical lens of CPT has also been used extensively to investigate decision-making in information technology under conditions of uncertainty. Kim and Kankanhalli (2009) used prospect theory to describe the resistance levels of individuals to new and changing technology, and Polites and Karahanna (2013) used the lens of prospect theory to understand the reluctance of decision-makers to switch to a new technology due to the perceived costs of this switch. More recently, Sanjab et al. (2017) used prospect theory in research designed to enhance the cyber-physical security of drone delivery systems, and Ma and Zhang (2020) took the core tenets of prospect theory and extended it to create a multi-attribute decision-making model for use with cloud models.

Using prospect theory has implications for both the research design and data interpretation in this study. CPT highlights the need to reflect on and analyse the language used when discussing post-quantum cybersecurity threats. CPT may also help to further understand the decisions being made by NZ businesses around quantum preparedness during data analysis by using it as a lens to examine the language of communication around quantum threats and the cognitive limitations that drive decision-making in risky or uncertain environments.

Chapter 4: Research Design and Methodology

4.1 Introduction

Methodology is the theoretical analysis of the methods and principles appropriate to a field of study (Savin-Baden, 2013). This chapter aims to identify and describe the appropriate methodology to investigate the issues raised in Chapter 2 around the potential cyber threats that quantum computing may pose to NZ.

Classical pragmatism was chosen as the overarching research philosophy, supported by a pragmatic and reflexive research approach. Qualitative data collection and analysis methods facilitated this approach, including semi-structured interviewing, RTA, and reflective journaling.

This chapter transparently describes the research design decisions, the rationale behind them, and how they were applied during this study. Ethical considerations and how the study upheld both ethical norms and quality are also outlined.

4.2 Purpose

This study aims to describe NZ's cybersecurity preparedness for a quantum computing-enabled world. The study seeks to understand the awareness and preparedness of organisations critical to NZ's security, infrastructure, and economic stability to face quantum computing-enabled cyber threats. Additionally, it explores the role the NZ Government could play in global conversations around the cybersecurity and ethical impacts that quantum computing may pose.

Quantum cyber threat preparedness was initially defined in this study as the ability of an entity to effectively identify, protect against, detect, respond to, and recover from cybersecurity threats posed by quantum computing (NIST, 2018a). However, this study also aimed to further evolve this understanding of quantum cyber threat preparedness by developing a conceptual framework to identify the specific factors contributing to emerging quantum cyber threat preparedness in NZ and provide a more holistic understanding of this phenomenon.

4.3 Research Questions

To understand and describe the cybersecurity preparedness of NZ to operate in a quantum-enabled environment, this study aimed to answer the following research questions:

1. How prepared are NZ organisations to face quantum computing-enabled cyber threats?
    a. How aware of quantum computing cybersecurity threats are critical NZ organisations?
    b. If aware, how are NZ organisations currently planning for emerging quantum computing cybersecurity threats?
2. What role could the NZ Government play in global conversations and policy development focused on the cybersecurity and ethical implications of emerging quantum-enabled technology?
3. What factors will contribute to NZ's cyber threat preparedness in a quantum computing-enabled world?

4.4 Research Approach

The effectiveness of a research study can be limited or increased by the approach undertaken, necessitating careful selection. Quantum computing and cybersecurity are technology research areas which often rely on quantitative methods to assess relationships between existing defined variables (Lee & Liebenau, 1997). However, it could be argued that known variables derived from previous research may not provide a complete answer to preparing for future cyber threats faced by NZ because of quantum computing, as this landscape is uncertain and still evolving.

Additionally, despite the existence of well-understood technical solutions to combat cyber threats, NZ organisations and government agencies are still experiencing these threats. These ongoing impacts indicate the need for a greater understanding of the landscape that NZ technology professionals operate in when preparing for cyber threats today and into the future. Therefore, a qualitative approach was adopted due to the ability of qualitative methods to look closely at the lived experience of the participants and generate situated and strongly contextual knowledge, rather than testing existing hypotheses as commonly seen in quantitative research (Braun & Clarke, 2022).

Using a qualitative approach also enabled deep exploration into the issues raised by the participants and allowed for new insights and new factors to be found that will contribute to the preparedness to face cybersecurity threats in a quantum computing-enabled environment (Savin-Baden, 2013).

4.5 Philosophical Lens

This qualitative study was approached through the lens of classical pragmatism. A key driver of this study was to contribute practical, useful, and relevant knowledge that incorporated and reflected the experience of participants tasked with managing cyber threats from emerging quantum technology. This desire to produce actionable knowledge is a central tenet in pragmatic inquiry, as classical pragmatists were concerned primarily with knowledge that had practical consequences (Kelly & Cordeiro, 2020).

Traditional research philosophies often encompass either an ontological position of objectivism professing that “social phenomena and their meanings have an existence that is independent of social actors” (Bell et al., 2022, p. 12) or one of subjectivism professing that “social actors are continually accomplishing social phenomena and their meanings” (Bell et al., 2022, p. 12). In contrast, classical pragmatism rejects this notion of dualism and asserts that the meanings we attach to life cannot be reduced to entities with independent ontological reality, nor can they be independent of our actions or collective history (Simpson & den Hond, 2022).

Classical pragmatism also challenges many epistemic principles commonly used to describe how acceptable knowledge can be gained and described by encompassing a view of knowing as a social and situational experience that shapes and is shaped by the lived experience of knowers (Vannatta, 2011). Therefore, in classical pragmatism, epistemology and ontology cease to be distinct concepts.

The classical pragmatism movement, founded on the work of Charles Peirce, William James, and John Dewey, originated out of a desire to focus inquiry on issues that were significant to humans rather than metaphysical debates such as the nature of truth and reality (Cassell et al., 2018). This focus on practical and applicable knowledge has led to the wide use of a pragmatic lens in research focused on organisations

or organisational processes. Kelemen and Rumens (2013) present examples where organisational phenomena such as collaboration, ethics, finance, and public administration are examined using a lens of pragmatism, and Lorino (2018) demonstrates how pragmatism can inform organisational research and organisational practice simultaneously.

Pragmatism is unique in that it focuses on human efforts to cope with the day-to-day challenges of the real world rather than abstract concepts. In pragmatic philosophy, thinking and doing are inseparable, and no meaning can be independent of our experiences (Cassell et al., 2018). Knowing is contextual and shaped by experience (Kaushik & Walsh, 2019). This study's participants are professionals heavily embedded in day-to-day business operations, and the use of a pragmatic lens allowed for the recognition of the participants' practical knowledge gained over time by operating in this context.

Classical pragmatism is also future-focused. As Menand (2001) described, pragmatism recognises that we bet on how the world will be tomorrow, and these bets shape the actions we take today. It combines a "what if" anticipatory sensibility in conditions of uncertainty with the capacity to develop choices for alternative futures. This idea aligns with a study centred on emerging technology such as quantum computing, where uncertainty demands we simultaneously "make bets" about what risk this technology may pose and take actions to mitigate the predicted risk.

Classical pragmatism describes three principles for inquiry that serve as the critical lens for this study:

1. Emphasising actionable knowledge

Pragmatism supports the goal of creating practical knowledge with utility for action to make a difference in practice (Goldkuhl, 2012). It supports a plurality of methods as part of an overall research plan, using the most appropriate method to answer the questions posed. This principle supported the aim of this study to produce actionable cybersecurity preparedness guidance for a quantum computing-enabled landscape, and drove the selection of methods used.

2. Social justice

Ideas of social justice were central to the original pragmatist movement, with its founders all reformist intellectuals driven to improve society (Menand, 2001). Pragmatism demands that the researcher pursue the most important issues for the individuals and communities involved. It emphasises the need to decide what goals are meaningful in research and the appropriate methods to obtain them (Morgan, 2014).

Dewey opposed the use of economic domination that could limit the growth of other social groups (Morgan, 2014). As the review of literature related to this study demonstrates, access to quantum technology has the potential to change power balances that exist amongst nations and individuals. A future where only wealthy nations or businesses can use quantum computing may render the goal of equal access to privileges such as data privacy and a stable banking system difficult. Society has an ethical responsibility to manage new technology to avoid the creation of social injustice and adopting a pragmatic lens supports the inquiry of ethical issues such as these. Morgan (2014) also recognised that pragmatism strongly aligns with the advocacy of social justice, as ethical questions are essentially questions about appropriate actions and the difference made by acting one way versus another.

3. Experiential inquiry

Dewey conceptualised epistemology as a theory of inquiry that encompasses experiencing, knowing, and acting, whereby interpreting knowledge leads to action and reflecting on action leads to new knowing and acting methods (Morgan, 2014). Knowledge from a pragmatic paradigm is the result of the active process of inquiry.

Dewey's process of inquiry can be summarised in five steps as follows:

1. A problem is recognised
2. The difference made by defining the problem one way or another is considered
3. A course of action to respond to the problem is developed
4. Potential actions are evaluated in light of their likely consequences
5. Actions are taken that are likely to address the problem (Kelly & Cordeiro, 2020)

Therefore, inquiry is recognised as a continuous process, as highlighted by the iterative nature of steps 2 and 4. Undertaking inquiry may involve multiple cycles of reflecting on beliefs and actions and asking and answering questions that explore the likely outcomes of applying current beliefs to future actions. Inquiry as a process of self-conscious decision-making is central to Dewey's thinking and highlights the importance of using reflective techniques at all stages in this study.

4.6 Methodology

The lens of classical pragmatism drives the need for research to use strong reflective techniques and flexible methods to ensure actionable knowledge. Therefore, the choice of a pragmatic and reflexive methodology for this study is warranted.

Feilzer (2010) highlighted that using a pragmatic approach to problem-solving offers a more reflexive guide to research, as applying a pragmatic lens requires constantly questioning what difference it will make to our research if we approach it one way versus the other. This questioning shapes and determines the methods used in this study, which is undertaken using a formal methodology of reflexivity.

Reflexivity as a formal and comprehensive methodology is described by Alvesson and Sköldberg (2017). It focuses on awareness of the various possible interpretive dimensions available to a researcher at different levels and the ability to address these reflexively. The formal structure of the reflexive methodology chosen involved four levels of reflexive interpretation, as described in Table 5.

Table 5

Levels of Reflexive Interpretation

Level of reflexive interpretation	Description
Empirical material	Interviews, transcripts, observations, documents
Interpretation	Underlying meanings
Critical interpretation	Power, ideology
Use of language and text reflections	Selective voice representation, claims of authority

Note. Adapted from "Reflexive Methodology: New Vistas for Qualitative Research," by M. Alvesson and K. Sköldberg, 2017, SAGE.

Formal reflexivity through these four levels was undertaken at each step of the research process using the tools of journaling and field notes. Journaling included noting ideas, concerns, and researcher judgements related to the approach being undertaken and the interpretation of the data. Field notes made during the interviews recorded observations, impressions, participant body language and tone, and contextual issues in the environment, such as whether it was busy or quiet and whether the participant was interrupted.

The use of a pragmatic paradigm influenced the research method selection by driving a process of continuous questioning to evaluate whether a proposed method would result in actionable knowledge. The researcher's role and influence in this study were explored and understood at each stage of the research process by embracing the pragmatic understanding of inquiry as an experiential process. Practically, this demanded a reflexive enquiry into the function, purpose, and potential outcomes of all ideas and interpretations explored. Finally, focusing on the pragmatic principle of producing actionable knowledge as a vital outcome of the study shaped the examination of the data and the presentation of findings to ensure the resulting output was useful.

Authors such as Tashakkori and Teddlie (2003) have previously criticised using a pragmatic research approach, as they believe that clearly articulated criteria do not exist for determining what knowledge is useful. However, this criticism is offset in this study by allowing participants to articulate what they, in their experience, find useful, thereby including them in the experiential nature of the inquiry.

Further criticism of this research approach in the literature describes how a very narrow interpretation of pragmatism is often used in studies focusing purely on the concept of "what works" rather than the rich underlying philosophical roots (Hesse-Biber, 2015). In this study, the underlying philosophy of classical pragmatism was explored in broader areas, such as social justice and the nature of inquiry, to ensure deeper insight was gained.

As described by Savin-Baden (2013), a pragmatic approach is well-suited to professional fields. It is best suited for this study to ensure the outcome of knowledge production that will inform professional practice in NZ around cybersecurity preparedness in a quantum computing-enabled world. A structured reflexive methodology additionally supports this approach.

4.7 Methods

The methods used in a research study are the “practical means, the tools, for collecting and analysing data” (Grant & Giddings, 2002, p. 12) that underpin the philosophical framework and methodology chosen. The methods used in this study, which included interviewing 32 participants, formal reflexive journaling, document analysis, and the mechanisms of data analysis, are described in this section.

While a pragmatic approach opens the possibility for using qualitative and quantitative methods, classical pragmatists such as Dewey (1931) recognised that “the world in which we immediately live, that in which we strive, succeed, and are defeated, is predominately a qualitative world. What we act for, suffer, and enjoy are things in their qualitative determinations” (Dewey, 1931, p. 93). Therefore, in a study that aimed to understand the issues and concerns of security practitioners in business, using primarily qualitative methods was warranted. In a pragmatic approach, multiple data collection strategies may also be undertaken to enable comprehensive understanding. This study used in-depth semi-structured interviews and document analysis as the primary data collection methods to ensure practical knowledge was obtained.

4.7.1 Semi-Structured Interviews

Qualitative interview use for primary data collection has a long and varied history across many disciplines, including the business and technology domains represented by this study (Brinkmann & Kvale, 2015; Roberts, 2020.) The rationale for using the qualitative interview as the primary method for data collection in this study is centred on the classical pragmatic belief that experience is the only admissible source of practical knowledge (Simpson & den Hond, 2022). According to Charmaz (2014), “qualitative interviewing provides an open-ended, in-depth exploration of an aspect of life about which the interviewee has substantial experience, often combined with considerable insight” (p. 29), and therefore qualitative interviews enable the exploration of knowledge in a pragmatic way by questioning participants about their experiences and reflecting on these to obtain understanding and insights (Seidman, 2013).

Semi-structured interviews also support the gathering of rich qualitative data for analysis (Wengraf, 2001) and can allow information to be captured that is currently not documented in literature or known to the researcher, contributing unique insights about the topic (Patton, 2015).

As Marshall and Rossman (2006) described, the qualitative interview method can have weaknesses. For example, participants may be unwilling or too uncomfortable to share information in an interview, leading to limited discovery. In this study, participants were informed upfront that they might elect not to answer any question posed, and it was further suggested that they say “pass” if they wished not to answer and that the interviewer would move on immediately without further questions in that area. Examples in this study where a participant may opt not to answer a question include situations where the participant may not have sufficient knowledge to answer or where there may be a conflict of interest previously unknown to the researcher. This technique was successfully used by participants in the interview process to alleviate any potential discomfort, enabling interviews to flow and the rapport built between interviewee and interviewer to remain positive.

Another potential weakness in the interview method was the need for the questions and their responses to require good comprehension. In this study, the participants were purposefully selected for their high level of expertise in this area, and the interviewee also had substantial industry knowledge, ensuring comprehension was not an issue. To enhance understanding, an information sheet about the research topic was pre-supplied to participants to ensure they had context before entering the discussion and an opportunity to ask any questions before and after the interview.

Two rounds of semi-structured interviews were planned for this study. The first round was intended to explore research questions one and two. The second round was intended to involve a different participant group and primarily address research question 3 while also contributing to the discussion on research question 2.

4.7.1.1 Interview design

Participants

Careful selection of participants was integral to this study. A purposeful and maximum variation sampling strategy was used whereby "information-rich cases' were chosen for in-depth study, and maximum differences in perceptions about the research questions were obtained (Savin-Baden, 2013).

In round 1, only participants from large-scale businesses were included in the study as large organisations ordinarily have more resources to focus on cybersecurity and are often leaders in the business environment regarding preparedness for emerging cyber threats. In addition, as this study aimed to describe NZ's emerging threat preparedness landscape, the number of participants was limited to those working at NZ organisations.

Purposive sampling of participants was undertaken from large NZ organisations in a variety of industries to include those with the following characteristics:

- Ethnically diverse
- Public and private
- Listed and unlisted
- Where IT is a core part of the business and where it is purely a support function
- Nationally significant (includes vital economic generators, key government departments, niche exporters, research institutions and critical national infrastructure operators (NCSC, n.d.).

A sample of 15–20 business leaders from various NZ organisations, including organisations of national significance, was targeted. This number of participants was chosen to enable the maximum variation sampling strategy whilst being realistic and achievable in the research timeframes.

In round 2, a sample of 15–20 academic, public policy, and science leaders was targeted.

Purposive selection was undertaken from the academic and political community from a variety of NZ institutions or organisations whereby the potential participants included:

- ICT, quantum science, or emerging technology researchers

- Ethics researchers
- Technology policy researchers
- Technology policy creators or influencers

Participant recruitment

All recruitment was conducted directly rather than via general recruitment approaches (such as advertising) to support a purposeful sampling strategy. In most cases, the potential participants were already known to the researcher. Potential participants were initially contacted by email or in person to ask for an "in principle" agreement to participate in the study. An information sheet outlining the research purpose and the role they were being asked to play was included in the invitation, along with a consent form (see Appendices A & B).

Interview participants were given as much time as necessary to consider the invitation. A single follow-up contact occurred if no response was received following the invitation (for example, after several weeks). Where contact could not be made, alternative participants were identified and invited. Before the interview, participants were asked to sign the consent form that indicated they were fully aware of the boundaries of the research, their rights in the process, and what would happen to the data generated from the interview.

Additional contact was made with participants who agreed to participate to clarify interview logistics, including their preferred date, time, and place. However, the targeted participants held senior positions and were extremely busy, which meant interviews were often rescheduled numerous times, and some participants who initially agreed to be interviewed did not follow through.

The technical and highly specialised nature of this research also meant that some potential participants felt they lacked the required knowledge to contribute. Further clarification of the intent of the interview process (i.e., that the interview was not a "test" but rather a conversation to gain insights into their unique experiences in this landscape), was given in these circumstances. This clarification alleviated some but not all of these concerns. Figure 3 shows a reflexive note describing this study's occasionally challenging participant recruitment process.

Figure 3

Reflexive Journal Note - Recruitment

Feeling slightly anxious around my ability to recruit enough participants. I'm thinking that perhaps the topic matter is too intimidating and rethinking my decision to include potential interview questions in the invitation. I had one response to an invite that just read "Wow – that is intense". They also declined to participate citing a lack of knowledge in quantum despite being a senior figure in a technology business.

Interview protocol

The design of the interview protocol used in this study reflected the interview protocol refinement framework (Castillo-Montoya, 2016), which incorporates four phases for protocol creation as follows:

- Phase 1: Ensure the interview questions align with the overall research questions.
- Phase 2: Balance enquiry and conversation in the interview protocol to ensure rapport can be built whilst still obtaining the data required for the study.
- Phase 3: Acquire feedback on the interview protocol.
- Phase 4: Pilot the process.

Phase 1 – Interview question development

To ensure valid and useful data collection, the central questions in a qualitative interview are ideally closely aligned with the research question (Roberts, 2020). Therefore, the literature review and theoretical framing for this study were used to provide the initial concepts to explore in the interviews and ensure the interview questions addressed the primary focus areas of the study. Major concepts extracted from the literature used as starting points in question development included the dynamics of external relationships, organisational awareness, national readiness, and industry readiness.

The initial question, “Can you tell me what you know about the threats quantum computing may pose to existing systems and cybersecurity mechanisms used today?” was intended to be a tour question which Rubin and Rubin (2012) define as a question that allows the interviewee to provide the interviewer with a tour of the topic. This allowed some insight into how much prior knowledge the interviewee held about the specific topic of quantum threats and guided the specificity and depth of the subsequent questions. Additionally, starting with a more general tour question allowed time for rapport to build and for the interviewee to develop trust in the process (Brinkmann & Kvale, 2015).

Follow-up questions were created to ensure the topic was explored from every angle and to provide a prompt to ensure the interview flow. Roberts (2020) supports the creation of these, describing how they help to avoid only a surface account of the phenomena being described by the participant and assist in keeping the discussion on track.

The order of the questions was designed to assist the interview flow by starting with more general concepts and proceeding to more specific details. The pragmatic methodology was supported by recognising the varied experiences of the participants and by giving them the autonomy to decide what knowledge was important to convey. Therefore, the questions were not posed in a strict sequence, and the order and level of coverage of the main questions and any probing questions differed based on the participant’s response and their desired conversation direction.

Finally, to enhance the data collection needed to create actionable knowledge in this area, the following closing question was asked, “Is there anything else that I haven’t asked today that you think I should have asked or that you believe is important to know?” This allowed participants to raise or reintroduce any areas they felt were important and not sufficiently covered by the conversation. It also acted as an opportunity to wind down the conversation and indicate that the session was ending.

The final lists of indicative questions for both rounds 1 and 2 can be seen in (Appendix C).

Phase 2 – Balancing enquiry and conversation in the interview protocol

An interview guide was created to ensure the enquiry balanced detailed data collection for analysis along with general conversation to establish and enhance rapport with participants.

The interview guide ensured a semi-structured interview protocol was followed that kept the interview focused and helped facilitate a deeper response from the participants (Rubin & Rubin, 2012). The guide included the main questions directly related to the research questions and some potential follow-up and probing questions for use as appropriate. The guide also outlined preliminary tasks and introductory and closing information as references for what needed to be addressed in each session.

General conversation was undertaken at the start of each interview to orient the participant to the interview. This included giving the participant some general knowledge of the topic and the purpose behind the research, ensuring consent was understood, expressing respect for their role as an expert in the field, and reassuring the participant that there were no expectations as to how they answered the research questions. The intent was to develop a general rapport and ease of conversation before asking the interview questions that supported the enquiry. For example, the phrase “I want to hear and understand your thoughts and experiences in this area – will you help me?” was used to reinforce the participant’s role in this process.

Phase 3 – Seeking feedback

Feedback on the interview protocol was sought from three different areas: the AUT ethics advisor and committee review, the research supervision team, and peer review. In this phase no feedback resulting in changes to the interview protocol was received, and all reviewers advised piloting the process.

Phase 4 – Piloting the interview questions

A preliminary pilot interview was undertaken to review the effectiveness of the interview questions and obtain feedback on the process from the pilot participant. The feedback and learnings gleaned from this process were insightful, and several changes to the interview protocol were made as a result.

Some of the proposed questions were found to be too lengthy and, therefore, confusing when spoken aloud. As a result, the questions were shortened and the language was simplified to aid clarity and flow.

In the initial pilot, there was no script for additional probing questions. This proved a mistake as improvisation was required during the pilot interview when more detail or further discussion was needed. Improvisation resulted in the interviewer stumbling over words and asking poorly framed questions, which caused confusion for the participant and ultimately did not result in the intended clarification. A list of potential probing questions was therefore included in the final interview guide.

The pilot interviewee expressed difficulty when trying to discuss the tangible implications of the topic (emerging quantum-enabled cyber threats) as, to date, it is a theoretical scenario. They suggested that providing specific examples or more context to the participants may be useful to frame the discussion. In response to this feedback, further contextual information and the main research questions were included in the information sheet sent to all potential participants. As Rubin and Rubin (2012) supported, sharing

the interview guide enables more transparency in the overall process and was intended to help clearly set out the nature of the interview before a participant's acceptance.

Interview mode

A flexible approach to the interview medium was adopted to support research participant choice. Classical pragmatists believe qualitative research should occur in the natural settings of the participants (Savin-Baden, 2013). This natural environment is flexible for technology-savvy business professionals and typically may encompass modern office spaces and virtual settings.

Participants were therefore given the option to be interviewed in person at a location of their choice or online via MS Teams. Giving multiple options to the participants supported the study's pragmatic approach. It also gave the participants a degree of control over the process, encouraging an equal relationship between the interviewer and interviewee (Hanna, 2012).

When conducting a purposeful conversation in person, an interviewer and respondent can be present to one another in ways that are not possible using other methods (Oishi, 2003); however, there are also benefits to conducting research interviews online. Hanna (2012) highlights that conducting research interviews online enables both the interviewer and the participant to remain in a safe location without imposing on each other's personal space. The interviews for this study were conducted during the COVID-19 global pandemic, and as such, many individuals were working from home, unwell, or limiting their contact with others to avoid becoming unwell during these months. This meant that offering an online interview mechanism was essential to ensure safety and sufficient levels of participation.

An additional benefit of offering an online interview mechanism included the ease with which an online interview could be rescheduled in contrast to in-person interviews, which require travelling time and can lead to a feeling of obligation by the participant to attend even when they have other matters that need attending to (Holt, 2010). The targeted participants were extremely busy senior professionals working in an environment where business as usual must take precedence. For example, a security leader must address an active cyber incident threatening their business over participation in an interview. Therefore, the ability to reschedule interviews easily proved beneficial in this study as six participants required several changes to their interview times.

The synchronous interaction between participants in MS Teams meetings ensured that this medium came the closest to the interaction experienced in an in-person setting (Hanna, 2012) and enabled the interviews to be easily recorded. Possible risks when using an online medium include faulty technology (webcam, microphone) and poor or no internet connectivity; however, this was not experienced in any of the online interviews.

As the participants ultimately determined the interview locations, a researcher safety protocol was designed and followed. The safety protocol involved ensuring that the primary researcher informed either the primary research supervisor or a family member via phone immediately before attending an interview (including leaving location details and expected completion time with them) and once again informing them when leaving the interview.

Data collection

The views of business leaders in NZ companies, academics, quantum and technology scientists, and public policymakers were sought around what preparedness for cybersecurity threats in a quantum computing-enabled world would look like and what aspects of their environment drive decision-making and preparedness activities for these threats. The role that the NZ Government could play in discussing emerging global technology threats was also discussed. By interviewing these stakeholders, I sought to capture their "lived" realities and understand their level of preparedness for quantum-enabled cyber security threats and their perspectives on NZ's role and readiness.

A total of 32 interviews were conducted between August 2022 and December 2022. 12.5% of the participants were female and 87.5% male. Despite planning for two distinct rounds of interviews, in practice, it became obvious early in the data collection that most participants spoke to all three research question areas. Therefore, the scope of each interview was ultimately driven by the participant and their unique knowledge and experience rather than the interview round they were intended to be part of. Twenty-five participants were NZ business technology leaders from a diverse range of industries, including telecommunications, energy, information technology, logistics, transport, engineering, health, education, retail, construction, finance, and professional services. These participants held various job titles such as CEO, CTO, CIO, board member, and consultant. Seven participants were from a technology public policy or quantum science background. While the intent was to recruit more experts in the second group, this was not possible and highlighted the small size of this community within NZ.

Two participants chose an in-person interview, while 30 opted for online interviews. The interview environments chosen by the participants had some impact on the overall interview experience. One in-person interview that was held in a coffee shop was interrupted several times by serving staff, interrupting the conversational flow. Additionally, the noise levels in this environment led to the need to repeat questions for clarity.

In most of the online interviews, there were no environmental concerns; however, in two virtual sessions, participants appeared to become distracted by other alerts or notifications on their computer screens during the later portion of the interview. The reflexive journal entry in Figure 4 describes the first instance where participant distraction was observed and how it was handled moving forward.

Figure 4

Journal Entry That Reflects on Losing the Participant's Focus During the Interview

> *I felt I lost the participant's sole focus about 40 minutes into the conversation and believe this was due to the Teams environment which enables participants to multitask – i.e., see emails coming in on their screen while also still being in a meeting (I have seen this a lot in business meetings online). This resulted in me rushing to conclude this interview which in hindsight was a disappointing reaction and while I want to respect the participant's time and really don't want to tick them off, it was frustrating – perhaps I could try offering a break if I observe this again but think there is value in continuing.*

Whilst each interview was scheduled for 60 minutes, the time taken varied from 40–90 minutes and averaged 56 minutes. All interviews were recorded, and participants were informed that the recordings would be transcribed verbatim. After their interview, all participants were sent their transcripts for review, editing, and approval.

Limited handwritten notes were also taken during the interviews to record any observations and reflections that may not be apparent in the recording (to ensure these were captured). However, comprehensive notes were not taken during the interview, as this took attention away from the interview conversation and added an unwanted distraction.

Formal reflexivity during data collection

Formal reflection was undertaken immediately after each interview, and deeper thoughts and observations from this process were recorded in the research journal. The notes made both during and after each interview served as a vital guide to modifying and refining the interview process, questions, and responses, for constant improvement throughout the study. For example, when reflection indicated that the flow of one interview was not ideal, the order of questions was adjusted accordingly for the subsequent interviews.

4.7.1.2 Data transcription

The researcher undertook interview transcription. Whilst this was a time-consuming process, completing the transcription allowed a deep understanding, engagement, and familiarity with the content that assisted in the initial data coding and analysis. The transcription process often required replaying interview segments several times to ensure accuracy. During the replay process, several important points raised by the participants that were initially missed or misunderstood during the interview were uncovered.

The initial transcripts were then reviewed whilst listening to the interview recording to ensure a level of verbatim was achieved. Pauses, laughter, and filler words such as (um and ahh) were included, and any corrections or further observations and reflections were noted.

Transcript reviewing

Interviewee transcript review (ITR) has long been used in qualitative studies as a technique to improve rigour, and researchers in many fields, including business and technology, have adopted this process (Ardley, 2006; Dobrow, Hagens et al., 2009; Schroeder & Pauleen, 2007). ITR allows interviewees to change or clarify information provided in the original interview, and it reinforces the rights of each participant to withdraw their responses from the study.

Using ITR in this study supported the maintenance of interviewee confidentiality by allowing the participants to remove any data they felt may reveal their identity, be commercially sensitive, or compromise their safety. At the interview's conclusion, participants were reminded that the transcript would be sent to them for review. All edits to the transcripts were documented, and only the edited copies were used for the data analysis process.

A potential disadvantage of ITR is the possible loss of useful data to the researcher. This did not prove to be an issue in this study as only two participants requested that some limited data be removed (this data was irrelevant to answering the research questions). ITR also requires an additional time commitment from participants as transcripts can be lengthy to read. To save the participants time, the researcher reviewed each transcript before sending it to the participant and highlighted any areas that may have included potentially sensitive information.

Some of the participants in this study found reviewing the raw, near-verbatim transcripts uncomfortable and became concerned that their answers were not tidy and edited for easy reading. Reassurance was

given that this was raw data which would undergo analysis; however, comments made by the participants, such as “What a strange read. I sound like someone who should be committed to an institution”, reflected their unease. However, no participants opted to remove their transcripts from the study after undertaking ITR.

4.7.1.3 Data coding and analysis

As Saldaña (2016) described, the qualitative data analysis process is cyclical. The data analysis methods used in this study reflect this cyclical nature by using two first-cycle coding techniques, thematic analysis and strong reflexivity, brought together under a structured RTA approach.

The six-phase approach to RTA, as described by Braun and Clarke (2022), was adopted for use in this study for data coding and analysis as it offers an accessible, semi-structured and robust method for qualitative researchers to refine their understanding of thematic analysis theory while undertaking the craft. As this was the first qualitative study undertaken by the researcher, the well-documented RTA method helped provide structure and clear guidelines for the analysis while remaining flexible enough to accommodate a pragmatic approach. Importantly, the strong reflexive elements embedded in the RTA process aligned with the strongly reflexive approach chosen for the study. In RTA, reflexivity is acknowledged as being the key to quality data analysis, and the six phases formally incorporate its use (Braun & Clarke, 2022).

A core strength of RTA, as described by Braun and Clarke (2022), is that it can produce analysis with actionable outcomes and inform policy development, which is a critical aim of this study. Additionally, it can generate unanticipated insights, which was an initial driver for using a qualitative approach for this research. The RTA approach has also been successfully used previously in qualitative studies focused on technology (Alexander, 2022; Gillies-Walker et al., 2023; Sewell et al., 2023; Shafi & Mallinson, 2023).

In congruence with the classical pragmatist philosophy that knowledge is contextual and found in practice, RTA embraces the idea that knowledge is situated and subjective and moves away from the idea of a singular truth. The RTA process is also much like the concept of experiential inquiry described by classical pragmatism, in that it promotes a cyclical, recursive analytic process of inquiry to drive strong data analysis.

RTA offers flexibility in its use, and data analysis may be completed using these techniques along a spectrum of epistemological and ontological standpoints. Although the philosophy of classical pragmatism cannot truly be described using a typical ontological or epistemological spectrum, it is sometimes considered to sit somewhat midway between the paradigms of realism and idealism or constructivism (Morgan, 2014) and therefore, the use of RTA aligned with the overall research approach. However, the choices made while completing each phase of RTA required strong reflection and were important to maintain methodological congruence.

RTA assumes that researcher subjectivity is a strength and a tool, highlighting that data analysis and interpretation are never objective. Classical pragmatism also considers a degree of subjectivity in research purporting that experiences are constrained by environment and our understanding of them is limited by interpretation; however, it is not a purely subjective phenomenon as experience is not viewed as inside the individual but as a cyclical process involving subject and object (Brinkmann, 2017). Savin-Baden (2013) situates pragmatism slightly closer to objectivity than subjectivity on the spectrum of research philosophies,

and in practice, the data analysis and interpretation choices made in this study support this positioning by acknowledging the need for subjective interpretation whilst adopting a more experiential, semantic, and inductive orientation to RTA. This slight leaning towards logic also reflects alignment with the "common sense" notions of pragmatic research methods.

The aim of the data analysis and interpretation in this study was more experiential than critical to remain true to the participants' lived experiences. The orientation to the data was more inductive than deductive, relying on the data content to drive the theme development. Deductive data analysis was used minimally when exploring and interpreting how two existing lower-level theories from literature, the theory of DOI and CPT, might apply to the themes generated in this study.

The classical pragmatic notion that knowledge is judged based on utility rather than accuracy required the analysis to be grounded in the participants' verbatim accounts. Therefore, a semantic focus was primarily used to describe the data at an explicit level, and language was viewed as intentional in this study, conveying the speaker's unique reality.

The six thematic analysis phases and the various nuances of the approach used in each phase during this study are described next.

Phase 1 – Familiarisation

Phase 1 of RTA involved undertaking the three analysis processes of immersion, critical engagement, and notetaking to ensure familiarisation of the dataset.

Full immersion in the dataset was required to drive deep knowledge of its content. This was achieved firstly by listening and re-listening to the interview recordings. While the process of transcribing greatly aided in dataset familiarisation, re-listening to the recordings was also undertaken to ensure thorough notes were made on tone, repeated word usage, common threads of topic, body language, and the content of the interview discussion. The interview transcripts were also read and reread until it was felt that the content of all the interview data could be broadly described without using transcripts.

Active engagement when listening and reading was needed to critically engage with the interview output as data rather than just information. This required distancing from the dataset whilst also being immersed closely in it. Critical engagement was achieved through the process of active reflection during immersion. A sample of the questions asked while undertaking the data familiarisation were:

- What assumptions around the approachability of quantum computing is (*participant name*) basing this response on?
- What frustration is (*participant name*) really trying to describe here?
- Why did I react to that comment so strongly?
- Is (*participant name*) speaking from a place of privilege when discussing this?
- Why did this interview not seem to flow well?

Notetaking was undertaken throughout the familiarisation phase. In many cases, these notes were in the form of questions and answers and were added to the ongoing field notes and reflexive journaling process. Annotations were also made on printed copies of the interview transcripts.

Undertaking familiarisation highlighted how the data and participant meaning could be interpreted very differently when tone and body language were apparent versus when read on a page. Excerpts from reflexive notetaking shown in Figures 5 and 6 describe the influence tone and emotion had on interpreting the participants' contribution to the study by firstly presenting an interpretation of the interview directly after rewatching and listening and secondly an interpretation after reading the transcript without audio or visual input.

Figure 5

Excerpt from Reflexive Notetaking After Initial Rewatching and Listening to Interview 8 Recording

Wow, I think this will be an outlier. It was obvious from the first 2 minutes that the interview did not go in the direction of my standard questions. Participant was very passionate but incredibly negative. Found it incredibly difficult to keep interview on track, keep a positive and neutral mindset, tone, and response to his statements as they were so negative. I'm not sure of the value of this session in answering the actual research questions…clearly, he believes there are much greater potential threats as a result of quantum – should I review my scope? I seem to have found it hard to balance empathetic responses while still avoiding leading questions or encouraging his views – I was agreeing with some statements rather than maintaining neutrality, as that seemed to be what he wanted. He seemed very frustrated – but was it the topic, me, or his current experiences?

Figure 6

Excerpt from Reflexive Notetaking After Transcript Review – Interview 8

OK, so I started this transcript review a tad wary as immediately recognised the session and remembered it being tense. Consciously taking a step back and put on my hat of curiosity and interested observer to read this… Honestly, I didn't have much hope for useful data from this interview however what a surprise (and relief). (Participant name) has made some really valuable and unique!!!! observations. Definitely feel more encouraged about the final research output. (Participant name)'s frustrations seem to be very directed at the cultural landscape and attitude in NZ of "just doing enough" and while negative there are solid ideas here that could help!

At the start of the familiarisation process, the sheer volume of the interview data became overwhelming, and the sheets of typed notes began to feel disjointed. Therefore, a more visual handwritten text and image "doodle" method was adopted to assist in this process when re-listening to the recordings. Braun and Clarke (2013) suggest this method may help in remembering ideas you have started to engage with and managing larger volumes of data. Engaging with the interview data this way made the process less arduous and more fun. As the doodle reflection displayed the whole interview on one page, it also supported critical thinking and memory by allowing easier linking of key ideas between one interview and another. Figure 7 shows the familiarisation doodle created during one audio interview review.

Figure 7
Familiarisation Doodle Representing One Audio Interview

Finally, systematic familiarisation notes were made that encompassed the full dataset. Notes were made to capture the overall impressions, possible patterns, and outstanding questions from the data analysis in this phase. The overall notes in this study comprised broad statements and questions about possible ideas to explore further.

Phase 2 – Coding

Coding in RTA is an interpretive process that involves carefully reading all written transcripts and tagging all pieces of text that appear to contain meaning or relevance to the research questions (Braun & Clarke, 2013). Braun and Clarke (2013) view the subjectivity of the coding process as a strength rather than a weakness and that rigour is driven by the depth of engagement with the data. In this study, all interview transcripts and the research journal (including field notes) were systematically and fully coded to ensure detailed data interrogation and to support rigour and analytic completeness.

Both deductive and inductive coding techniques were used; however, the majority was inductive. Initially, a small set of 10 priori codes was derived from the research questions, interview questions, and theoretical framing concepts. Preliminary coding was undertaken on a pilot dataset to refine these priori codes. This refined set of codes was then used in the first coding cycle. As the coding process evolved, the discovery of new concepts in the data drove the creation of many more inductive codes. Subsequent coding cycles evolved the coding scheme further, and many of the original deductive codes were subsumed into broader categories or changed to represent the data more accurately.

Descriptive coding was used as the first coding method. This involved creating a code based on a summary description of the actual topic written or talked about. Once again, the volume of the data presented a

challenge at this stage and therefore, initially, macro coding was undertaken, whereby larger groups of text that described only the essence of the data and the major concepts were coded (Saldaña, 2016). This first descriptive macro coding round resulted in the creation of 30 codes and led to an index of the data contents for further coding and analysis.

The desire in this phase of RTA is to capture singular ideas with codes, not multi-faceted themes (Braun & Clarke, 2022) and after inspecting the code output from this first attempt, the codes were deemed to be too high-level as they summarised groups of ideas rather than clearly articulated individual ideas. Therefore, a second, much more granular round of descriptive coding was undertaken to ensure a deeper and more trustworthy data analysis. This granular coding resulted in the creation of some codes which were too fine-grained to contain more than one reference, and these were combined where possible to represent a more general concept.

During this phase, the number of overall codes varied widely from around 50–170 at any time. The codes were constantly refined through multiple further rounds of coding, and a snapshot of each coding round was saved to ensure the code creation process could be reviewed as and when necessary for further refinement. Experts disagree when discussing an ideal number of codes for a research study, and the literature suggests that anywhere from 30 to 300 different codes should be generated. However, most authors agree that the final number is one large enough to capture the nuances in the dataset whilst also being manageable (Creswell, 2018; Friese, 2014; Lichtman, 2013). Ultimately, 70 codes representing the content were finalised for this dataset.

RTA recognises that data can be coded at various levels of meaning, from descriptive and participant-driven (semantic) to researcher-driven or conceptual (latent). Using descriptive coding led to the initial generation of semantic codes that stayed closer to the participants' language. For example, the code "not enough time" was created when several participants repeated those exact words. Using primarily semantic codes was also a conscious choice driven by the desire to reflect the study's practical nature and capture the participants' true experience. However, as the descriptive coding progressed, several latent codes did evolve. For example, when coding an interview passage where the participant described a collection of issues they were experiencing, such as lack of funding and resources and expressed clear frustration that this was not changing, a more latent code of "cybersecurity is not valued enough" was created.

Resisting the desire to move ahead of the process and develop early themes was a challenge throughout the coding stage and required intentional effort to avoid. To manage the inclination to jump ahead, high-level notes on possible themes were taken but consciously parked in the research journal to enable the focus to return to the individual codes. The reflexive journal entry shown in Figure 8 outlines the frustration felt during this stage.

Figure 8

Reflexive Journal Entry Created During Coding Round 2

Alright this is hard. I hate coding right now. It seems endless and I am definitely questioning whether it's worth the hours of effort. Getting impatient. I can clearly see large-scale themes/topics already jumping out at me … they've been jumping out since the interviews really. But – are they just what I always expected to see???? Possibly. I know that ultimately, I should get a different/better result if I stick it out and do this thoroughly so I'm just noting things down as ideas and going back to the granular. Committed to sticking with the process as it must be for a good reason, and I need to push away my preconceived ideas about the final product!!!! Try working for shorter coding time blocks to help stay focused.

In addition to descriptive coding, an affective method was used called values coding (Saldaña, 2016). Values coding allowed the participants' worldviews and perspectives to be highlighted by coding values, attitudes, and beliefs. This output was categorised and reflected in terms of overall meaning.

Descriptive and values coding methods were used as they were most suited to generating answers for the research questions. For example, descriptive coding can reveal answers to epistemological questions, such as whether a participant understands quantum computing-enabled threats, whereas values-based coding may uncover personal interpretive meanings, such as participants' ethical views on quantum computing (Saldaña, 2016). Initially, attribute coding was also considered for use; however, it was ultimately discarded as the output from this coding style, such as demographic data, was judged irrelevant for answering the research questions.

The data was coded primarily using NVivo. NVivo allowed the coding framework to be designed and applied across all data captured, and it was invaluable when analysing the large volumes of unstructured text collected through this process to identify the key themes and derive insights. While using NVivo successfully enabled the streamlined management of the overall dataset and coding process, manual coding (pen and paper) was also undertaken. The manual approach was used mainly at the start of the coding process when developing the codes for an individual transcript proved difficult. Using pen and paper coding enabled engagement with the data in different ways and in different locations, and it was found to be successful in removing blocks that had been present in the coding flow. Manually reviewing the created codes also assisted with the code refinement process, as additional linkages and overlaps in codes that were not obvious in NVivo were discovered. The output from manual coding was then transferred into NVivo to maintain consistency.

The final list of codes generated in this phase can be seen in Appendix D.

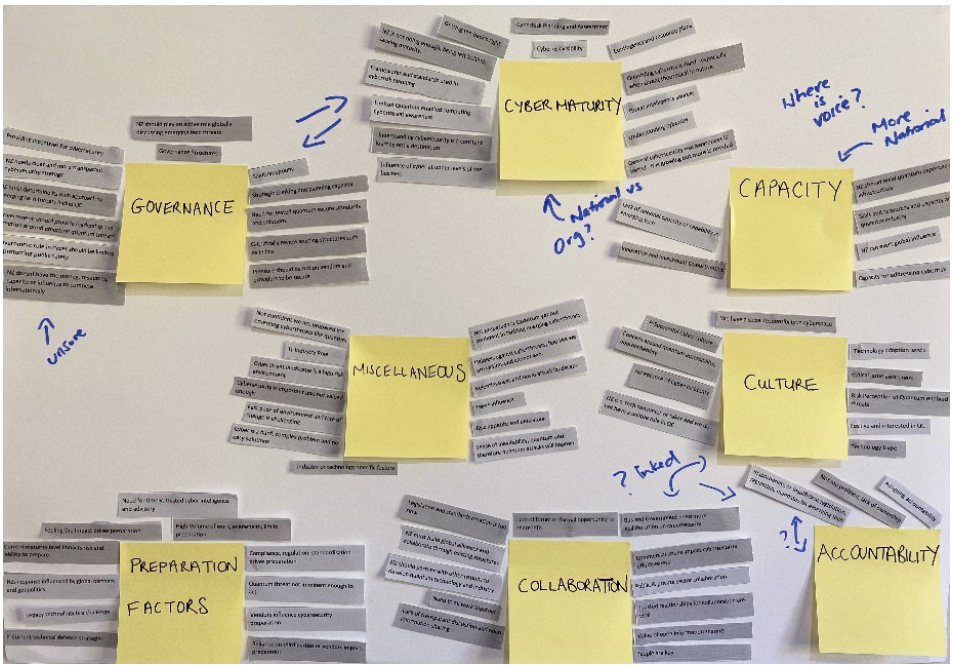
Phase 3 – Generating initial themes

At this stage, the focus shifted from micro detail to macro-scale data analysis to generate themes from the dataset. Compared to other thematic analysis techniques, a key distinction of RTA is that a theme represents a 'conceptual pattern' rather than a summary of the range of responses collected on an issue (Braun & Clarke, 2022). The value of the more granular coding rounds undertaken became very apparent at this stage, as the initial macro coding would not have allowed for pattern identification.

To derive the initial themes, codes were clustered into groups to identify broad ideas across the data and determine any patterning. Firstly, a manual mapping process was undertaken to group the various codes physically and explore possible patterns. An example of this early analysis is presented in Figure 9.

Figure 9

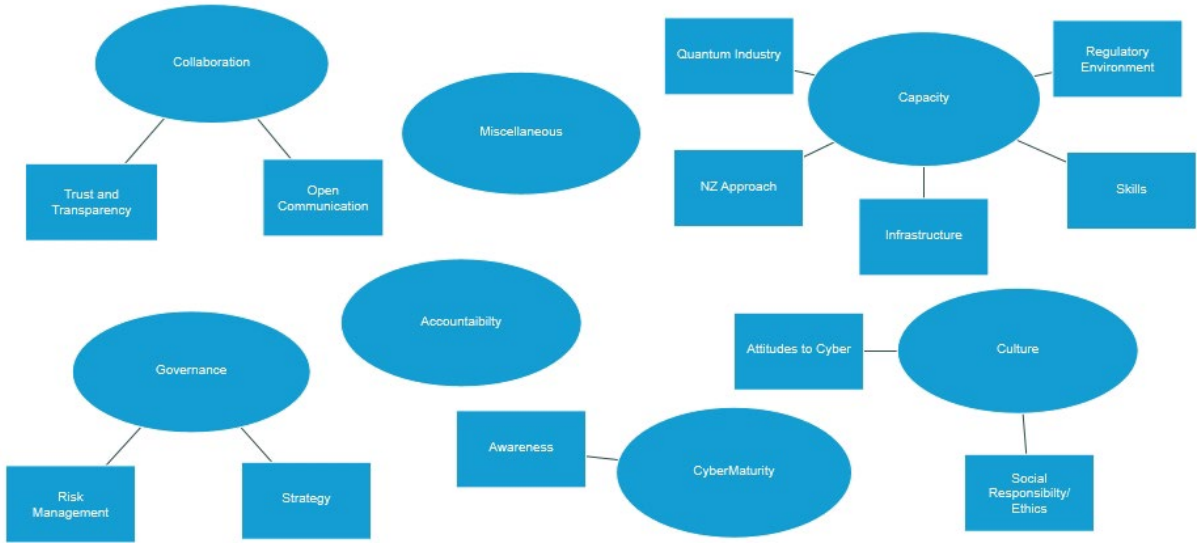
Manual Map of Initial Theme Creation



A variety of thematic maps were created in NVivo and the final candidate themes were decided upon (see Figure 10).

Figure 10

Thematic Map of Phase 3 Candidate Themes



In this phase, a group of codes that covered government resources, infrastructure, solutions, investment, and the overall need for greater capacity in the emerging technology space were identified, creating a

candidate theme, *capacity*. Several subthemes of *capacity* were identified, including the *NZ approach*, *infrastructure*, *skills*, *quantum industry* and *regulatory environment*.

A cluster of codes around the need for intelligence and working together were grouped and described in a candidate theme of c*ollaboration* with related subthemes of *trust and transparency,* and *open communication*.

Governance was initially a code in phase 2. However, when clustering the codes, it was determined that many sat within the overall concept of governance. Therefore, this code was promoted to a candidate theme with risk management and strategy subthemes created to highlight some related but strong concepts within *governance*. Nesting the codes that formed a pattern of *accountability* as a subtheme of *governance* was an initial option; however, the concept of accountability was such a strongly recurring idea throughout the dataset that it warranted the creation of an overarching candidate theme at this stage.

A pattern of codes describing maturity was combined in a candidate theme of *cyber maturity* with *awareness* created as a subtheme of this. Codes that described a pattern of values in the landscape generated the candidate theme *culture* with subthemes of *social responsibilit*y and *attitudes to cyber* nested beneath.

Using a suggestion from Byrne (2022), a *miscellaneous* theme was also created to hold the orphan codes where a link to the other candidate themes or a clear pattern was yet to be discerned. This enabled these codes and ideas to still be visible in the high-level analysis diagrams for consideration.

Developing themes this way was a new skill, and at times, topic summaries instead of themes were explored. For example, an initial theme idea around preparation factors (see Figure 9) resulted in a collection of codes that summarised why NZ businesses were not preparing for quantum-enabled threats. This initial theme contained a variety of issues, such as the high volume of work, reliance on vendors, current technical controls, and the need for cyber intelligence. While this collection of codes resulted in some useful ideas for developing the conceptual model of preparation, it also contained a wide variety of contradictory data. It was recognised as an early mistake as the output was clearly a topic summary rather than a theme, and it was therefore discarded.

As with generating codes from a dataset, no correct number of themes identified in the literature is ideal (Saldaña, 2016). The number of themes generated in this phase was intentionally not constrained, as these could always be refined in subsequent RTA phases.

Phase 4 – Developing and reviewing themes

In phase 4, the full dataset and initial candidate themes were revised to validate their scope and quality and identify any potentially better patterns. This phase also drove further reflection to ensure the themes proposed best represented the story of the data while remaining close to the data itself.

All data coded to each candidate theme was reviewed to ensure the theme remained viable by having clear boundaries, containing meaningful evidence, being coherent, and conveying something important to the research questions. This process was time-consuming and highlighted where occasionally data had been coded incorrectly or in duplicate, and the negative impact of over-coding in phase 2 to “err on the

side of caution" was felt. However, despite finding this process arduous, it further refined the themes and themes that were much better defined in scope and size.

One challenge faced in this stage was ensuring the content of the themes did not overlap. For example, the candidate themes of *accountability*, *governance*, and *maturity* all tended to overlap, and many data extracts were coded to two or all three of these themes. The documented RTA process tasks the researcher to fully define the themes at the next phase; however, due to the clear overlapping of several candidate themes, the need to create definitions for these areas became important in this earlier phase to move forward with clarity.

Defining and reviewing the themes led to removing *governance* as an overarching theme and placing it as a subtheme of *cyber maturity*, as the insufficient governance mechanisms described ultimately contributed to cyber maturity levels. After a full review of the codes in the *accountability* theme, it was determined that whilst it was a strong narrative throughout the data, the need to assign accountability as described in the data was a concept of governance. Therefore, this theme was removed at the top level, and the codes within were nested under *governance*.

After reviewing the codes within the subtheme of *strategy*, they were raised to a top-level theme and renamed to apply *a strategic lens* to better capture the content.

Capacity remained a top-level theme as it conveyed an important and independent concept.

Finally, reviewing the theme of *collaboration* led to a name change to *trusted relationships* to better reflect its concepts.

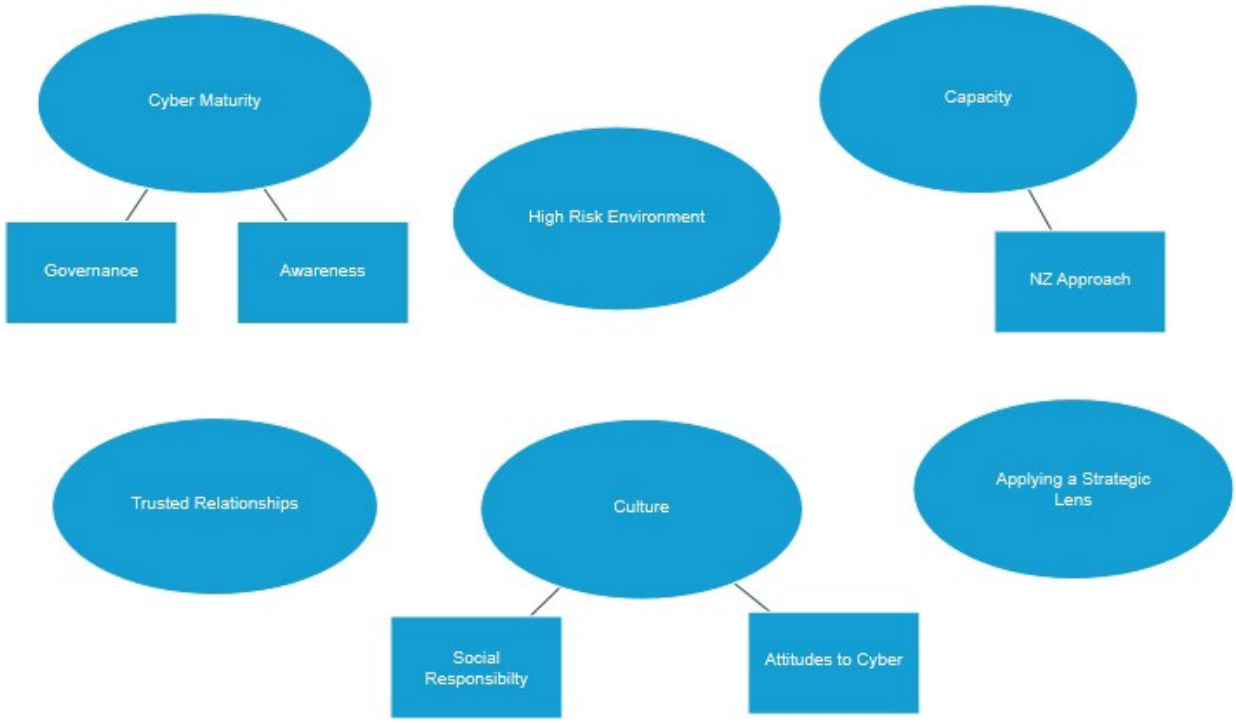
Once the data coded to each candidate theme was reviewed and a set of revised candidate themes was produced, they were reviewed against the entire dataset. According to Braun and Clarke (2022), this step allows the analysis to move once again closer to the dataset as a whole. An observation at this point led to the review and rebranding of the *miscellaneous* theme to an important concept not yet captured by the candidate themes – that of the high-risk environment. Several codes from other themes that fit better within this narrative were also moved to the new theme of *high-risk environment*.

Additionally, Braun and Clarke (2022) caution that the purpose of this process is not to create a multi-layered, fully demarcated map; therefore, several subthemes were removed from the maps as the concepts they described could be sufficiently represented in the narrative findings.

The final output of this phase was the provisional themes outlined in Figure 11.

Figure 11

Thematic Map of Phase 4 Provisional Themes



Phase 5 – Refining, defining and naming themes

1) Refining and defining the themes

In this phase, theme definitions (or abstracts) were created or refined, if created previously, to clarify and illustrate the themes. This process in RTA is intended to refine and test the scope of each provisional theme to see whether the core concept can be effectively described (Braun & Clarke, 2022). The questions asked during this phase to create the abstracts were derived directly from Braun and Clarke (2022) as below:

- What is this theme about?
- What are the boundaries of this theme?
- What is unique and specific about this theme?
- What does this theme contribute to the overall analysis? (Braun & Clarke, 2022, p. 111).

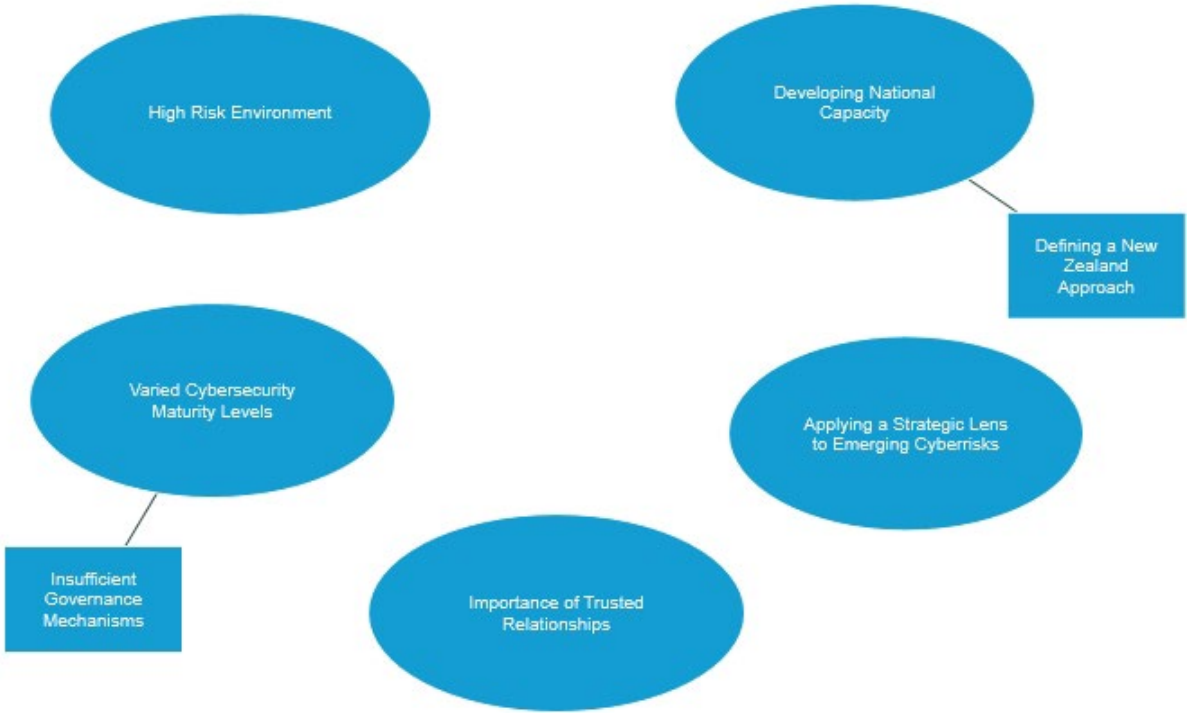
As a result of creating definitions for the remaining candidates, a final change to the high-level themes was made. The theme of *culture* was removed as each of the underlying subthemes and concepts were already encompassed within other high-level themes, and therefore, this theme did not contain the breadth and depth of unique content needed for it to remain. For example, ethical awareness was covered in *awareness levels* under the theme of *cybersecurity maturity levels* and the ideas conveyed within the subtheme of *attitudes to emerging technology* were already represented in several other areas, such as *high-risk environment* and *applying a strategic lens*.

2) Naming the themes

Braun and Clarke (2022) identify that a good name for a theme "is a short phrase or heading or subheading that captures the essence of the theme and engages the reader" (p. 112). Prior to this stage, the proposed themes had largely been represented by one word, which identified the topic but did not represent the patterning of the data within. Naming proved challenging, with multiple attempts to capture each theme's intent and scope. Acceptance that the naming may remain imperfect depending on the reader's viewpoint ultimately allowed progress. A depiction of the final themes can be seen in Figure 12.

Figure 12

Thematic Map of Phase 5 Final Themes



Similarly to classical pragmatism, experiential inquiry is described as an iterative and continuous process, and the steps described above to complete RTA were strongly recursive. While the major shifts in the thematic analysis are described in each step in this section, the process itself was not undertaken strictly in sequence, and in practice, moving back and forth between phases to refine and modify the outputs was undertaken. For example, while reviewing the codes in each candidate theme in phase 4, it was clear that several codes could be combined into one, and adjustments were made to the master code list to reflect this. Additionally, the names of some codes and themes changed whenever the data analysis provided further insights to warrant this.

Phase 6 – Writing a thematic report

Phase 6 in RTA involves writing up the process undertaken and the analysis output in the form of results and discussion, as seen in Chapter 5 (Findings) and Chapter 6 (Discussion).

RTA values a subjective, situated, aware and questioning researcher (Braun & Clarke, 2022). The researcher's voice in this study is that of the interested observer. As such, the writing tone is not completely

impartial as a positivist stance might demand, but one that acknowledges an important degree of subjectivity whilst also ensuring the practice of strong reflexivity drives interpretive output that remains true to the contextual knowledge and experience of the participants.

Research utilising RTA often combines the writing up of findings and discussion in one section (Braun & Clarke, 2022). However, as this study derived findings from two separate methods (interviews and document analysis), the findings of each are presented separately before a discussion combining insights from all areas is presented.

4.7.2 Document Analysis

Organisations of all types increasingly use online documents to communicate information, and pragmatic qualitative studies have successfully used these available documents as data as they provide an available source of information through which the research context may be better understood (Savin-Baden, 2013). Despite being used for many years, document analysis can be described as underutilised as a research method (Merriam & Tisdell, 2016; Morgan, 2022), and consequently, the literature describing its use is limited. However, document analysis can be valuable for a variety of reasons, including allowing easy access to data that may otherwise not be available for research. For example, in this study, the use of document analysis allowed data that represented the stance of other nations on quantum computing threats to be included, which was something not otherwise accessible to the researcher.

The importance of formal, written documents as key characteristics of the bureaucracies in which modern society functions is emphasised by Weber (2015), who described how documents exist within "social fields of action" or within the lived environment where people interact, thereby enabling them to record and shape aspects of experience. This ability of documents to represent contextual knowledge ensures that document analysis aligns with the classical pragmatic philosophy adopted for this study.

Document analysis can be useful for triangulation because convergent views from multiple sources may help overcome any potential weaknesses that arise from using a single data source (Saks & Allsop, 2013). In this study, document analysis supports the triangulation of the findings derived from the interview data. The document analysis additionally provides further evidence to understand and examine NZ's roles on the global stage when addressing the potential threats of quantum computing and the factors that influence cybersecurity preparation in a quantum computing-enabled world.

4.7.2.1 Sampling

It is important to choose a sampling technique that enables suitable data to achieve the research goals (Morgan, 2022), and purposive sampling satisfied this criterion for this study.

The types of documents included for data analysis in this research were textual documents that were publicly available using standard retrieval methods, such as internet searches. The process for document analysis in this study followed the design described by Savin-Baden (2013), involving three main stages:

1. Collecting and organising: As many relevant documents as possible were initially collected. However, selecting the most appropriate documents to analyse when conducting document analysis is crucial to ensure trusted findings (Morgan, 2022); only those relevant to the specific research questions were saved and recorded for consideration. An initial search collected nation-

state-created or endorsed documents that specifically referenced quantum computing and cybersecurity. It was quickly observed that this potential document scope was too limited, and it was expanded to include any documents that talked about emerging threats in the cybersecurity landscape, even if quantum computing was not specifically mentioned. Draft or discussion documents were included where a final version had yet to be produced, as these demonstrated the most up-to-date thinking on the research topic.

2. Assessing quality: The quality of the collected documents was then assessed using the criteria proposed by Scott (1990) of authenticity, credibility, representativeness, and meaning. Documents were only included when they were deemed to meet the following:

    a. The source was deemed genuine, and the document was retrieved from the primary source. Using only documents from the primary source ensured that versions or interpretations of the original document which may contain misinterpreted content or content omissions, were not included. While upholding authenticity, this introduced additional limitations on the sample of available documents as it meant that only documents available in English from the original source were included. Strategy and planning documents from countries such as China were necessarily excluded from the scope, limiting the ability for global views to be represented. While a translation of source documents from these countries was sometimes available, a conscious choice was made to exclude these as any translation by nature will have its own potentially biased interpretation already imposed on the content, and the researcher could not confirm the legitimacy or accuracy of these translations.

    b. The documents had been authored by groups or individuals with authorised credentials. Each author was researched to check for a known publication history in the research area and formal credentials. This criterion was easily confirmed for the documents included in this study.

    c. There were no obvious errors or versioning conflicts. The versioning of the documents collected could be confirmed in all but two instances. These two documents did not have any version control; however, they were ultimately included as all other criteria were confirmed and no alternative versions could be found. One potential document was discarded from the collected set at this stage as it contained spelling errors that seemed inconsistent with the quality of the final publication.

    d. The content was clear, comprehensible, and transparent regarding the intended purpose. There are advantages to using documents, including the ability to reveal what people do or value (Savin-Baden, 2013). In this project, they gave insight into various nation-state and organisational perspectives regarding quantum computing. However, it is important to acknowledge that documents can be “staged” in that they can be designed to show what a particular group wants others to see about it. Therefore, ensuring the documents had a clear purpose was included as a measure of credibility in this study, ensuring the researcher remained mindful of this staging.

3. Analysing: Morgan (2022) highlights the importance of choosing a form of data analysis that enables new insights to be developed during document analysis and advocates for a reflexive thematic approach to achieve this. Therefore, the analysis of the documents followed the same formal RTA process used for the interview data to generate key themes. Documents selected for the study were imported into NVivo for coding.

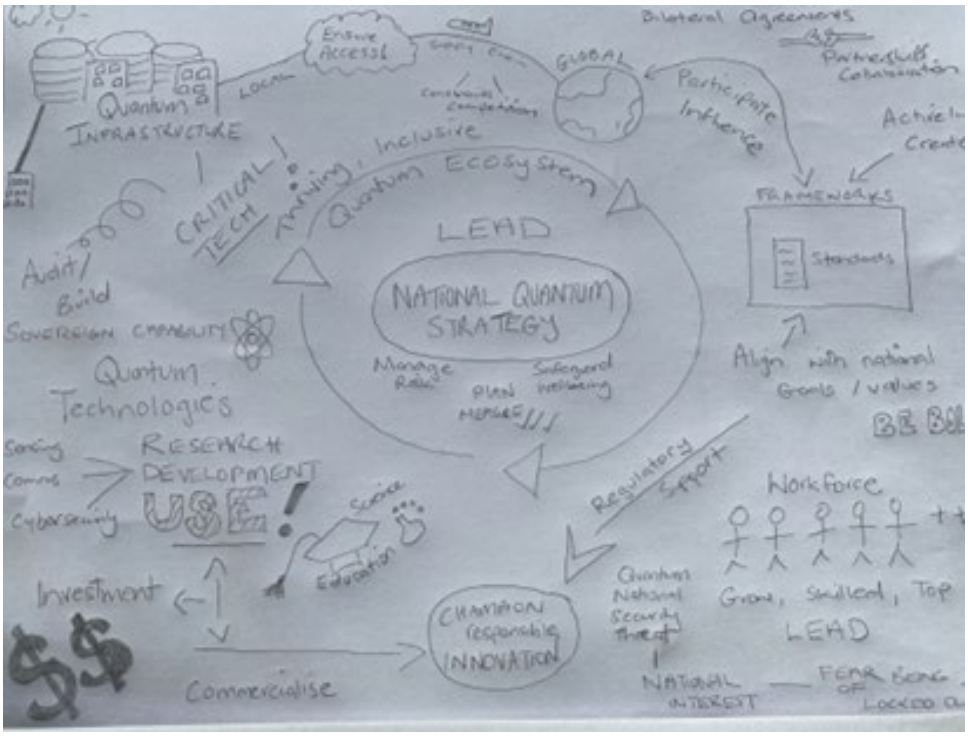
Phase 1 – Familiarisation

Immersion in the dataset was achieved by reading and rereading each document. Familiarisation with the document content was comparatively easier than familiarisation with the interview data as the data in each was well structured, and the nuances of body language and verbal punctuation were absent.

Notes around the document tone, assumptions, and researcher's reactions to the text were taken whilst reading each document to ensure critical reflection. Familiarisation doodles were utilised as they were with the interview data to capture the main concepts of each document on one page. An example of a doodle is presented in Figure 13.

Figure 13

Doodle Output During Familiarisation in Document Analysis



Unlike when undertaking data analysis during the interview method, full overall familiarisation notes were not created early in the document analysis process as the collection and inclusion of document data was much more iterative and a final set of documents was not determined until later phases. To ensure overall impressions of the dataset were still captured, a working visual depiction of the core concepts across the dataset was created, edited, and maintained throughout the entire data analysis process.

Phase 2 – Coding

An inductive coding process was used for the document analysis whereby codes evolved with the researcher's understanding of the data. Descriptive and fully semantic coding was used, focusing on explicit meaning to represent the practical nature of the documents. The scope of relevant data within the documents was more limited than that found during the interview data analysis. Therefore, the coding process resulted in fewer codes being generated to fully represent the concepts. A total of 46 codes were created.

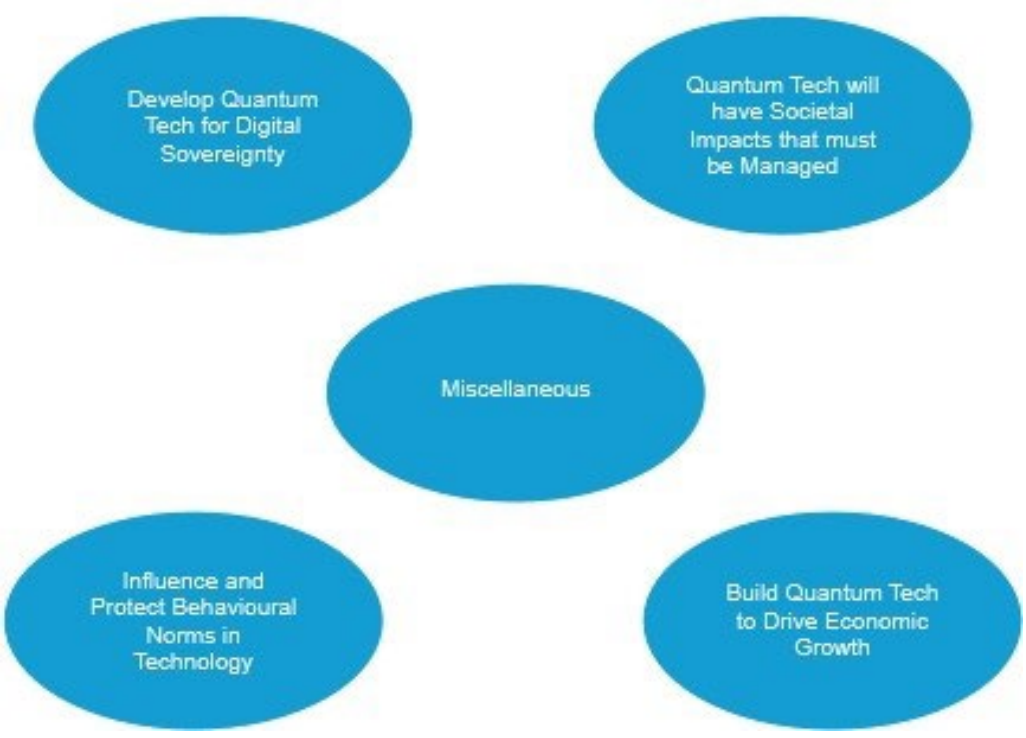
All data coding in this phase was undertaken in NVivo, and the full list of codes can be found in Appendix E.

Phase 3 – Generating initial themes

The process of inductive coding allowed themes that reflected patterns of shared meaning to be generated from the dataset (Braun et al., 2019). The codes generated were clustered in groups representing core concepts or patterns in the dataset. The thematic map in Figure 14 shows the initial candidate themes generated from the document data.

Figure 14

Thematic Map of Phase 3 – Initial Candidate Themes



Codes representing various aspects of digital sovereignty, including how quantum technology will influence the establishment and maintenance of national digital sovereignty, were grouped in the candidate theme of *develop quantum tech for digital sovereignty*.

Another group of codes that described the positive and negative impacts foreseen by quantum technology were clustered together into a candidate theme of *quantum tech will have societal impacts that must be*

managed. Several codes that described collaboration as necessary to forward national values in cyberspace and penalise those who do not behave in alignment with these values were recognised as a pattern. These codes were therefore combined in the candidate theme of *influence and protect behavioural norms in technology*.

Codes that associated the development of quantum technology with economic growth and success and how that may occur were grouped in the candidate theme of *build quantum tech to drive economic growth*. Finally, codes where a discernible pattern could not be seen but may still be important to the analysis were grouped and parked in a *miscellaneous* theme.

Phase 4 – Developing and reviewing themes

In this phase, candidate themes were reviewed to ensure that the patterns generated in phase 3 best represented the full story of the data and that they were each well-defined and had sufficient evidence to address the research questions. The review of all data within each candidate theme led to the changes depicted in Figure 15.

Much of the content of the candidate theme, *build quantum tech to drive economic growth,* described the economic benefits and advantages of developing quantum technology. On reflection, this theme did not contain sufficient evidence to answer any of the research questions and was removed as a primary theme.

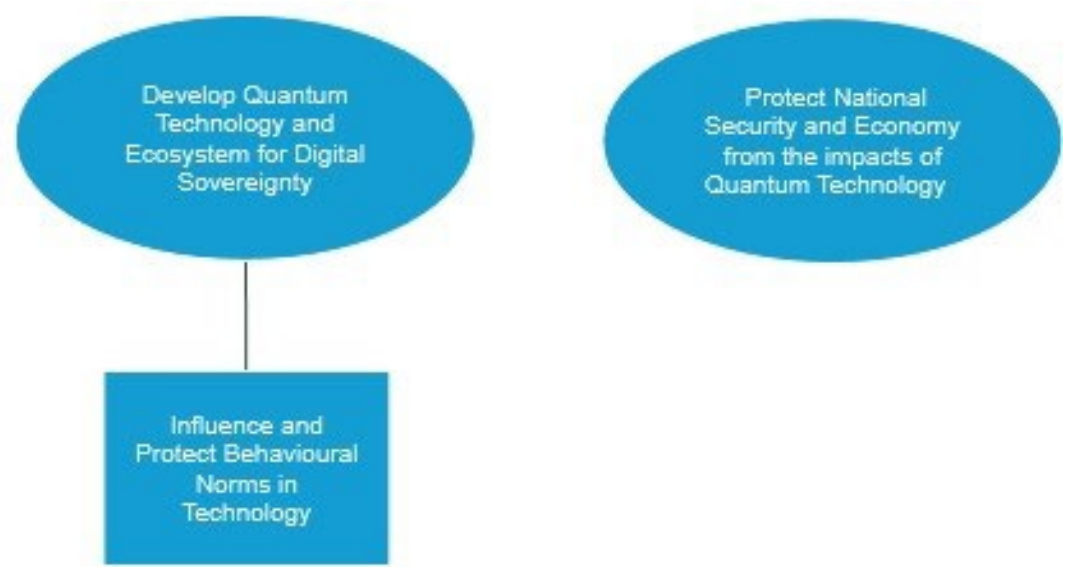
Several codes relevant to the research question from *build quantum tech* to *drive economic growth* related to wider issues around a quantum technology ecosystem, such as creating a quantum-enabled workforce. When added to several codes nested under the miscellaneous candidate theme, these codes also contributed to a pattern that resulted in the creation of a candidate theme of *develop quantum tech for digital sovereignty*. After fully reviewing the content of this theme, including the newly subsumed codes, the theme name was broadened to *develop quantum tech and ecosystem for digital sovereignty*.

Exploration and reflection around the candidate theme *influence and protect behavioural norms in technology* led to the understanding that this belonged as a subtheme to *develop quantum tech for digital sovereignty*. Digital sovereignty requires the ability to act in alignment with national values; therefore, creating and protecting national values in technology aligns closely with, and contributes to, the overarching theme.

Finally, the content of the codes under the candidate theme *quantum tech will have societal impacts that must be managed* was critically reviewed to ensure alignment with the research scope. As a result, one code was discarded as the content was deemed irrelevant, and the theme was renamed to *protect national security and economy from the impacts of quantum technology* which better described the core concept of the theme that contributed to answering the research questions.

Figure 15

Thematic Map Created in Phase 4 – Candidate Themes



Phase 5 – Refining, defining and naming themes

Theme descriptions were created for each of the proposed themes from phase 4. Creating these descriptions enabled the scope of each theme to be clearly defined and gave confidence that the themes generated accurately described the dataset. At this stage, no changes were made to either the themes or their names.

Phase 6 – Writing a thematic report

The findings from the document analysis are presented in Chapter 5 (Findings). Extracts from the documents were used to illustrate the major themes. Further interpretation of these findings, including an exploration of the wider theoretical, literary, and contextual interconnections, is presented in Chapter 6 (Discussion).

Data collection and analysis of the documents was an iterative process, where emerging findings continually informed how to obtain and interpret further data. The number of documents to be included in the analysis was not determined prior as it was not clear how many documents of this nature existed in the public record or how many documents would be required to gather enough data to generate themes and reach a point of redundancy whereby the researcher ceased to gain further insights around the topic. The document analysis was deemed complete when it was felt that the researcher sufficiently understood the area and scope of possible approaches presented and felt they had obtained a complete to a nearly complete set of available documents relevant to the area of inquiry. In total, 31 documents were analysed. A full list of the documents included in the study can be found in Appendix F.

4.8 Quality

Qualitative methodologies have been criticised in the literature for lacking rigour, transparency, and integrity of findings (Hadi & José Closs, 2016), and therefore, explicitly describing in this section how quality was maintained during this study is of paramount importance.

Researchers have raised concerns about the gap between academia's interest in high-quality research and the real-life issues practitioners face in their environments (Daft & Lewin, 2008; Zundel & Kokkalis, 2010). Rigour in academia is often achieved by relying upon standard methods that aim to develop universal truths or transferability in findings (Chi Vo et al., 2012; Gulati, 2007), whereas the characteristic of relevance can be more important for those in practice where knowledge that is context specific and contains clear recommendations for action is valued (Palmer et al., 2009). A pragmatic approach to research design that promotes more flexibility in method choice can support relevance; however, this approach has been criticised for focusing on the concept of "relevance in practice" at the expense of rigour. Therefore, demonstrating both the characteristics of rigour and relevance is critical to ensure the research findings are trusted enough to impact policy and practice in the field, which is the desired outcome of this pragmatic study. Adopting Dewey's classical pragmatic stance, which views knowledge in terms of usefulness and replaces any dualistic views of ontology or epistemology, allowed this study to embrace the concepts of relevance and rigour.

The body of literature describing how best to judge quality in qualitative research has been described by Rolfe (2006) as primarily divided into three opinions. The first opinion argues for adopting positivist practices such as validity and reliability; the second opinion rejects positivist paradigms due to the variety of philosophical and theoretical paradigms used in qualitative research and challenges the notion that any pre-determined criteria could work for all studies. Finally, the third opinion also rejects positivist measures but promotes using a set of alternate criteria that include dependability, credibility, confirmability, and transferability to define rigour (Lincoln & Guba, 1986).

Guided by the philosophical lens of classical pragmatism and a reflexive qualitative approach, this study upheld rigour by addressing Lincoln and Guba's (1986) four criteria of credibility, transferability, dependability, and conformability. However, as this study advocates for an inclusive approach that maintains rigour while ensuring relevance, the unique quality dimension of usefulness was added. The specific techniques used to maintain rigour and relevance are described next.

4.8.1 Credibility

Credibility refers to providing enough evidence that research findings are accurately represented and involves demonstrating how bias is potentially identified and mitigated throughout the research process (Johnson et al., 2020). Credibility is considered here from the perspective of the individual researcher, the participants, and the academic process.

Twenty-five years of work experience within the NZ information technology sector enhanced the researcher's credibility in undertaking this study. This work involved reviewing cybersecurity governance, helping businesses prepare for and respond to cybersecurity incidents, and seeing the daily challenges organisations face trying to combat cyber threats. Formal reflexivity and self-reflective journaling were used to question the researcher's personal lens at all stages of the study to ensure that interpretation was conscious. Additionally, the researchers' position regarding the research questions was fully described to support transparency.

Participant credibility was maintained in this study by ensuring the interview findings were presented truthfully and with contextual clarity. Fossey et al. (2002) described the importance of ensuring the

participants' perspectives are authentically represented and interpreted to enhance credibility, and the use of transparent methods in recruitment, transcription, coding, and analysis in this study supports these concepts. The use of a pragmatic lens in this study additionally scaffolds this process by ensuring a strong focus on the "lived experience" of the participants during the interview process and data collection. Interview transcript review was also used in the data collection phase as a member checking or respondent validation technique to enhance credibility and dependability.

In the discussion and findings, exact quotations allow the participants to "speak for themselves" and support authenticity (Guba & Lincoln, 1994, p. 277). A record of used quotes was maintained to ensure that a balanced viewpoint was represented throughout the findings and discussion chapters and that a range of voices was heard.

Academic credibility was supported using regular supervisory meetings to discuss the research process, question the data interpretation, and explore alternative perspectives. This technique of peer debriefing or "analytic triangulation" supports credibility by allowing the researcher to ensure emerging findings or theories are sensible and derived from the data (Hadi & José Closs, 2016).

Congruence between the researcher's beliefs and values, the research topic and purpose, the participant's context, and the methodology and methods used to complete the study are important to support rigour (Gilkison et al., 2016; Mills & Birks, 2014; Spiers et al., 2018). Choices made during this study are transparently described to demonstrate how methodological congruence has been considered and upheld.

4.8.2 Transferability

Transferability refers to how the research findings may be generalised to other bodies of knowledge, contexts, or populations (Johnson et al., 2020). Classical pragmatism describes knowledge as always contextual. Therefore, transferability was enhanced in this study primarily by providing strong contextual detail at all stages to enable the reader to determine whether results may apply to a different situation.

Additionally, a purposive sampling method was used to ensure the greatest diversity in the participant sample, optimise data sources, and promote a rich pool of responses from which to draw conclusions.

4.8.3 Dependability

Enhancing dependability involves describing the research process in sufficient detail so that the process can be repeated (Johnson et al., 2020). The use of maximum transparency when describing the methods used in this study increases its dependability and the ability to compare and test the findings.

4.8.4 Confirmability

Confirmability refers to the ability of the researcher to communicate that the results presented reflect the data gathered and are not based on researcher bias (Johnson et al., 2020). Triangulation was used in this study to combine the methods of semi-structured interviews with document analysis and avoid the inherent bias associated with using a single data collection method.

Strong reflexivity was built into each step of the methodology to ensure researcher subjectivity was always consciously examined, and the nature of "inquiry" inherent in the classical pragmatist lens was utilised to

constantly reflect on how the approach used at each stage might contribute or influence possible findings and outcomes.

4.8.5 Usefulness

A quality criterion for knowledge in classical pragmatism is whether the knowledge is useful in empowering people and helping them cope with the world (Wicks & Freeman, 1998). Ensuring usefulness involves constantly assessing whether conclusions shed light on real-life experiences and difficulties, enabling them to be better dealt with (Dewey, 2000a). This study maintained constant inquiry and reflection to ensure the assessment of findings generated useful knowledge.

Another strategy for maintaining usefulness involves making academic knowledge more accessible to technology and business practitioners, such as ensuring academic findings are accessible to participants who are not overly familiar with formal research methodology (Jarzabkowski et al., 2010). Therefore, the language and terminology used in this study were carefully considered, particularly in writing the specific guidance for business participants (see Section 6.5). The content, which was contextualised, focused specifically on problems the participants had raised and offered solutions.

Dewey criticised research that failed to return the refined outputs back to the context of actual experience (Dewey, 2000a), and therefore, a plan was made to give feedback on the findings of the study to all participants. Additionally, ensuring the participants had an opportunity to describe what outputs would be of value to them was undertaken, and the feedback was acted on. For example, several participants expressed a desire for the researcher to come and speak to their teams in person to discuss the study findings rather than receive a written report. As a written report was unlikely to be read widely, this approach was deemed more useful to them and was included in the feedback plan.

4.9 Ethics

Ethical standards govern research conduct, and adhering to these principles protects the dignity, rights and welfare of research participants whilst also ensuring trustworthy research output that complies with commonly accepted methodological and ethical norms (Congiunti et al., 2023). This project was approved to proceed by the AUT Ethics Committee on June 13, 2022 (see Appendix G). Areas that required ethical consideration included safeguarding participants using formal processes of informed consent, preserving the confidentiality of the participants and the organisations they worked for, ensuring a safe and respectful relationship was maintained between the researcher and the participants, and explicitly describing how the research contributes to interested parties and the wider NZ community. This research did not directly involve Te Tiriti o Waitangi obligations, and therefore, a full consultative process, as outlined in guidance such as Te Ara Tika (The Pūtaiora Writing Group, 2010), was not deemed necessary. However, as this research is situated within NZ and included participants from diverse cultural backgrounds, including experts working with iwi-owned businesses, sensitivity to Te Tiriti concepts of whakapapa, tika, manaakitanga, and mana was demonstrated.

4.9.1 Informed Consent

Potential participants were sent an information sheet describing the research study's topic, scope, and purpose (see Appendix A). Sample interview questions were included in the information sheet to drive

transparency and further inform consent. The potential participants were asked if they were willing to be interviewed, and if they were willing, they were invited to fill in and return the consent form, also attached to the email (see Appendix B).

Completing the consent form indicated the participant's willingness to participate and that they had been provided with an opportunity to ask any questions about the research or interview process. The consent form confirmed that the participant knew the interview would be recorded and transcribed and that the researcher would take notes. The ability to withdraw from the study at any time without being disadvantaged in any way was explicitly stated. Assurance was also given that the participant would be given the opportunity to review the interview transcript and remove any information believed to be sensitive in nature. Written consent was obtained either before or at the time of each interview.

Participants were contacted prior to the completion of the analysis phase and given an opportunity to review and provide confirmation that they accepted their transcript as accurate. As a result, three participants requested minor edits to the transcripts, which were immediately incorporated into the final version used to derive the research findings.

4.9.2 Participant Confidentiality

The information form given to all potential participants outlined how their identity and business identity would remain confidential in all research output. All responses were de-identified.

It was identified early in the design phase that there was a risk that potentially commercially sensitive information may be discussed in the interviews as business processes and standard practices were part of the enquiry. Care was taken to ensure that any material that may be damaging or sensitive to organisational practices or the individual was removed from interview transcripts before use. The transcript review was first done by the researcher and then by the participant, enabling the identification and removal of any comments that appeared to be commercially sensitive.

Participant privacy was always maintained, and participants were not named or otherwise identified within the research or any written output resulting from the research without express consent. All participants were given the option to withdraw from the research at any stage, whereby all data relating to them, including any recruitment correspondence, would be deleted immediately to maintain confidentiality.

A data management plan was created for this study to ensure the security and confidentiality of electronic and physical data (see Appendix H).

4.9.3 Researcher/Participant Relationship

Principles of partnership, participation, and protection were embraced to ensure that measures were undertaken to minimise the risk of harm to the researcher and the participants while undertaking this study.

As described by Brinkmann and Kvale (2015), the qualitative interview gives a researcher "privileged access to people's basic experience of the lived world" (p. 172). This privilege was recognised and honoured in this study by ensuring all interactions were respectful in tone, the time given by each participant was used wisely, the duration of interviews kept to agreed schedules, and the nature of the questions asked were relevant to that participant.

This study intended to develop valuable shared knowledge for practical use by the individuals who contributed insights to the study. This knowledge included high-level guidance for developing preparedness strategies. Using a semi-structured interview guide and pragmatic approach allowed a high level of autonomy in the participants' interview responses and encouraged participants to direct the interview content, thereby highlighting knowledge they believed to be valuable and recognising their lived experiences. All views were respected and represented. All participants were offered the opportunity to validate the transcription of their responses should they have the capacity and willingness to do so.

The participant's primary role was to share information and experiences, and they were asked to share their thoughts and knowledge openly and honestly. Open-ended interview questions allowed participants to express their views without restrictions.

Power imbalances were avoided to ensure no overt or underlying influence was possible in the conversations by excluding participants from the study if they had a current working or personal relationship with the researcher. The interviews were designed to be collegial and exploratory, and the tone was pitched at allowing the researcher to obtain "expert insight" from the participants. It is recognised that if a researcher is preoccupied with their own predispositions around the research question, they may inadvertently shut themselves off from the participant's experience (Peredaryenko & Krauss, 2013). An intentional attitude was therefore adopted during the interviews of open discovery, with the participants being the experts in their experiences. This attitude proved easy to achieve due to the nature of the participants, who were all highly respected and recognised as experts in their domains.

Participants give a lot more than they receive when participating in research by providing their valuable time and energy (Brinkmann & Kvale, 2015). This study acknowledged this by expressing the importance and value of their participation and incorporating a plan to ensure they received a koha and a summary of the research findings at the conclusion of this process. Two participants contacted the researcher after their interview as they had further questions about the topic they wished to be answered. In each case, time was prioritised to satisfy these needs.

4.9.4 Researcher Influence

A researcher's worldview can significantly impact the outcome of a study (Corbin & Strauss, 2015). All researchers bring assumptions and a level of bias to their topic under study, and therefore, Corbin and Strauss (2015) recommend that a plan be formed to reduce the impact of these assumptions. In this study, journaling was used to formalise reflection on the decisions made at each point in the research process and ensure undue bias was avoided. An awareness of how body language and verbal responses may influence the course of the interviews was also kept in mind.

Self-reflection is a key tool for a researcher to question their motives, thought processes and initial interpretations to become and remain aware of their personal bias (Bettie, 2014). After each interview, time was set aside to reflect and write about the interview experience. In addition to the formal reflexive questions designed to be asked at every stage of this study, reflective notes were made on interview impressions, body language, themes, surprising content, potential biases, and any context that may have impacted the interview. Any challenges that arose were also noted. This reflexive journaling was a critical part of the approach.

A research journal was maintained throughout this study. The journaling process ensured that reflexivity was maximised by formalising the iterative practices of reflective thought at each stage of the research journey. Unless written consent was obtained to identify any participant in research outputs, the confidentiality of the participants in this journal was preserved.

The journaling process additionally enabled transparency of thought processes and decisions made, ultimately assisting in maintaining researcher integrity. The journal was a place to express frustrations or doubts over the process or record unanswered questions. Questions such as whom I should contact to participate and internal methodological and method debates were addressed here. The journal was kept in electronic format, and relevant areas were included in formal study outputs, which aided in transparency and clarity of approach.

4.9.5 Benefits of the Research to the Community

The impetus for this research was the personal experience of working with NZ businesses and seeing first-hand the damaging impact of cyber threats on society. This research was designed to create outputs of knowledge that can be used by the wider NZ community to ultimately prevent or minimise the potential harm arising from emerging cyber threats.

A summary report of the findings will be given to all participants to ensure the knowledge is disseminated to those who can best use it. This summary will be designed to be as understandable and practical as possible by using plain language and describing actionable steps the community can take to act on the findings should they wish to. Practical preparedness advice was created as an output of analysing the data. This advice could contribute to national, industrial, and organisational policy development.

The research community will learn more about the current level of awareness of quantum cybersecurity threats in NZ. The research will also indicate whether further research is warranted in this space and in which areas this research should focus.

The research community, government, and the IT industry will gain additional knowledge on how NZ could participate globally in planning and preparing for the emerging cybersecurity threats that quantum computing may pose.

4.10 Conclusion

This chapter has explained the philosophical and methodological choices in the research design. It has outlined the main research questions and sub-questions and the methods, data collection, and analysis approach used to answer these questions. Additionally, this chapter has described how ethics and academic rigour were established and maintained.

Chapter 5 reports the findings obtained from the interview and document analysis methods.

Chapter 5:Findings

5.1 Introduction

Chapter 4 established the research methodology for investigating NZ's role and readiness to face cyber threats in a quantum computing-enabled world. The main research question and sub-questions were formed based on the review of relevant literature undertaken in Chapter 2 that identified potential security risks around emerging quantum technology and a limited understanding of these issues in the NZ context.

This chapter presents the findings obtained from the investigations into quantum computing preparedness. Section 5.2 presents the results of the interviews conducted to determine how prepared NZ organisations are to face quantum computing-enabled threats. Section 5.3 presents the findings from the document analysis undertaken to support the interview data and identify the approach the NZ Government could take both domestically and on the global stage when addressing the potential threats quantum technology may pose.

Overall, the data analysis yielded seven primary themes and three subthemes that describe the core concepts of the primary data. RTA of the interview data resulted in the identification and creation of five of these primary themes along with two subthemes, and the document analysis resulted in the creation of the additional two primary themes and one subtheme. A description of each of the themes found as a result of the analysis and documented in the subsequent sections is presented in Table 6.

Table 6

Identified Research Themes

Theme name	Description of the core concepts included
High-risk environment	Describes the variable conditions in the NZ business operating environment that drive cyber risk, including the cyber-attack landscape, operating models, and the rate of technological change.
Varied cyber maturity levels	Describes the degree of knowledge, platforms, structure, practices, controls, and processes NZ organisations have to respond to proactively prevent cybersecurity incidents, determining overall cyber maturity levels.
Insufficient governance mechanisms	A subtheme that describes the current state of mechanisms such as roles and responsibilities (RACI) and definition and risk management processes that govern cybersecurity and influence cyber maturity.
Importance of trusted relationships	Describes findings around the dynamics of various relationships and their influence on cybersecurity. Cultural levels of trust and sharing are included.
Applying a strategic lens to emerging cyber threats	Describes current thinking and planning horizons for cybersecurity and the influence of these on preparing for cybersecurity threats.

Theme name	Description of the core concepts included
Developing national capacity	Consists of issues around capacity in technology, ethics, and quantum science skills, education systems, and research opportunities. It also includes infrastructure and quantum industry capacity and the legislative and enforcement structures to support quantum computing issues.
Developing an NZ approach	A subtheme that encompasses the potential drivers for NZ to identify a unique approach to managing quantum computing issues domestically and globally, including issues of sovereignty, cultural values, and perceived uniqueness.
Develop quantum technology and ecosystem for digital sovereignty	Describes findings around driving the development of quantum technology to enable national digital sovereignty, including increasing sovereign cyber skills, infrastructure, industry, research, and legislation.
Influence and protect behavioural norms in technology	A subtheme exploring global beliefs around sovereign capabilities and their influence on upholding perceived "norms" and "values" in technology.
Protect national security and the economy from the impacts of quantum technology	Describes findings in areas of developing quantum technology, transiting to quantum-resistant systems, and driving the quantum industry to protect national security and enhance economies in a quantum-enabled world.

5.2 Interview Findings

5.2.1 High-Risk Environment

The literature reviewed in Chapter 2 highlighted an ongoing rise in cyber-attacks on NZ organisations, and the findings here reinforce and further emphasise that NZ organisations face an extremely high-risk landscape in 2024.

5.2.1.1 Relentless, large and novel attack landscape

When discussing the current operating environment, participants overwhelmingly referred to the relentless nature of cyber-attacks, describing their businesses or industries as "*targets*" and "*victims*". Participants expressed how they were "*attacked all of the time, constantly*" and how "*the threats are constant, 24 by 7, 365 days a year*" despite having robust protective systems in place. Participant 19 described the interplay between their cybersecurity function and the attackers as "*an arms race that you're fighting on many different fronts*", and Participant 23 described it as "*Whac-A-Mole, as fast as you put your counter, they move forward*", highlighting the constant battle organisations face today when trying to secure against cyber-attacks that do not stop.

When discussing mechanisms for identifying cyber-attacks, Participant 21 explained that "*whenever we light up a new tool that gives us more visibility of what's happening, we always discover that there's been people trying to nibble at the edges the whole time, and we just didn't know it*", and Participant 7 described an employee mechanism for reporting suspicious activity as "*flooded, constantly flooded with stuff*" further highlighting an environment of constant attacks.

In addition to the relentless nature of the attacks, the participants described experiencing a range of attack types and novel vectors, including DDoS, as reported by Participant 23, "*we've had two DDoS attacks in the last 4 weeks, vectors we didn't know existed*", and social engineering attempts as described by Participant 3, "*we're all getting invoices all the time from random places, you know,* "*please pay this invoice*". *And you're like,* '*Yeah, okay, that's not right*'". Participant 27 summed up the overarching sentiment of the participant group by stating that, "*it's hard for everyone, all organisations are getting hacked, and there's breaches of all types all the time*".

Participants also expressed concern about the "*scary*" scale of recent cyber-attacks and the ongoing severe impacts on themselves and their teams, interfering with their ability to address further threats. For example, Participant 24 discussed the aftermath of a successful recent attack, stating, "*that team are completely deflated*. *The wind's been knocked out of their sails, they're just struggling to keep afloat*. *They're not doing anything new*".

5.2.1.2 Complex operating environment

Participants raised several issues, including competing demands, scale, legacy technology, and third-party vendor reliance that result in a complex daily operating environment for NZ organisations attempting to secure IT systems.

Firstly, the need to balance and prioritise different demands in their operating environments was highlighted as a challenge by participants. For example, Participant 18 discussed the competing demands of delivering a positive customer experience while implementing sufficient technical security controls, stating, "*you've got to give customers trust and confidence that you are managing their data safely, but you don't want to make it too difficult to work and buy from*". Similarly, Participant 8 described juggling a multitude of demands and the difficulty in prioritising these as "*we are dealing with increasing cyber threats and establishing security and the regulatory load of all this happening in multiple jurisdictions*. *We are dealing with having acquired a bunch of businesses and trying to integrate their needs into the business at the same time*. *Trying to put another concern alongside all those other things…How do I prioritise this? Where does it stop?*".

Participants described a cyber operating environment that is growing in scale and complexity, with participants expressing how cyber security is "*such a massive domain now*". The sheer scale of modern IT environments ensures they are a challenge to secure due to the increased number of devices that can introduce vulnerabilities. As Participant 28 described, "*the more things that you have connected, the more your vulnerability grows exponentially with each one*". When discussing why a business may not prepare for quantum computing-enabled threats, Participant 23 emphasised how scale and complexity impact threat visibility, explaining, "*so, it's easy to say patch your servers but we've got 520 apps…we might have 60 to 100,000 servers, forget end-user devices*. *But you only need 10 of these things to have that zero exploit, to have a vector in...So it's not because we don't want to do it, it's normally because we just don't know it's there*". Additionally, even with knowledge of what must be done to secure technology, many participants described how difficult it can be to implement the necessary cybersecurity changes in large environments. As Participant 16 described, "*the problems in a large organisation are hard to solve*. *So, you can turn the tanker as hard, you can have all the knowledge and still not be able to execute*".

The increased complexity of today's technical environment is detrimental to implementing the specific changes needed to prepare for quantum computing-enabled cyber threats. Participants predicted increased difficulty in updating algorithms and securing systems against these threats. For example, Participant 25 explained that, "*20 years ago, if you wanted to change from SSL version 3 to TLS 1.0, you had web browsers, and I think that that was pretty much it. Whereas now everything is TLS-enabled, including a whole bunch of embedded devices and home control systems and automation and factory process controllers and stuff that can't really be updated. So, while 20 years ago doing a shift would've been easy, now, in some cases it's going to be impossible*".

The proliferation of legacy technology also added complexity to the current operating environment and increased the difficulty of securing against current and emerging cyber threats. Participants spoke of how much legacy technology remains, for example, "*it's amazing how much ancient software is still running, how many ancient devices there are*", and described the issue as "*hurting us*" and "*a big problem*" (Participant 27).

Legacy technology debt has arisen in various industries, resulting in insecure systems and a backlog of remedial work for NZ organisations, as described by Participant 8, "*unfortunately in New Zealand, we were very progressive in the '90s. That left us with a massive technical debt legacy, which we haven't really recovered from...the insecurity is gigantic*". Participant 24 summed up the evolution of this legacy landscape, stating, "*I think the problem right now is that, you know, we've gone from decades of building technology, to now, a huge, huge race to try and secure that technology*".

Many participants believed the legacy environment was so vulnerable that they had no confidence in securing it against current cyber threats, let alone any future threats that quantum computing may pose. This lack of confidence was described by Participant 20, who stated, "*I wouldn't even say we're prepared for current threats at the moment because of the infrastructure…I'm not confident that the infrastructure on-prem has caught up with the changes that the business has made. I don't believe they're secure*".

The need to upgrade and address legacy technology also takes up significant time and resources today, limiting any focus on future threat preparation. As Participant 16 described, "*the problem is there are so many laggards, so we're still dealing with 1990s-type issues in IT organisations*". Additionally, when explicitly discussing changing cryptographic algorithms to more quantum-safe versions, participants described how legacy technology would limit the ability to achieve this change. For example, Participant 1 stated that, "*there have been issues with supporting encryption on large databases that are historical in the technology stack, devices that can't be updated, haven't got the computing power to run the new technology. That is a security problem today, let alone when quantum computing comes out. And that's probably the main cause of security vulnerabilities and incidents right now*".

While many participants reported active attempts to replace legacy technology, others reported frustration that this was not happening and a belief that security concerns would not be enough incentive to drive sufficient upgrades and investment in this space. For example, Participant 9 confirmed that, "*if security is the only reason to migrate something, it just won't happen. That has been my experience*".

One area that most participants agreed added complexity to their security operating environments was a strong reliance on third-party providers. NZ businesses rely on third parties to provide information about

threats, develop secure products, and ensure security upgrades occur. Participants described being "*heavily reliant*", "*very dependent*", and needing to place a "*high amount of trust*" in their vendors for various activities, including "*to keep us informed around any critical technical patching*", "*to keep us informed of upcoming cybersecurity threats*" and to "*manage our applications*".

When discussing the need to upgrade to quantum-safe systems and algorithms, participants were clear that they needed third-party provider assistance and expected vendors to play a leading role in ensuring security upgrades. Participant 11 described how they could not complete cryptographic upgrades without vendor assistance, stating, "*it's not something that we can say, 'All right*. *We are going to switch out the algorithm from this piece and pop in a new one'*. *It's not quite that simple*. *We're heavily reliant on our vendors*", and Participant 4 described how they were unaware of the state of their cryptographic algorithms as they expected their provider to be across these security upgrades explaining, "*when I think of the cryptographic algorithms that were used, it's not even on my radar because it's taken care of in a library somewhere…Amazon, is taking care of that for us…I've got no clue what AWS* [Amazon Web Services] *uses and if it's even agile enough to be swapped out, it's nothing we even ask*".

Most participants felt third-party technology providers should lead in ensuring security mechanisms were updated sufficiently to protect against any potential threats that quantum computing may pose. For example, Participant 32 described how vendors are the experts in this area and should, therefore, take responsibility for security, stating, "*I do really think* [vendors] *are going to probably be leading the charge on that front, it makes sense, because ultimately, it's their role, keeping their customers safe*. *And they're the experts*".

Despite the extensive use of third-party providers, the need to rely on them did not sit easily with many participants, as expressed by Participant 5 in stating, "*I find vendors the bane of my existence and yet at the same time, I can't exist without them*", and participants perceived challenges in these relationships around inadequate skills, understanding, communication and action that added further complexity to their operating environments.

The primary reason given for using third-party providers to manage cybersecurity was a lack of in-house skills and resources. As described by Participant 1, "*there's a resource gap, there's the people gap, there's a shortage of security professionals worldwide, and definitely in New Zealand…I think the only way forward for most organisations is to partner with someone that can provide those services*". However, while most participants outsourced aspects of the operating environment to third-party providers to gain access to security expertise, some felt that these organisations also lacked adequate cybersecurity skills. As Participant 17 described, "*we outsource a lot*. *And so, I have to rely on our MSP* [managed service provider] *who charge through the nose, and actually 90 or 80% of the time that I've had experience with them, they don't actually have the skillset that's required*".

Challenges also exist because of the commercial nature of the supplier relationships, as participants felt third-party providers may not disclose all security issues when focusing on selling a product or service. For example, Participant 18 explained, "*I believe our suppliers are typically proactive, but they don't highlight where the vulnerabilities or flaws are in themselves…they don't necessarily point out the things that they don't protect you against*".

Participants also felt that third-party providers did not understand their businesses sufficiently to provide an adequate level of protection and that they were not always responsive or quick enough to respond to the cyber threats relevant to them. Participant 17 described this lack of understanding, saying, "*I think nobody cares about your business like you do, and they don't understand it. For all the sales and marketing, the pitches, they can't deliver. They can't…They don't understand the day-to-day needs and pressures of the business and the systems we are dealing with*".

NZ organisations expect more than they are getting from their third-party providers, and participants highlighted the lack of adequate security advice and support currently received. For example, Participant 16 described a lack of advice, stating, "*it's just not good enough…they don't come to me and advise us on security*". Participant 5 described an example of inadequate support with Microsoft, "*there's several different vulnerabilities that have been put to them to resolve in the last 3 months. They've come back and said either, 'We don't see that as a problem' or 'Yes, we see it as a problem but we're not going to address it anytime soon'. And some of these are quite serious vulnerabilities, and because it doesn't fit within their business model, you're not getting the help you need*". Additionally, threat intelligence information from providers was too slow, with participants expressing frustration that they were aware of cyber threats before their service providers. Participant 17 explained that, "*the information's out there and somehow these big MSPs aren't getting that, they should be getting it faster than me*".

Ultimately, while heavily reliant on third-party providers, most participants were aware that NZ organisations needed multiple sources of cyber security intelligence, advice, and support to succeed in this environment rather than solely relying upon their vendors. For example, Participant 5 explained, "*there is a certain amount of trust you put in* [vendors] *but you can't be silly about it…you take everything with a little bit of a grain of salt*".

When discussing the preparation for quantum computing-enabled threats, participants felt vendors would be key in providing suitable solutions; however, none had been given any information on this topic to date from their third-party providers. Participant 19 described this lack of information and related it to the commercial aspects of the landscape with, "*we're not seeing any information on quantum...I think that's because people aren't shopping for a quantum solution…there's no money to be made in selling a quantum solution that nobody wants*".

5.2.1.3 Rate of technological change

The difficulty of operating in an environment of fast technological change and the challenge of keeping up with the pace of change was a consistent theme throughout participant interviews. Participants recognised how "*technology's changed so much, it just blows my mind*" and described the difficulty in keeping up with the "*constantly shifting*" environment. Participant 4 described this challenge by stating, "*there's so much to focus on now within the security space; just trying to keep pace with normal computing is hard*". The impacts of this fast-changing technological landscape included participants feeling they were "*always on the back foot*".

The pace of change in cybersecurity has accelerated recently due to external events, including the COVID-19 global pandemic. The pandemic added further challenges to an already complex environment by driving fast and insecure operational changes, as described by Participant 3, "*we work with* [client company]. *They*

have secure networks and data centres into Hyderabad…and they wouldn't let our company in New Zealand into those because it's highly secure. And then the pandemic comes, and in India, a large amount of the population went back home. And so suddenly they had to do a complete security 180... Before you had to come to a secure facility in India, to talk over VPN directly into [client company name]*'s environment. And suddenly, it's gone from that security to a guy sitting under a lamp post in a village with his laptop on Wi-Fi, updating core mainframe code*".

The findings show that accepting the fast-changing technology landscape is critical to business success, as described by Participant 1, who said, "*I think it's a change in mindset that you need to be prepared for; things will change rapidly, so you need to get comfortable living in a disrupted world*". Participants also explained the need to adapt and ensure business processes that allow quick responses to changes in the cyber landscape. For example, Participant 6 stated, "*you actually need a cyber risk committee to keep your eye on the ball because things move fast. They move really, really, really fast*". However, the pace of change will be "*too intense*" for some organisations and not all will be able to adapt to the changes that emerging technology such as quantum computing will pose, as explained by Participant 1, "*there will be organisations that just go out of business I guess, because they haven't dealt with the rate of change*".

Culturally, there is an expectation of a "*continued trajectory of technology evolution and pace*" in NZ, with participants noting the perceived positive relationship between technology change and efficiency. For example, Participant 28 highlighted that "*there's an assumption and a pretty successful ideological push to create the association between having things be digital and efficiency and delivering value for New Zealand. There is an immediate assumption that that's just the way forward and that any kind of analogue processes or storage is just moving backwards*".

Participants showed concern that this fast technological change had outstripped society's ability to fully understand its impacts. For example, Participant 28 described this lack of understanding and how aspects of our society, such as legislation, have not kept up with the change and that "*the last 20 years is a great example of technological capabilities really, really massively outstripping our ability to understand and predict their impacts and our ability to deal with them legislatively*".

Some participants saw benefits in slowing down the rate of technology evolution, believing "*there's a very, very compelling argument for slowing down*". For example, Participant 6 described a positive security outcome when using older technology as follows, "*I was at* [company name]*, and we had the power station, the generators were so old they actually had these black boxes that are not software enabled. That was actually a real benefit...because a country with a red flag on it got all the way to the black box, but they couldn't get into it*".

Some participants took the idea of slowing down further by suggesting that some societal functions should be taken offline to prevent them from being vulnerable to existing and future cyber-attacks. Participant 28 described, "*I think that a lot of anything that is core should just not be connected to the internet and ideally should not even be digital. Voting should still be on paper, government records*". However, despite the desire to slow down the rate of change, all participants recognised that slowing down was highly unlikely, stating, "*I don't think it will happen*", primarily due to the cultural assumption that technological advancement is always positive and the widespread appeal of the "*latest shiny gadget*".

5.2.1.4 NZ organisations cannot keep up with the cyber-attack landscape

It was clear from participant responses that NZ organisations were struggling to keep up with the current attack landscape. Cybersecurity professionals felt they "*are never going to be across everything*", and when discussing the environment, the inability to secure everything was a widespread sentiment, as described by Participant 28, who stated that, "*all of this is so inherently vulnerable*. *You can never fully secure anything*".

The findings also show that participants believe being impacted by a cyber-attack is inevitable. When discussing general cyber-attacks, a common sentiment was "*it's not a matter of if, it's a matter of when*", and participants felt it was sensible to adopt a stance of "*you've already been hacked, you just don't know it yet*". When asked if they thought quantum computing would pose a cyber-attack risk, most felt these were inevitable. For example, Participant 4 explained that "*the speed of quantum breaching us means that no human can ever keep up with that and we'd never be able to catch up*".

Many participants expressed not just the inevitability of attacks but conveyed a sense of resignation and helplessness in this landscape. For example, Participant 4 stated that, "*you can't defend against it*. *It's like playing Russian roulette literally every single day*. *That's what my job feels like*". Participant 6 further emphasised this feeling of helplessness, stating, "*ultimately you could spend your entire budget just on security and never do anything else and you still could get breached*", and Participant 8 displayed resignation by stating that, "*the people who are attacking us, this is their day job, all of it*. *And you just can't compete with that…personally I'm kind of resigned to the fact that that's just how the world works*".

This feeling of helplessness against current cyber-attacks extended to defending against the attacks that quantum computing may bring. For example, when discussing the possible preparatory measures to defend against quantum attacks on cryptography, Participant 22 stated, "*to be honest, it doesn't matter whether you create a new encryption key, because it'll just decrypt it*" and Participant 25 expressed serious doubt over whether currently proposed solutions would help reduce cyber-attacks in the future stating "*they can come up with new algorithms, but the attackers don't care what the algorithms are, they'll bypass them, I don't think it's going to make any difference*".

This sense of helplessness against cyber-attacks influences whether organisations prepare for emerging cyber-attacks. To illustrate this point, Participant 16 described an attitude of "*why bother*" seen in NZ organisations today, "*a really interesting conflict in the C-suite I've seen is they don't believe in the solution…We can spend all this money, but we'll never get it done or it won't work so why bother anyway? They're fatalistic about it*". This lack of confidence that any solutions exist was a common sentiment expressed by many participants and was summed up by Participant 20, who said, "*the bad actors will always find a way around it*". A similar sentiment of helplessness leading to inaction exists when specifically discussing actions to prepare for quantum-enabled cyber threats as evidenced by Participant 13 who said, "*it seems to be one of those things where it's going to happen, we don't know when, there isn't anything that I'm aware of that we can buy now that's going to prevent it from happening*. *So then there's nothing that I can really do about it*".

The findings show that trying to manage cyber risk in the current environment is driving high levels of fatigue, overwhelm, and burnout among NZ cyber security professionals. This was described by Participant

5, who explained, "*the problem that we face is fatigue…It can get quite draining*", and Participant 1, who described their own experience trying to keep up with the attack landscape by saying, "*I have felt overwhelmed by events before, yeah…it's a challenge*". This negative impact appeared widespread, with Participant 14 concurring, "*there's definitely a reasonable level of burnout there*".

5.2.1.5 Cybersecurity is a high-risk issue for NZ organisations

The findings show that cyber is recognised as a high-risk issue for NZ businesses. The risks that result from the current cyber threat environment have risen to the top of company risk registers in recent years, as described by Participant 1, "*cybersecurity, or the risk of cybersecurity attacks and privacy breaches*, *is pretty much the top risk on the company risk register now*. *In the last 5 to 10 years, it's gone to the top*".

NZ organisations take cyber security risks seriously, with participants describing how "*this is a real business risk*" and speaking about being "*deeply passionate about protecting customer data*". Participant 23 emphasised how cyber risks are given priority due to their seriousness, explaining that "*we take it very seriously, and we do a lot of work*. *But the default risk position is high, or very high, related to cyber*". *S*ome participants also felt that current cyber risk levels were so high that they were now unreasonable to operate in. For example, Participant 13 created an analogy to explain this untenable position as, "*we live in a world where if you click on a link or open a PDF, you can destroy your enterprise and that's insane*. *That's literally like driving a car and at some random moment, if you use the indicator your car might explode*. *It's like, 'What?' There is no way that is reasonable*".

The findings throughout this theme demonstrated that NZ organisations operate in a high-risk environment. Relentless attacks and complex, fast-moving environments combine to create an ecosystem that drives burnout and limits effective cybersecurity planning and management.

5.2.2 Varied Cyber Maturity Levels

Cybersecurity maturity concerns cyber security position relative to risk environment and tolerances. The findings in this theme consistently describe varied but insufficient cybersecurity maturity levels in NZ to drive effective planning, preparation, and response in the current cyber risk environment. Governance mechanisms that drive mature cybersecurity practices, such as defined roles and responsibilities and structured risk assessment and management processes, were found to be fledgling, informal, inconsistently applied, or even absent in some NZ organisations.

NZ businesses use a variety of existing cyber security mechanisms in their organisations today, with many participants describing a "*layered security approach*" and using a "*comprehensive arsenal of tools*" to manage cyber threats. Typical tools included traditional and application firewalls, endpoint network detection and response, and anti-malware. As explained by Participant 18, "*we use a very layered security approach, from out in the demilitarised zone in terms of broader networks through to your traditional firewalls, and network protection, anti-malware, and others*".

Participants expressed hope that NZ organisations were preparing for the impact of quantum computing-enabled threats by engaging in forward contingency planning. For example, Participant 6 stated, "*I just hope that organisations are doing a lot of contingency and scenario planning*". However, more information and specific playbooks for identifying and responding to quantum computing-enabled threats are still

needed to assist organisations in this area, as participants were unclear on the possible scenarios, as evidenced by Participant 22, who questioned, "*you'd have to have a process in play to detect that type of thing, right. So what are you looking for when it comes to a quantum attack?*".

The findings indicated varied levels of organisational cybersecurity maturity in NZ. For example, Participant 16 described this variance as, "*I've worked with a lot of businesses and there is an enormous spread of maturity and capability from doing the best that we can through to utterly naive and probably borderline reckless*". Some NZ industries, such as banking, are reported as "*pretty well aware of their risks and deficiencies*", whereas others, such as the healthcare industry, are described as "*really really bad*" with "*really low maturity*" and likely exposing NZ to "*considerable systemic risk*".

Low maturity was also seen in our technology and cybersecurity industry. For example, Participant 16 described how they could not source cyber security services at a required level of maturity within NZ because, "*when you go to market and look for services, particularly managed security services, those services are often not the level of maturity or security in the New Zealand market that we want*".

Overall, NZ's cyber maturity levels were found to be low, with participants describing NZ as a "*pretty immature environment honestly*". Participant 3 highlighted this immaturity compared to other countries when describing how international IT professionals react when first coming to work in the NZ environment as, "*we have engineers who've come from overseas, and they'll bring with them the security best practice, but they'll be surprised at the areas New Zealand is behind in. We're a bit bottom of the Pacific here*".

A historical belief of NZ not being big enough or important enough to be a target for cyber-attacks led to the slow establishment of critical national cyber resources such as a computer emergency response team, which was one reason identified for the lack of maturity in our current environment. For example, Participant 1 commented, "*I think culturally, we just said, 'Well, we're not that important or that big'*". Additional reasons found to be driving NZ's low cyber security maturity were the absence of large global technology companies, as suggested by Participant 7, "*the reason New Zealand's behind is that we haven't had hyper scalers here, like Google, Azure and AWS*" and a perceived acceptance of mediocrity, as Participant 9 noted, "*it's low expectations, happiness with mediocrity...we find all of that okay in New Zealand*".

Low levels of cyber maturity significantly impact NZ organisations' ability and drive to prepare for emerging cyber threats. Participants often reported the maturity of an organisation as a deciding factor as to whether they would consider preparing for an emerging threat. For example, Participant 15 explained, "*I guess it would all come down to our maturity model. So if we're further along in the maturity model, then everyone is going to be open to start talking about how we are prepared against emerging threats*".

The findings also show that many NZ organisations are struggling to get the cybersecurity basics right, further emphasising low maturity. For example, Participant 16 stated, "*we are not very efficient in our practice of doing the basics*", and Participant 23 described how easy preventative actions are just not done because "*fundamentally, if you patch everything, you've shut off access, that's a great place to start. And you'd be surprised at how much we don't do that*". This inability to execute basic security hygiene was frustrating to many cybersecurity professionals, as expressed by Participant 15 as, "*there are some areas*

that they're just shocking. *And I'm like, 'Why are we struggling with, as you say, just basic security hygiene'*".

The inability to implement cybersecurity fundamentals has made many organisations find it hard, if not impossible, even to consider more future-focused threats, such as those posed by quantum computing. This difficulty was described by Participant 16 as "*getting very basic things to be consistently executed across the board or where they matter is really, really hard*. *So honestly thinking about quantum threats would feel like a science project in most real-world organisations*". Therefore, it was found that getting cybersecurity basics in place must happen before any NZ organisations will consider preparing for future cyber threats. For example, Participant 26 commented that, "*with limited resources, we kind of have to do the basics really well before we reach for the stuff that doesn't have a very easy answer*".

However, the level of support given to NZ organisations and cybersecurity practitioners within organisations was not currently good enough to implement cybersecurity fundamentals well. Participants expressed frustration at the lack of adequate support, such as funding, guidance, and regulation from the government when discussing a focus on getting the basics right, as expressed by Participant 19, "*to be fair, we don't get the support we should be getting from the government on that*" and at the insufficient support from within their organisations to implement robust basic security hygiene. For example, Participant 15 described the desire for a quick return on investment rather than a more sustainable approach to cybersecurity as "*waiting for years and being like, 'Oh, look*. *We slowly got better, and now we're doing really well, but it took 2 years to get here*". *No one wants that*. *We're doing it the quick and dirty way'*. This NZ culture of the "*number 8 wire*" was described by participants as being used in many fundamental cybersecurity areas, such as "*across governance and architecture, and across general hygiene*", emphasising the lack of support for getting the basics implemented sustainably.

Overall, participants expressed that NZ was falling behind other nations in cybersecurity maturity and that NZ, both at a national and organisational level, was not doing enough to prepare for the negative impacts of emerging cyber threats such as those posed by quantum computing. Participants expressed how, as a nation, "*we're not doing enough*" and how "*we need to get better*" or "*if we stay on the current path, we'll never be better than a victim*".

Participants believed that greater investment in cybersecurity was required to lift overall cybersecurity maturity in NZ. For example, as Participant 2 expressed, "*if we know that there's a big chunk of the market that are not doing okay, how do we move them up to a baseline standard that we want? You have to throw money at it*". To achieve greater resiliency*,* the focus of cybersecurity investment also needs to shift from an overreliance on funding tools to funding a more comprehensive range of contributing areas such as people and processes. Participant 15 explained *that* "*a lot of companies' approach is still very tool-based, and that doesn't work*. *No one wants to acknowledge that people are the key to security…they are willing to invest in just about any tool that you put up*. *But they're not willing to invest in years of engineering effort to actually get a tool to the point where it works properly*".

A fundamental aspect of cybersecurity maturity is cyber risk awareness. The findings show that general cyber security risk awareness varies between NZ organisations and that some industries "*need more work than others*". It was found that general cyber risk awareness has grown because of the media attention

given to recent large-scale cyber-attacks, as described by Participant 18, "*the general media is also very much on cybersecurity, and cyber threat plays at the moment*". However, overwhelmingly, participants did not believe that cyber awareness and understanding levels in NZ were good enough for the high-risk environment. For example, participants described cyber security awareness in NZ as "*particularly limited*" and "*not particularly great*". Participants also expressed that while effort was being put in to lift awareness, it was still not at sufficient levels, as described by Participant 12, "*a lot of our people are naive when it comes to computing…I think we've done a lot of work, but you wouldn't say there's a high level of sophistication around technical understanding of cyber*".

A "*lack of knowledge*" and "*awareness*" were specifically highlighted as reasons NZ organisations would be prevented from addressing general cyber threats, and this lack of awareness and understanding was also preventing the preparation for future quantum computing-enabled threats. When discussing preparation for these threats, participants highlighted that awareness must come first. For example, Participant 9 expressed that no preparation would happen with the current lack of understanding, stating, "*I think they're not going to prepare for it because they don't understand it*".

At the time of this study, the participants had extremely limited awareness of the threats that quantum computing may pose. When asked if they were aware of the potential threats, most participants replied negatively using phrases such as "*no*", "*haven't looked at it*", "*nothing*", "*very limited*", "*I don't really know anything about it*", "*no one's talking about it*", "*I know bugger all about quantum-enabled computing*". Some participants did express awareness of the potential for quantum computing to increase computational speed, leading to the "*ability to attack traditional cryptography*", an "*exponential improvement in DDoS*", and a potential "*cybersecurity apocalypse*". However, the participants who were somewhat aware of quantum computing-enabled cyber threats were also concerned that their knowledge was shallow. For example, Participant 16 described that, "*in true terms,* [my knowledge] *is very limited*. *I think to me quantum computing probably fits into a bucket of buzzwords like blockchain and AI that everyone might get very excited about and read an article about but really have no good sense of the practical implications of*", and Participant 6 stated that, "*I know only a little but enough to be worried*".

Only limited knowledge around mitigations for quantum computing-enabled threats was also found. Some participants were unaware that any mitigations existed, such as Participant 13, who stated, "*it's going to be a problem, but I'm not aware of anything that can be done in preparation for it*". Other participants were aware of the need to increase the bit length of existing algorithms but expressed challenges in achieving this. For example, Participant 15 explained, "*you really have to start increasing the bits that all those algorithms are using so that it takes a lot longer to break*. *But then you've also got to have the infrastructure to support that*". Other mitigation strategies posed by participants included "*airgapping*" and "*pulling back all data from network access*".

No participants were aware of any organisational activity planned or in progress to prepare for quantum computing threats. For example, when asked whether they had considered these threats or had anything on their roadmaps to prepare for them, Participant 17 explained, "*I'm aware of it, but I'm not taking proactive steps yet to do anything about it*" and Participant 21 stated, "*not that I'm aware of, no*".

Despite limited cyber threat awareness, participants expressed a positive and interested attitude towards quantum computing and its cyber security implications, describing the topic as "*interesting*", "*exciting*", and "*fascinating*". However, many participants also described how confused they were about quantum computing and how difficult it can be to understand. For example, Participant 21 stated that, "*quantum computing's massively confusing to me*. *I've had it explained maybe 10 times and I go, 'It can be a one and a zero at the same time'*. *No, I don't understand what that means…it's hard to understand*". This difficulty in understanding the area leads to challenges when discussing preparation for the threats that quantum computing may bring. Participant 20 described the perceived challenge of attempting to lift awareness by stating, "*it's impossible if you sit in front of a board or some directors to explain something so theoretical that you have a problem understanding it*".

All participants believed it critical that cyber security awareness is grown and that quantum-enabled cyber threats are understood. When discussing the need for quantum computing threat awareness, most participants believed "*you need to be having that conversation now*", and that awareness is crucial to success. As described by Participant 32, "*I think awareness is really the key*. *Knowing that this stuff is coming down the line and it is going to change the face of cybersecurity, and it does mean that we're going to have to improve our own security posture by using new tools and new features and new technology*".

When contemplating how greater awareness may be achieved, participants highlighted the need for government support to "*build awareness and frame the conversation*", in addition to widespread education and making the complex concepts involved in quantum computing more approachable. Using less technical language to describe the concepts of quantum and the resulting cyber threats was considered useful. For example, Participant 31 suggested framing quantum computing simply as a resource, and "*I try and talk of it as a resource*. *So it's a resource like any other resource*. *This just allows you to do, and you don't need to understand how*".

When describing board and senior-level cyber security threat awareness, most participants described this as too low, a challenge, and "*not where it needs to be*". For example, Participant 9 stated, "*we still have boards that don't understand technology*", and Participant 20 described how difficult this is citing, "*it's an ongoing struggle, they don't understand the risk*". There is a need for a focused effort to increase awareness at this level, as described by Participant 3 who believed, "*I think at director level there's still work to do…a lot of awareness work, and how risks translate into fiduciary responsibility for directors*".

Along with recognising the need for greater levels of understanding at senior organisational levels and "*better cybersecurity expertise from the top down*", there is a particular need for awareness that cybersecurity is a constant journey rather than a one-off risk that will be solved with a point solution. For example, Participant 5 described this need as, "*I think boards… they really need to get it into their heads that this is an ongoing thing that needs to be managed and monitored forever…It's just not going to go away*".

Steps to improve board-level awareness and understanding were not seen as a priority in NZ, which is "*discouraging*" for cybersecurity professionals and negatively impacted cybersecurity posture. For example, when discussing how to improve general cyber maturity within NZ organisations, Participant 6 stated, "*I think if I was on a board and I'd be really studying up and getting some coaching and getting*

some advice at the moment, I don't know that a lot of them are". The negative result of this low understanding was described by Participant 5 when explaining a typical response to raising cybersecurity issues with the board, with a typical response being, "*cyber security, that's an IT problem. That's not going to affect our business. Why is it at the board level? I don't care. Move along, move along*".

Where organisations have successfully lifted board-level awareness, several participants credited the New Zealand Institute of Directors, which issued a framework around board responsibilities in cybersecurity. Participant 5 discussed the impact this framework had on awareness levels as, "*Institute of Directors came out here in New Zealand and made a statement that cyber is the responsibility of the board and the boards need to pay attention. I think that's created a much greater awareness, specifically at that board level, around their responsibilities, some of the risks*".

Participants who reported experiencing greater organisational levels of cyber maturity and awareness cited "*annual security awareness training*", "*huge investment*", "*formal induction*", "*transparent risk management*", and making cybersecurity part of the organisation's "*vision*" as key to having a positive and cybersecurity aware culture.

5.2.2.1 Subtheme – Insufficient cybersecurity governance mechanisms

Study participants expressed a range of issues, such as a lack of clear responsibility and accountability for cyber security, unclear reporting mechanisms, and difficulty in risk assessment and risk management practices that added to an environment of insufficient cybersecurity governance.

When discussing where the responsibility for cybersecurity lies, all participants agreed that it is everyone's responsibility and that everyone has a "*role to play*", as stated by Participant 11, "*you can't have just one team responsible for security. Everybody has the responsibility*". However, when discussing assigning accountability for security breaches, little clarity was found in the current landscape. Participants expressed this lack of clarity around who should be held accountable after a cyber-attack when, "*you see a debate in breached companies, were they the victim of a crime and do we blame the attacker, or do we blame the company for poor defence? Perennial debate*" (Participant 16).

Many participants believed that cyber-attack victims should not be blamed and instead wanted to assign this blame to the cyber criminals. For example, Participant 1 stated, "*just because you've been breached doesn't mean that you're to blame*", and Participant 13 stated, "*it's the criminal's fault*". However, a blame culture still exists in the NZ cyber-attack landscape, as described by Participant 13, "*there's a real mob mentality, baying for blood*".

This unclear or ill-defined responsibility and accountability for cyber security in NZ organisations contributes to cyber incidents. Participant 2 described an example of this as, "*who's responsible? That was the exact problem that led to the cyber incident in the first place…the responsibility and the lines of accountability around cybersecurity were very unclear, extremely ambiguous*".

The findings determine that software vendors, organisations, and directors could all be held to greater account for insufficient cybersecurity that contributes to or results in cyber incidents. Currently, technology vendors are not held overly accountable for product vulnerabilities, and some participants believed this leads to shifting inappropriate security risks onto organisations. Participant 13 explained the impact of low

vendor accountability, "*so we have no software liability*. *The big software houses churning out software, the Microsofts and the Googles and the Apples, they're not held to account for the quality of their software*. *And so, we're now spending billions of dollars and being stolen billions of dollars by criminals because we're constantly fighting this rear-guard action trying to protect this shambling mess that is an enterprise IT environment… there was no other software that you could buy, but now, it's your responsibility to secure it*".

Participants also agreed that organisations must be held more accountable than they are today for protecting themselves and sustaining a basic level of security hygiene. For example, when discussing the aftermath of cyber incidents, Participant 19 commented, "*if it's due to really, really poor cyber hygiene in the sense that really duty of care was not there, then surely there must be some form of consequence? It feels like there really isn't*".

Finally, increasing the accountability held by NZ company directors for cybersecurity was also suggested as necessary to improve the cyber maturity landscape positively. One reported way of achieving this was to introduce personal liability. Participant 26 confirmed that some participants were open to implementing greater director liability in NZ to drive accountability and stated, "*probably the strongest thing that they can do is just to create director's liability*". However, some participants expressed concerns about instigating directors' liability, noting that the cybersecurity environment is so complex and nuanced that it is hard to hold any individual accountable. Participant 2 describes these concerns as, "*in terms of a directorship and a governance perspective, is it reasonable to expect a board director to really understand the security position in detail of their company such that they can be accountable for it?*".

Participants showed a lack of ownership when discussing the preparation for quantum computing-enabled cyber threats. For example, Participant 23 described not feeling responsible for this, stating, "*we wouldn't worry about quantum computing simply because it's everybody's problem*". This lack of accountability and subsequent action was reflected in the participants' hope that someone else was preparing for the potential threats. Participant 19 expressed this hope as being "*like climate change*. *We'll all be suffering at the same time, so maybe someone else is thinking about it*".

Participants believed that NZ organisations were looking to the government to take ownership and lead the preparation for emerging cyber threats. For example, Participant 4 explained that, "*quantum needs to be dealt with at a government level because that's likely to be their attack vector*", and Participant 25 agreed, stating, "*we've got the GCSB*. *So we have an organisation tasked with worrying about that and doing that sort of stuff*". Additionally, some participants felt that if cybersecurity and cyberthreat protection were important, then the government would mandate them. For example, Participant 16 stated, "*I think there is a mood, maybe in the boardroom but definitely in the C-suite, that if this was really important, the government would make us do it*".

Another aspect of cyber governance that the findings indicate could be improved across NZ organisations is the processes of cyber risk assessment and management. Participants reported the formal assessment of the threat landscape as "*very haphazard*".

The findings highlight how risk appetite influences decisions about whether, when, and how organisations will prepare for cyber threats. Participant 6 discussed this concept when talking about organisational

preparation, saying, "*well, it'll come down to risk appetite...some may be, 'Hey look, this is all about getting out to market we're going to take that risk'. Other organisations, typically banks and insurers are going to be a lot more conservative*". Additionally, whether to adopt new technology that may be required to protect against emerging cyber threats is also influenced by risk appetite. Participants described NZ organisations as having a conservative approach to adopting cutting-edge technology as described by Participant 19, "*there's a reluctance to be the first kid off the block with some of this emerging stuff. So even if there was someone touting a quantum silver bullet, everybody would sit back and wait*", suggesting NZ may fall behind in embracing protective quantum technology.

NZ organisations typically use traditional risk logs and simple measures of likelihood and impact to assess cyber risks and plan mitigation measures. For example, Participant 18 described the standard process undertaken by most participants, "*a lot of organisations have traditional risk logs…and then undertake the normal risk assessment process in terms of impact and likelihood*". However, there was also a level of discomfort around the accuracy or completeness of current methods to assess risk, as described by Participant 19, "*the problem I'm uncomfortable about is that we haven't got a quantitative risk view*".

Many participants expressed how cyber risk assessment was more "*an art than a science*", frequently referring to relying on "*gut feel knowledge*". However, it was also found that using formal frameworks and complying with industry regulations were drivers for more "*structured*" and thorough risk management processes, which led to greater maturity. For example, Participant 6 described this situation in the financial services industry, stating, "*there's a lot of regulation that has driven a lot of investment back into risk management and compliance in the industry. A lot of that has been useful in maturing processes for identifying and categorising and monitoring both risks and controls and accountability*".

Many participants described adopting frameworks as part of their formal risk management processes, with the NIST CSF being the most cited, followed by the CIS controls and ISO standards. Participant 1 explained that, "*most organisations are adopting an industry or government-sponsored security framework. For instance, we use the NIST cybersecurity framework to provide guidance for designing security controls*". The participants found cybersecurity frameworks helpful in several ways for cybersecurity governance, mainly to "*take the emotion and panic out of and show traceability to investment decisions*" and indicated that using these frameworks helped with cyber threat preparation. For example, Participant 24 described that, "*if you're working to a good framework that's got continually updated and good standards, then you've got that level of preparedness coming through those processes*".

However, the findings concur with the literature review in that current cybersecurity frameworks have limitations and are not the complete answer to governing or improving organisational cybersecurity. Participants reported struggling with the high-level nature of the guidance given in frameworks, as highlighted by Participant 2, "*so the…framework, It's very general. It's quite high-level. You wouldn't read that document and come away with a clear plan around how you were going to implement it in your organisation*". Participants also highlighted the lack of context-specific information in the frameworks and the difficulty in determining implementation scope as challenges for their use. For example, Participant 19 stated, "*the problem, it's really about scope. Also, there's no context to those things. So if you're* [specific industry business]*, where do you need to be on all those different levels? So it doesn't really help. It gives you an interpretation of your capability that's full of holes*". Ultimately, some participants doubted the true

value of frameworks to make real changes, as described by Participant 2, "*those things are good box-ticking exercises. I'm not really convinced what practical impact they have on the ground*".

Despite not being enough on their own, frameworks are crucial to driving preparation for emerging cyber threats such as those posed by quantum computing. For example, Participant 3 described how they would not ignore preparation guidance if it were explicit within these frameworks, "*yep, if it's on their checklist. And I'm being told that that checklist is the Bible. I wouldn't ignore that item. I would not ignore that item*".

Other aspects of governance found insufficient in NZ organisations today were the level of cybersecurity representation at the board level and the influence cyber security professionals have within NZ organisations.

Participants expressed significant concern about the lack of cybersecurity professionals at the board level in NZ. For example, Participant 9 discussed the typical board makeup in NZ as follows, "*most boards in New Zealand companies are made up of lawyers, accountants, and ex-politicians. And quite frankly, that is not a really good combination when you are in a highly technology-dependent economy*". Participant 16 continued discussing this concern and highlighted a belief that this situation is not improving as, "*there's a lot of people who speculated that boards would look for cybersecurity skills. As a director, the strong feedback I get is no they don't, they're still seeing it as very transactional risk*".

In addition to being underrepresented at the board level, many participants expressed that cybersecurity resources within NZ do not have adequate influence within the organisations they work for to influence positive change. For example, Participant 16 stated that, "*large organisations tend to have their own security teams often a bit underpowered and not as influential in the organisation as they should be. So they tend to have people who know what needs to happen. But those people are often not being listened to by the organisation*". Participant 26 highlighted this lack of influence at the lower levels of an organisation, explaining how it limits necessary threat analysis and preparation activities in stating, "*I mean in a very practical sense, say, I'm a senior developer, and I think that, quantum could present a risk to our product. I have very little power or authority to actually go off and start thinking about that*". Participant 16, however, highlighted how the difficulty in getting a message across and influencing change also extends to the top of most organisations, with structural change needed to ensure cybersecurity concerns can be heard, "*I've a view that there needs to be much deeper engagement between someone on the board and the CISO outside of the meetings because it's very hard as a CISO to land a message to the board because generally speaking, you're not senior enough to have visibility of the whole board proceedings*".

5.2.3 Applying a Strategic Lens

The potential cyber threats posed by quantum computing are seen as a risk to NZ society; however, the uncertain but potentially long-term timescales involved both to prepare for these threats and to see the impact of these threats mean they may require a level of strategic cyber risk planning not currently found in the NZ landscape. The findings in this theme demonstrate the necessity of longer-term thinking in this area and the challenges currently preventing it.

Participants considered the future threats that quantum computing may pose as "*high-risk*" with "*huge implications*" for NZ; however, they did not understand the boundaries of these risks. For example, Participant 22 described, "*it's just a question of how far does this go? I already can't get my head around*

that. *No one really knows at this point*". Despite not fully understanding the potential risks, most participants agreed that NZ should be planning and preparing for these threats today. Participant 5 described this need to start preparation as, "*I think we need to be thinking about it earlier rather than later simply because if we don't, we will be caught out*. *It's the economic manipulations that I'm particularly concerned about*. *I think we just can't underestimate that*". Participant 10 agreed with the need for early planning and preparation despite the still theoretical nature of the threats, stating, "*I think the theoreticals are closer than most people might realise*. *So I do think we need to be talking about things*".

While most participants agreed on the need for early planning and preparation, they also reported several contradictory beliefs and behaviours that prevent NZ organisations from strategically managing cyber risks and preparing for these early.

The first reported belief was that the cyber threats posed by quantum computing were "*not imminent enough*" to act on or prepare for. Participants highlighted that their entire focus was only on immediate and near-term cyber threats. For example, when discussing quantum computing-enabled threats, Participant 11 reported, "*right now, on a radar, it's on the very edge; I've got other threats that are far closer to what I need to protect*. *I'm not worried about the stuff on the edge right now*. *I need to deal with what's here and now*". Participant 23 agreed, confirming, "*the only threats I'm looking to are the threats that live in the existing paradigm*". This belief that quantum-enabled threats were not imminent enough to act on directly contradicts the earlier reported belief of the participants and in the literature that early planning and preparation for these threats is needed.

Overwhelmingly, participants described a landscape dominated by reactive responses to emerging cyber threats, with "*someone already feeling the pain*" or "*companies being hacked*" quoted as the main reasons to initiate any cybersecurity planning or protection measures. Participants confirmed that most NZ organisations will only start planning and preparing for potential quantum computing-enabled cyber threats once they have seen or felt their impact. For example, when discussing what would drive preparation for these threats, Participant 21 reported, "*if we saw it happen…once that happens, we'll get a fright, and then have to have some crisis talks about what we're going to do*".

Another behaviour preventing early planning and preparation for future cyber threats are the current cyber risk planning horizons used by NZ organisations. All participants described their current cyber risk plans as near to medium term only, with most participants reporting plans that "*go out to about 18 months*" and some reporting plans that look to a horizon of "*2 years, 3 years tops*".

NZ businesses are not extending cyber risk planning beyond 18–36-month timescales for various reasons, including how the planning is "*tied to the funding process*" and the uncertain nature of changing technology. Participant 19 described a belief that planning beyond the near term is too difficult, stating, "*anything more than 18 months is just a bet, really just guesswork*". Some participants also expressed concern that a lack of investment drives this reactive and short-term outlook to cyber risk planning. For example, Participant 10 expressed, "*business is never willing to invest in enough resourcing to actually start looking a few steps into the future*. *It's always a case of a response game or just trying to stay on top of the current issues*. *And that seems to be very widespread*".

The currently reported cyber risk planning timeframes may not allow NZ organisations to effectively prepare for the known cryptographic threats that quantum computing will pose. When asked to estimate how long a complex organisation may need to transition their existing cryptographic algorithms to quantum-safe alternatives fully, most participants could not answer. Participants who answered predicted transition timeframes ranging from a minimum of 3 years and reaching up to "*about 8 years*".

The findings show that fully understanding, quantifying, and communicating cyber risks that are theoretical in nature, such as those posed by quantum computing, is hard. Participants agreed that this difficulty is another factor that prevents more strategic cyber risk preparation in NZ.

Participants expressed a strong reluctance to raise theoretical threats that are "*somewhat ambiguous*" to boards due to a lack of definitive answers around the risk impact, cost, and solution. Participant 12 described this reluctance as follows, "*it's not a threat you'd want to put in front of a board without a, so what are you going to do about it, answer?*" and Participant 19 concurred, expressing "*putting quantum on the table…you can't really spend political capital on it. It's very difficult for people to think about what it would mean for* [our business]*, our government and for the country*". Participants highlighted how difficult it is to justify spending on cyber threat preparation and mitigation when the exact cost of the impacts cannot be quantified. For example, Participant 19 stated, "w*e can't say there's this quantum threat that's coming and if it happens, it's going to cost this much. Therefore, if we spend this much to mitigate the threat, that is something everyone will approve of*".

Another concern expressed by multiple participants was the possibility of raising a theoretical threat at the board level only for it to never happen. Participant 12 described this fear, saying, "*the risk for me personally would be I go and say cry wolf here and there. Spend all this money and it never happens, I'd lose all credibility*". These findings suggest a lack of support for cybersecurity professionals when discussing uncertain or ill-defined problems, thereby limiting the ability for early cyber threat contingency planning.

All participants believed the current highly reactive method of responding to cyber threats "*isn't sustainable*" and that applying a more strategic lens to cyber risk planning would be beneficial. Participant 13 expressed how NZ is currently failing in this space, stating, "*failing to plan is planning to fail. So yeah, it feels very much like we are planning to fail*", and Participant 3 expressed a common participant desire for greater forward-thinking in this area, as "*I think there is space, and in an ideal world, we'd be doing lots more thinking ahead of the curve about these sorts of things*".

Some participants felt that applying a strategic lens to these issues was the NZ Government's responsibility, urging our government to "*work on it now*". Participant 26 summed up this expectation of the government by stating, "*in the public sector, there is an expectation that government should be doing that mitigating risk prevention role and thinking into the future and doing the things that individual players can't do because they've got the size and scale and power. In a private business, you have commercial concerns. You can't just have some person sitting there thinking about stuff without creating value*". However, it was felt that NZ lacks a strong transparent vision and clear recommendations for addressing cyber threats. Participants believed that the government was not "*proactive*" in outlining "*good practice*" and "*minimum standards*" in cybersecurity in general, and in particular, noted the lack of forward-thinking

guidance for NZ future landscape. For example, Participant 3 described that, "*it does feel a lot of the time like it's catch up…what's the vision that we have nationally?*".

Participants also felt the NZ Government should be strategically thinking about the ethical concerns that may arise with emerging technology and plan legal frameworks to deal with future cyber threats should they arise. For example, when discussing quantum computing, Participant 11 emphasised that NZ should already be thinking about and planning for any issues, stating, "*we should be already thinking about regulations and how we ensure that it is used in an ethical manner*". While acknowledging the uncertainty around these future issues, participants still felt that planning could occur nationally. For example, when discussing potential regulation, Participant 15 expressed a desire for it to occur along with doubt that it would, "*even if there was preparation work, and it wasn't necessarily enshrined in law, that would be an adequate response*. *But it just seems like they take forever to even realise it's an issue and then actually start acting on it*".

In addressing the lack of strategic cyber risk planning, multiple participants compared the future cyber threats of emerging quantum technology to other global challenges requiring strategic planning and widespread action, such as the threat of a "*solar flare*" and climate change. Participants considered quantum cyber threats similar to climate change threats in various ways, including the complexity and "*difficulty in understanding*" the threat, the scale of the threat, the lack of immediate tangible impacts for most individuals, and the lack of clear responsibility lines for responding to the threat. For example, Participant 19 compared the difficulty in understanding climate change to quantum cyberthreats stating, "*like the climate change example*. *It's very difficult for people to think about what it would mean for* [our business] *in the context of what it would mean for our government and what it would mean for the country*".

It is clear from the findings that applying a more strategic lens to cyber risk would benefit NZ and drive greater cyber threat preparation; however, participants were uncertain and largely pessimistic about the likelihood of this area improving. When discussing strategic NZ Government initiatives, Participant 28 noted that, "*there are some ongoing discussions about how to create better long-term planning and midterm planning just basically beyond the next election cycle and how to create incentives that move people beyond that*. *But none of it really has gone anywhere and I don't see any of it being super impactful or realistic, to be honest*".

5.2.4 Importance of Trusted Relationships

The findings in this theme describe how people and the strength of the relationships formed between people are fundamental to protecting NZ from the harmful impacts of emerging technology. This includes the potential harmful impacts from future cyber threats that quantum computing may pose, as whilst technology changes, the need for people to work together to ensure technology remains beneficial does not. Participants emphasised how "*people are the key to security*" and how investing and building trusted relationships between people will be vital for NZ's cybersecurity success.

Cybersecurity is only effective when everyone ("*private sector, government, academic sector, everybody*") works together and acts with "*mutual responsibility*" to prevent any undue harm that may arise from emerging technology. Participants strongly emphasised how ultimately "*we're all trying to solve the same problems*" and described how the interconnectedness of industries and supply chains means that security

must be a "*team sport*", as evidenced by Participant 13 in stating, "*it doesn't work for us if one of the other banks gets hit and we are okay because that undermines consumer confidence in the entire sector*".

Participants also believed the cybersecurity challenges quantum computing poses will require a coordinated effort to overcome. For example, Participant 30 stated, "*where new technologies can threaten institutions or fracture society in new ways, then it's a problem, and it needs to be addressed by everybody, by citizens, by governments, by business*", highlighting the need for all parts of society to work together. Participant 32 took this sentiment further, explaining how we may all struggle to address the challenges of future cyber threats if any one area of society does not adequately contribute, stating, "*in terms of quantum computing, if everyone plays their role then we might be in a good position, but it's going to be a joint effort*. *If it falls over somewhere, then it might be tricky*". There is doubt over whether true collaboration and working together will occur between all groups, particularly between private and public entities, and some participants suggested the notion is unlikely or "*pie in the sky*". For example, Participant 11 expressed their experiences in this area, stating, "*what actually happens is that the vendors and the private sector work together*. *Then we advise the government*".

Significant value is placed on open information sharing for cyber security professionals attempting to prepare for and combat cyber threats in NZ. Participants expressed how open information sharing in the industry is "*extremely helpful*" and how opportunities such as "*round tables*" where information can be exchanged freely are "*very, very useful*". Participant 11 described the value of sharing and learning from peers as, "*learning from peers who are not competing is very valuable for me, extremely helpful*. *Hopefully, they could learn from me too*. *I think many other people in security positions would feel the same as well*".

However, this study found that the NZ cybersecurity industry is currently characterised by a lack of transparent discussion and open information sharing. Participants described how "*there's a lot of stuff kept under the radar*" and how sharing is not open enough. One area where participants felt a significant lack of openness was in sharing the learnings from cybersecurity incidents. For example, Participant 3 described, "*in New Zealand, we're not particularly exposed to retros and debriefs on security events*".

The findings revealed a culture of secrecy and "*reluctance*" to divulge information. For example, Participant 4 stated, "*everyone's very scared to, and scared would be the word, to divulge any weakness*", and Participant 22 concurred with, "*people I know at my and the CIO type level tend to not talk about what's going on for them from a security perspective, because that opens the conversation about potential threats*. *So yeah, it is a bit closed-minded and it's not very open*".

There is also a lack of formal opportunities to share and collaborate around cybersecurity in NZ, with most information and opportunities to collaborate being "*ad hoc*" and disseminated through "*informal networks*" and by "*word of mouth*" only. Participants expressed a desire for this situation to change, as proposed by Participant 22, who explained, "*I think there's an opportunity to find a common forum for which those types of things can be discussed at a confidential level, but it doesn't really sort of happen which is unfortunate*".

The findings show a need for timelier, trusted cyber threat intelligence and advisory in NZ. Participants described the information as critical to preparing for emerging cyber threats such as those that quantum computing may pose. For example, Participant 14 described, "*the emerging stuff that hasn't hit us yet, we want to hear what we can put up proactively or what alerts we can turn on and what's happened with other*

people”, and Participant 20 concurred, stating, “*what we need is information so that we can take that and act*”. Participants described using various sources of current cyber threat intelligence; however, a very strong preference was demonstrated for peer-to-peer discussion, as described by Participant 21, “*I prefer discussion around threat intel rather than a push post because there’s so many of them and anyone can read those and become alarmed*”.

Peer networks were currently the most trusted channel for receiving quality threat information in NZ today, with participants citing them as “*immediate, local, relevant*”, and “*strong*”. However, due to the ad hoc nature of these networks and the lack of trust in the NZ landscape, not all cybersecurity professionals can access them. For example, Participant 23 described the networks as “*very sub rosa*” and operating as a “*circle of trust*”. Participant 4 described the difficulty in making connections when new to the industry as, “*you’ve got the people you know and trust and there’s a free sharing kind of aspect and then you’ve got other people who you don’t know, you blank them*”, and Participant 5 highlighted the difficulty in building trust and how long it takes stating, “*there’s knowledgeable people but it takes time to build those relationships, they’re not just going to trust anybody*”. The time it takes to build trust is also a factor in trusting government sources of cyber guidance, as expressed by Participant 21 when they asked, “*are you going to trust a security agency that changes every 4 years? Probably not*”.

Trusted collaboration and information sharing were also found to be limited by both the commercial and competitive aspects of the NZ cybersecurity industry. Participants acknowledged that information coming from a vendor is often “*biased*” and “*motivated by profit*” and expressed their frustration over the commercial aspects of security. Participant 4 stated, “*the problem is it’s still a very commercial area*. *Security is the one area where the commercial aspect actually needs to go away*”. Competition also hindered collaboration and information sharing, as described by Participant 11, “*when there’s a competitor in the room, I’m going to be keeping my mouth shut*”.

The overall lack of trust and open information sharing described in the findings hinders cybersecurity collaboration and effectiveness in NZ. For example, Participant 13 described, “*my impression is that there’s a little huddle of people, little spokes, and they’re fiercely, fiercely protecting this information, and it’s coming at great expense to New Zealand being able to actually operate as a community*”. Therefore, building and maintaining trusted relationships is vital for collaboration within the cybersecurity industry and ensuring effective preparation to combat emerging cyber threats in NZ. Participants identified the need for a cultural shift to increase openness, citing ideas such as “*leadership with vulnerability – Brené Brown style*”, “*repeated gatherings*”, and “*public, private forums*” as tools to enhance this space.

5.2.5 Developing National Capacity

This theme describes various parts of national cyber capacity that are insufficient to meet the challenges of future cyber threats. It finds that NZ requires new and improved skills, infrastructure, and regulatory support systems to thrive in a quantum computing-enabled world.

5.2.5.1 Cybersecurity and quantum technology skills and capacity

Overall, the findings show a shortage of cybersecurity skills in the NZ workforce to combat the current cyber threats, and a “*dramatic upskilling of the workforce*” is required for future success. Participant 23 described this lack of workforce skill as a material risk to their business stating, “*my biggest risk around*

cyber security is having the people…That's a material risk on the security side". Additionally, NZ has very few skilled individuals in the area of quantum computing and cybersecurity. As Participant 27 acknowledged, "*there's hardly anyone in New Zealand that knows much about it at the technical level*".

Most participants felt that quantum computing-enabled cyber threat issues must be addressed at the NZ Government level. Participants felt the government has a role to play in setting quantum computing "*safety standards*" and protecting "*public safety*", "*state secrets*", and "*government interests*" against quantum computing threats. Participants also felt the government should take "*a lot of interest*" in ensuring that any required changes to underlying system algorithms in crucial industries such as finance and banking are well managed. Participant 12 described their expectations around communication from the government on future quantum-enabled cyber threats as, "*I would expect that the government would be engaging with the key participants around the potential impact to their business and what that would mean*".

Although there was an expectation of government "*leadership*" around quantum computing-enabled threats, the NZ Government does not appear to have the requisite skills or capacity to effectively address the current or future cyber threat landscape.

At a national level, NZ has some agencies, such as the GCSB and NCSC, to address cybersecurity; however, the findings show these agencies do not have sufficient skills to support NZ businesses when preparing for or responding to cyber threats. For example, Participant 17 explained their experiences with one of these agencies, "*NCSC. Yeah. Yeah…they would come in and meet with us, and we had a login into their portal…But again, we were a bit underwhelmed with the level of expertise...I mean, we knew more than they did about anything*". Participant 9 concurred stating, "*they don't have the skills, yeah, I just don't think I have seen good leadership come out of the New Zealand Government*".

Most participants felt that NZ Government agencies were under-resourced to assist NZ businesses with cyber threats effectively. Participant 17 described, "*you've got these organisations who are there to help, but they don't have the right people or not enough of them to know what to do…they've got to actually do something. And in my experience, that didn't happen*". This under-resourcing of government cybersecurity agencies means they were unable to assist NZ businesses in a timely fashion. Most participants described government support as "*always behind*" and "*slow*". For example, Participant 5 described an experience representative of most participants in stating, "*NCSC under the traffic light protocol would share certain information. But the problem is by the time that somebody would pass along information, it was so out of date and so late that it was of no use to me whatsoever*".

Participants also felt that NZ Government agencies were "*not really empowered*" or given sufficient mandate to address current or emerging cyber threats that may impact NZ. For example, Participant 19 reflected on current government support for critical infrastructure organisations as follows, "*I've tried to work out what the government support is for a critical national infrastructure company like ourselves. You've got an organisation which is predominantly focused on eavesdropping and intelligence gathering, who's also being given the task of defending the company from cyber threats. And they'll put some people on it, but really they're about intelligence…Protecting enterprises, even if they're critical to the nation...it's kind of a best efforts, but under-resourced and not really empowered thing*".

Participants believed there is "*space for an agency or ministry*" that can be responsible for emerging digital issues, highlighting the "*extremely limited*" capacity within official government structures today. The lack of a core and consolidated government technology assessment function to form "*long-term views on technology*" and to "*prepare people and prepare briefs for policymakers and politicians*" was identified as a significant challenge when discussing NZ's preparation for quantum-computing enabled cyber threats. The disparate and limited nature of technology horizon scanning was described by Participant 26, who explained, "*there probably is someone in some government agency somewhere who has some oversight of the quantum, but to my understanding, it's very limited. It is quite fragmented and individual agencies are doing their own thing and not consolidating or sharing that effort*".

The findings also show that NZ must grow its level of skill and understanding in quantum computing and the cybersecurity concerns it may present to ensure the country can engage nationally and internationally in useful dialogue to maximise the positive outcomes of this technology for NZ. Participant 14 described, "*my thinking would be that we have to develop by building the skills and the understanding of that technology so that we can have meaningful conversations at the right levels, with the people that matter, around quantum computing*". However, the NZ Government currently does not have the requisite skill level to discuss the issues that emerging technology may present. For example, Participant 28 explained this limitation as, "*a lot of the people in the public sector don't have a vocab to be able to talk about this issue. And they're not up-to-date*", and Participant 26 confirmed this, stating, "*we have a pretty weak depth of roster in terms of technology and ethics in New Zealand*".

There is a need to increase skills in quantum computing, cybersecurity, and ethics throughout the NZ workforce and public sector agencies. Participants emphasised the need to maintain people who understand quantum computing and "*what these technologies mean for us*". Participants desired "*more digital security professionals*", "*more ethicists*", and ideally, "*a pipeline for generating these skilled people*". Along with employing "*more technologists*" in the public sector, some participants felt there would be "*huge economic and societal benefits*" from having a good chief information officer in government who was mandated to think strategically in the cyber security and emerging technology space.

5.2.5.2 Education and research

The findings highlighted that improving NZ's technology and science education pathways was necessary to increase workforce skill levels and ensure NZ is not left behind in understanding quantum technology and cybersecurity. Participants acknowledged education as "*incredibly important*" and expressed a need to ensure the next generation is educated to ensure "*security's baked into people's skillset*". For example, Participant 2 suggested that, "*the new generation in 20 years will have to be living and breathing this stuff and will hopefully have an understanding of security and privacy that my generation is currently still struggling with…we need to go right back, build a baseline capability in society at large*".

NZ's current investment levels in educating our technology and science communities in emerging technology (including quantum computing) were considered insufficient. Participant 9 described that, "*one big problem is in New Zealand, we don't educate technologists and when we attempt to, I don't think we do so well. As a result, when it comes to more advanced problems…quantum encryption…we just have to take what is available overseas*". Not increasing this investment or strengthening the technology and science education and skills pathways will be detrimental to NZ's future economy. For example, when

discussing the outcomes of accepting the status quo in education, Participant 9 predicted a negative result, "*the effect on New Zealand businesses will be that increasingly, for higher levels of technology, we will be paying license fees to our technological overlords*".

Participants identified a need for more formal technology education starting early in "*high school*" and continuing with strong tertiary-level programmes. Participant 10 explained, "*change the education model. Focusing back on quality in education, you can have a strong, technically focused university, something really world-class*", and Participant 21 concurred, "*we have brain power, we have clever people who should be directed to learn about this stuff. Let's find those great minds, let's start them early*".

5.2.5.3 Insufficient legislation

The findings indicate that NZ requires greater regulation and mandates to drive the cybersecurity preparation required to combat future cyber threats, such as those that quantum computing may bring. The current level of legislation relating to technology and cybersecurity and the penalties associated with this legislation in NZ are seen as "*very light touch, almost not worth even bothering with*", suggesting it does not act as a motivation to improve cybersecurity protection today. For example, Participant 16 expressed, "*I think we're late to the party with all our regulation and then we're very light-handed with it*".

As well as indicating there is "*obviously not enough*" regulatory guidance in cybersecurity, privacy, and technology, some participants expressed disappointment in the strength of current legislation and the minimal punitive penalties associated. For example, Participant 2 described that, "*when that Privacy Act came out, I really just felt so disappointed on a whole number of levels. It was a real missed opportunity. Nothing at all about algorithmic fairness…all those things which are in the GDPR from years ago, completely absent. The penalties are pathetic*". Other participants also expressed a wish for increased penalties, such as Participant 26, who stated, "*we can definitely push up the penalties*", and some participants indicated a desire to see potentially more serious forms of consequence in place beyond the monetary or reporting ones currently used. For example, Participant 21 suggested, "*I think there needs to be something so that when you deploy or come up with something new, you are forced to think about the important issues, or you're going to jail*".

Overwhelmingly, study participants supported the need to introduce more "*sensible*" and "*pragmatic*" regulation in the areas of technology and cybersecurity to protect privacy, prevent undue harm, and drive preparation for quantum computing-enabled threats. Participants saw the benefit of legislation acknowledging its purpose "*to turn the risk equation*" and its ability to influence organisational behaviour.

Introducing mandates to transition to quantum-safe solutions was also widely supported. Some participants felt these mandates should apply to critical infrastructure only, such as Participant 28, who stated, "*anything connected to our critical infrastructure, I would be broadly supportive of a mandate that you have to have that secured under a quantum-resistant algorithm, let's say by 2032*". Other participants felt the mandates could be all-encompassing if they were "*logical and sensible*" and that a process of "*consultation*" was undertaken before introduction. For example, Participant 12 described, "*making this a mandate to require people to transition would be my expectation. It shouldn't be opt-in, it should be, you have to do this*".

Mandating other aspects of the quantum-computing technology landscape to prevent harm, such as how the technology is used, was considered more complex. Many participants felt regulating the use would be

beneficial and supported this idea, such as Participant 32, who stated, "*I think there would be a period of time where some kind of regulations around the use of the technology could be beneficial in terms of allowing everyone to catch up with their own security, to put themselves in a good position where they're going to stay safe against that quantum-enabled driven kind of attacks*". However, some participants also felt the practical aspects of regulating the use of quantum computing technology would be too hard. For example, Participant 31 described, "*I think it will be hard to regulate*. *Those big commercial players that are going to develop and to a certain extent, monopolise these resources*. *And they're going to want to sell it*".

Another area where participants raised possible beneficial outcomes of further legislative or regulatory control in NZ was when discussing introducing legislation to "*certify products*". For example, Participant 13 described a potential certification regime such as those in place in other industries internationally, "*you don't get to sell that in this market unless it meets our requirements and putting out a roadmap saying,* "*that's going to be acceptable this year, it'll be a little bit acceptable next year, and it won't be at all acceptable in 2 years' time so start planning your roadmaps accordingly*".

Introducing regulation around technology products to prevent harm is seen as challenging due to the large size of companies that dominate the market and the relatively small size of the NZ consumer market. For example, Participant 26 described, "*there's been this overarching narrative in New Zealand that we're a small country*. *We have a small number of users; we can't push too much against these big players because otherwise, they'll just leave our markets, and we will lose their products*". However, study participants wanted this situation to change, as expressed by Participant 2, "*I think it's quite clear that the current approach is not working…and that we really have to stick our necks out and say,* '*We've got to do something"*".

There are challenges to overcome when implementing further regulation in NZ, including the speed at which it can occur, the overhead of compliance, and gaining the support of those who do not believe a regulatory approach is ideal. Participant 16 cautioned, "*I think my recipe would be unfortunately regulation but be careful what we wish for because regulation won't be perfect, it'll be ham-fisted*".

Participants indicated that regulatory measures cannot be solely relied upon when planning to prepare for emerging cyber threats due to the slow speed at which they are developed. For example, Participant 20 described the lag in implementing suitable legislation for protecting against technology threats, "*the government seem to be about 5 years behind*. *Things happen, then they will then put in the legislation to protect companies*". Participants also described how regulation may need to be risk-based to avoid unnecessarily overburdening some organisations as described by Participant 1, "*I guess the downside is that it would be quite a burden on certain companies and certain sectors to become compliant*". Additionally, concerns were raised about the cost of verifying compliance to regulatory measures as described by Participant 2, "*that could get really red tape-y and bureaucratic in terms of how we verify somebody meets those standards*. *But I really don't see any way to avoid that now given the things that are happening*".

There was a lack of confidence that appropriate legislation would be implemented effectively in NZ to avoid the potential negative cybersecurity or ethical impacts of quantum computing. Participant 10 highlighted

this lack of confidence by stating, "*I don't think New Zealand from a legislative or regulatory perspective will do anything on quantum computing before its too late*", and Participant 2 concurred by comparing it to legislative inaction in AI, another technology area that also has the potential for societal harm, "*a very interesting parallel to your question around quantum computing is there hasn't been a large amount of regulatory or legislative change on the AI front…the people benefitting from it have no interest to make a change in that landscape*".

Additionally, the findings show that not all organisations will respond positively to regulation. A small minority of participants did not want this kind of intervention, as expressed by Participant 5 as follows, "*I would still rather deal with the devil I know of vendors working in their own interests than vendors trying to work under government mandate*". Therefore, standards should also protect NZ from potential technology-related harm. Participants believed standardisation would occur faster than regulatory measures and may be better received. For example, Participant 3 commented, "*standardisation across the industry moves a lot quicker*. *Regulation, I think you tend to get a mixed response, and potential negative behaviours from regulatory oversight*".

Finally, increased legislation may drive the necessity for increased law enforcement, and this is another area of national capacity that the findings identify could be grown and improved. Despite the challenges involved, participants felt the government should place more emphasis on prosecuting cybercrime. For example, Participant 16 described, "*we can keep improving our systems, or we could just go and hunt down and find and prosecute the people who are stealing money from businesses across the globe*. *We need to rely on governments to go after attackers more*".

5.2.5.4 Need to invest in quantum infrastructure and solutions

The findings identify a need for NZ to invest in and build quantum-enabled technology infrastructure. Participants acknowledged that NZ could choose to "*rely on what's happening overseas*" regarding emerging technology and adopt "*what others have developed*". However, participants also believed it is essential to build some quantum-computing infrastructure in NZ to ensure accessibility and confidence in this technology and to defend against the cyber threats it may pose.

Participants believe using quantum computers will be the best way to defend against potential quantum-enabled cyber threats. For example, Participant 4 expressed, "*we've lost unless we have a quantum computer ourselves that can fight against the quantum computer*". However, there is minimal quantum computing technology or infrastructure in NZ today, as described by Participant 14, "*no one can see these things, no one can touch them in New Zealand*. *We don't have any universities that are playing with this*".

Building quantum computing capability and investing in infrastructure to support this capability will be "*really important to protect*" NZ into the future and to ensure "*we don't end up just as a consumer*". Study participants wanted quantum computing made accessible to all, and providing this accessibility was one reason to justify NZ-based development in infrastructure and solutions. For example, Participant 32 described, "*I'd like it to be something that is accessible, which requires that the government play a role in terms of procuring and building that technology*".

The scale of funding required for quantum computing development means participants believed it was "*beyond the control of a single company*", and therefore, participants expressed a desire for "*national*

bodies" to start building the required infrastructure to support quantum-enabled technology and for "*vendors*" and "*government*" to lead research and development and start testing this technology now so that when organisations start to use it "*it's not completely new*".

The findings show that NZ must begin today by "*upgrading national infrastructure*" and finding niche areas in quantum computing technologies where it can specialise and contribute to the global market. For example, Participant 31 explained the pragmatic opportunities available to NZ, "*we are not going to win the race to build a quantum computer in New Zealand, but we could, in principle, build some key components for communication between quantum computers…I think that's where we should focus our efforts, find our appropriate niche and make sure that we are useful to people*".

5.2.5.5 Need to develop a quantum industry

The findings demonstrate that NZ should create its own quantum computing and technology industry as this technology will transform nations. Participant 14 described how NZ should participate in this innovation as follows, "*quantum computing absolutely is the new frontier; I hope in New Zealand we find a way to build, leverage, partner, be part of this wave because there's no doubt those machines will get bigger, faster, smarter*".

Some government-funded research into quantum-enabled technologies is underway in NZ through the Dodd–Walls Centre in Otago. The current research in this space is limited, and participants described it as "*restricted*", "*quite specialised*", and "*not many people are doing it*". However, it will be critical for NZ to maintain investment in this research so that NZ can contribute to the broader evolution of these technologies globally and ensure the country benefits from quantum technology advancements. For example, Participant 31 explained, "*we should remain engaged in the actual research and make sure that we are indispensable to that research or at least have something significant to add. The best way of remaining inside the tent is for people to need us*".

Currently, NZ does not have a quantum technology industry, and this idea is still in its infancy. The findings show a need to enable the commercialisation of NZ research to support the development of an industry. For example, Participant 29 described, "*there's certainly some research going on which the scientists would like to possibly try and commercialise at some level that could contribute to quantum communication networks...But there's no companies or industries that I am aware of in New Zealand that are specifically trying to make use of quantum technologies yet*".

Developing a quantum technology industry will be important to support the introduction of more secure ways of operating. Participants identified secure solutions such as "*satellite-based quantum distribution*" and "*quantum key distribution backbones*" as potential options for NZ to explore to enhance the future security of data transfer and communication. For example, Participant 31 highlighted, "*Singapore is putting in a quantum key distribution backbone, there already exist similar things around London…We probably need to either build or introduce our own ecosystem of quantum security companies to do that*".

Appropriate funding models must also be explored to promote innovation and drive a new quantum-computing industry. Participants described a current lack of support and "*business incuba*tors" for innovation. For example, Participant 9 discussed the inadequate funding models in NZ, "*one reason our*

business sector is so mediocre is that we don't have the right funding models…it limits the amount of funds that people can access for innovation".

Finally, to ensure greater innovation and commercialisation of NZ ideas in quantum technology and cybersecurity, there is a need for greater collaboration between academia, private industry, and the public sector. Participants highlighted the difficulty in accessing and disseminating "*national knowledge*" stemming from research and suggested "*greater integration*" is required between all groups.

5.2.5.6 Subtheme – Defining an NZ approach

"*New Zealand is a tiny little country that doesn't know it's a tiny little country*" (Participant 5)

NZ lacks a national strategy to address quantum computing opportunities and threats. Participants were unaware of any strategic national stance or recommendations around this technology. For example, Participant 26 explained, "*I haven't seen much evidence in the public sector that this is something that there is a concerted approach or strategy around*". A lack of transparency around activity that may be happening at a national level to address both current cyber threats and to plan for emerging cyber threats, such as those that may be posed by quantum computing, was also observed by study participants. Participants cited concerns around having no "*visibility*" of any potential good practices occurring and expressed doubt about government agencies acting "*in a transparent manner*". For example, Participant 30 stated, "*it's hard to know where that issue is with them*", and Participant Y explained, "*we don't really know what's going on behind the scenes*".

A national position on quantum computing opportunities and risks and a transparent plan to address these issues is needed, as expressed by Participant 7 in stating, "*I think there absolutely needs to be national strategies on that*". Participants would like to see "*greater leadership*" and "*clear direction*" from the government around how quantum computing risks must be managed. For example, Participant 18 described specific questions they felt were unanswered, "*how do they rate the risk and what do they believe as organisations we should be doing as a recommended standard and a practice?*". Many participants also felt this strategic guidance was required to ensure organisations use the technology wisely and were not left to act in "*morally ambiguous*" ways.

"*I mean, if we just pretend that quantum doesn't exist, then forget about it until it does, then we'll just be left behind*" (Participant 26)

The findings demonstrate that NZ must clearly define how it will approach and respond to the development of quantum computing and its enabling technology. Developing an approach will involve recognising NZ's strengths, limitations, and unique cultural ideals, which will influence its preferred response to these technologies and subsequent behaviour domestically and internationally.

NZ must consider how it will strategically respond to the challenges and opportunities presented by this emerging technology early to ensure the development of any quantum-enabled technology and standards make sense "*in a New Zealand context*" and advance "*New Zealand interests*". The importance of forming a national view on this technology was expressed by Participant 30 as, "*it's important New Zealand has a clear sense of our interests because we're not the same. We have different dynamics, and we need to think about them actively and decide what they are. What is the New Zealand perspective?*". Participants

raised "*Māori data sovereignty*" and "*physical sovereignty*" as examples of issues that drive the need for developing a NZ position around emerging technology.

Internationally agreed standards are required for the development and use of safe quantum computing technologies as described by Participant 22, "*there needs to be standards that are agreed to, United Nations level, to work through what are we going to say is ethical and what is not ethical when it comes making sure that we are working for a common good*". However, the formation of global standards must not preclude the ability to tailor these to suit individual countries and allow a national approach to be developed. This tailoring is possible, and Participant 18 gave an example of how this might occur in a similar realm of privacy as, "*there's an element here around taking examples around privacy frameworks that could be tailored for each geographical or a global region, but still sit on an overall set of principles around protecting the security of the individual and the privacy of data and services*".

Previous experience in successfully developing a unique national stance on emerging technology was found, demonstrating that it may be possible to do so for quantum computing. Participants referenced examples such as the "*TICSA legislation*", "*anti-nuclear stance*", and "*intellectual property*" to show where NZ has differed from other nations in their approach. For example, Participant 1 described the unique decisions NZ made in responding to perceived cyber threats when using Chinese telecommunications equipment in 5G networks as follows, "*the TICSA legislation was quite a different approach than other countries*. *Whereas other countries went,* '*No, we're just banning Huawei explicitly', New Zealand never said that…They say,* '*We look at each provider on its own merits, and assess the risks associated with that vendor"*". Another example of where NZ's approach differs from other large international players was explained by Participant 30 when describing our unique interest in IP, "*most countries are either very clearly sellers of intellectual property like the United States, then you have countries like China who are trying to lower the price of intellectual property because they need it*. *New Zealand is one of the only ones where we're at a balance of trade level*. *As we negotiate a position, we want a middle road*". While both previous examples suggest a moderate stance on issues, the anti-nuclear stance was cited by participants as evidence that NZ can also be "*controversial*" and bold in its approach where it perceives the potential for technology to cause harm. For example, Participant 5 reflected, "*I think back to New Zealand's choice to say,* '*We're not going to be nuclear*. *We're going to hold our ground*"".

NZ has several strong cultural values that could guide the creation of a national position on managing the advent of quantum computing and its related technologies. Participants expressed that NZ's approach should demonstrate a voice that is "*internationally independent*", "*free*", "*democratic*", "*principled*", "*responsible*" and it should show "*strong advocacy*" for current legally embedded human rights. Participant 8 discussed the vision as, "*real democracy, not the political system democracy, but the sense of a whole community of people who are all trying to have as good a lifestyle and as fair a share of power and wealth as possible*. *Let's find a way to use this for good*".

NZ has some limitations and benefits that may also influence its approach in determining a response to this technology. Some participants felt NZ is "*too small*" and does not have the "*resources or money*" *to* compete internationally in this area. NZ's lack of "*military capability*" was also acknowledged. Advantages also exist, and in particular, NZ's comparatively small size was highlighted by participants as allowing the

country to be "*nimble*". For example, Participant 30 described, "*we can all know each other, we can move quickly in unison…all things that big countries can't do*. *We can make our own decisions*".

There is trust that NZ is "*morally strong*" and that New Zealanders would not use quantum computing technology offensively for harmful purposes; however, the same level of trust was not shown towards other nations. Participant 7 described this sentiment when saying, "*I trust the New Zealand quantum computer owners to be ethically good*. *Do I trust other countries? Probably less so*".

The recognition that international users may not choose to act for the overall good when using quantum computing-enabled technology drives the need for NZ to promote its view of social responsibility when discussing the ethical development and use of these technologies on a global stage. Participants want "*meaningful conversations*" to occur globally and overwhelmingly believe NZ "*should be part of that conversation*". For example, Participant 17 stated, "*I think we definitely have to be part of that conversation because even if we can't leverage that technology for some time, we're going to be impacted and directly influenced by it…we can't let it happen around us*".

The findings show that participants felt that NZ is not currently playing the role it could play on the global stage in terms of these issues. For example, Participant 9 stated, "*I am somewhat disappointed in the New Zealand Government, and I do not believe that we play the role that we could play*. *In the cyber diplomacy area, the cyber law area*". However, participants were divided on whether NZ could influence global discussions on the ethical development and use of quantum computing technologies. For example, Participant 5 explained, "*it's good to show some moral fibre, but at the end of the day, New Zealand simply doesn't have enough sway to change the course of what's going to happen*". Other participants disagreed, believing we "*punch above our weight*" in global forums and can influence global opinion and action. For example, Participant 9 described, "*so this really comes down to what influence can you have as a small nation on politics*. *My answer to that is, quite a lot*. *As a smaller nation you can get quite a bit of moral force*. *Now, morality doesn't always sway the big players, but you can at least make them uncomfortable*".

Regardless of whether NZ can effectively influence global outcomes, participants wanted NZ to "*pick our moments*" and "*exert moral leadership*" around these issues on the global stage. For example, Participant 5 expressed, "*step up and say, 'We don't think that that's right*. *We don't think it's good for the world'. Maybe we'll make it a ripple, maybe we won't, but…we're going to be true to our beliefs and we're going to make our opinion known when it comes to advanced technologies like quantum*".

Current geopolitical dynamics will influence NZ's stance on managing quantum computing technology. There was concern about a sense of greater division and "*autocracies versus democracies*" in international politics today and how that division will influence NZ's approach to ethical issues around emerging technology. For example, Participant 11 explained how our unique position of being part of "Five Eyes" whilst having a "*very close*" trading partnership with China means NZ may not act in alignment with the values it holds close to, "*New Zealand*, *they're going to make sure that they don't sing out too loudly, even if they feel that the technology is being used unethically because we're part of the Five Eyes, but we're also very close trading partners with China*. *Now, if we piss off China, that's bad news for New Zealand's economy*. *If we piss off the US, that's also not great because they are our political allies*".

Some participants believed the "*leader of the Five Eyes*" alliance might determine the NZ approach as NZ will necessarily be "*interacting*" with allies who have "*heavy investments*" in quantum-enabled technology. Other participants cited the need for NZ to fully consider and balance its differing international relationships to ensure the right outcome for NZ, describing this as a "*difficult line to tread*". For example, Participant 30 explained, "*New Zealand's often being pressured into signing public declarations that make China seem inherently hostile to us…the idea that the world is just these two simple poles, it's bad for New Zealand and we shouldn't buy into that view*".

However, the increased geopolitical division participants observed may mean that NZ must consider taking a clear side on emerging technology issues. For example, Participant 31 expressed concern that continuing to straddle the geopolitical fence could lead to missed opportunities for NZ, "*where does New Zealand sit, which tent of quantum technologies? Do we align ourselves with our traditional Anglo-Saxon partners, Five Eyes...What about Europe? What's our relationship there? Because I think that there is a growing divide. And obviously China's our biggest trading partner, so we want to stay friendly there. My worry is that we get locked out of all three by trying to stay friendly with all of them*". Participant 10 also concurred with the need to make a decision, stating, "*we need to choose a side*".

International collaboration will be critical to ensure NZ can forward its unique interests, obtain access to quantum computing technologies, and mitigate their harmful impacts. For example, Participant 5 explained the need to ensure close ties with nations that are developing defences against quantum computing-enabled attacks such as "*quantum-resistant algorithms*" as follows, "*government…can direct treaties and relationships where we can piggyback on those who actually have the resources to develop the defences…we need to be really close to some who are willing to share that technology with us because it's going to play a part in the future*".

Participants highlighted the need for "*strong diplomacy*" and to maintain "*sensible alliances*" with other nations as there is "*benefit in a united front*". Placing more value and resources toward international diplomacy measures was considered necessary by the participants, and treating diplomacy as a "*core policy goal*" was suggested. NZ must also support strong international institutions and utilise mechanisms such as "*free trade agreements*" and "*treaty agreements*" to ensure its interests in quantum computing technology are possible. For example, Participant 31 highlighted the usefulness of initial agreements in this area, "*we've just signed a research agreement with the United Kingdom. I think…treaty level, the Horizons Europe is a treaty level agreement…I think those are useful*".

Overall, the findings in this theme demonstrate the need for NZ to hold "*public conversation and internal debate*" to decide what is in the nation's interest concerning quantum computing technologies so that the NZ Government can communicate a clear posture and "*advocate and push it*" both domestically and globally.

5.3 Document Analysis Findings

5.3.1 Develop Quantum Technology and an Ecosystem for Digital Sovereignty

The concept of digital sovereignty is woven throughout all the documents analysed in this study, and aspects of national digital sovereignty are addressed both implicitly and explicitly within these. The

Cybersecurity Strategy for Germany 2021 explains this focus by stating how digital sovereignty "*has grown considerably more visible and more relevant*" (Federal Ministry of the Interior, Building, and Community [FMIBC], 2021, p. 22) and this increased focus has resulted in an overarching theme of nations expressing intent to develop quantum ecosystems to support national digital sovereignty.

Securing national digital sovereignty is deemed important to ensure nations and regions can maintain "*autonomy*", "*independence*", "*prosperity*", "*global influence*", and "*safety*" in a future where society is highly digitalised. For example, The *Strategic Research Agenda* of the European Quantum Flagship explains, "*it is now widely understood that the mastery of deep technologies will determine the future prosperity of countries across the world*. *Sovereignty over these technologies will become the critical building block for the future economic development and digital self-determination of societies*" (European Quantum Flagship, 2020, p. 6). The analysis finds that multiple nations have declared the securing of national digital sovereignty a specific strategic goal.

To secure national digital sovereignty, it is necessary to strengthen and invest in sovereign cyber capabilities. Nations believe this will benefit their societies, as stated by *Australia's Cyber Security Strategy 2020*, stating, "*Sovereign capabilities benefit us all*" (Department of Home Affairs, 2020, p. 34). Additionally, the findings highlight how important cybersecurity is in achieving digital sovereignty as explained by the *Cyber Security Strategy for Germany 2021* as, "*secure technologies and solutions, alongside the ability to recognise and assess the opportunities and potential risks associated with digital technologies, are a key requirement for digital sovereignty*" (FMIBC, 2021, p. 22).

Many nations believe that developing, accessing, and securing quantum technology will contribute to national digital sovereignty as quantum technology has a "*special role*" in this regard due to its "*disruptive potential*" and possible application in "*secure communications and defence*". For example, GESDA's *Impact Story: Quantum Computing* report describes how several nations intend to use quantum technology to advance digital sovereignty as follows, "*governments, including those of China, South Korea, and Germany, have explicit goals to achieve* "*technological sovereignty*" *through local development and control of core quantum technologies*. *Others, including the UK, Sweden, and Japan, have announced plans to build their own quantum computer locally by 2030 or earlier*" (GESDA, 2022, p. 10). Therefore, the goal of building thriving national quantum ecosystems to support national digital sovereignty is found across almost all national strategies. Additional common reasons found for growing and investing in sustainable quantum ecosystems include providing "*worldwide leadership*", enabling the transformation of "*intellectual capital into economic value*", ensuring benefits are realised from new technology, maintaining "*a stake*" in the evolution of transformative cyber technologies, and supporting a "*quantum-enabled future*".

The document analysis found that several components are critical to a successful quantum ecosystem, including the presence of sufficient "*people and skills*", a workforce that is "*diverse*" and "*skilled*", an industry consisting of "*globally competitive quantum technology companies*", an engaged research community, and strong partnerships.

Formal strategies to manage general cybersecurity and the development, use, and impacts of quantum technologies are increasingly being created by nations to define, describe, and guide their approach to these issues. For example, the UK's *National Cyber Strategy 2022* describes the need for a cybersecurity

strategy as, "*sustaining our cyber power requires a more comprehensive and integrated strategy, considering our full range of cyber objectives and capabilities*" (HM Government, 2022, p. 11), and the Commonwealth Scientific and Industrial Research Organisation (CSIRO) roadmap, *Growing Australia's Quantum Technology Industry*, highlights how national quantum strategies are in place in several nations globally stating, "*the US, UK, EU, and China…have all established national strategies supporting quantum technology development"* (CSIRO, 2020, p. 12). Nations that lack a strategy to manage the evolution and impacts of quantum technology describe a less than-ideal and "*piecemeal approach*" to responding to emerging technology challenges.

All documents included in the study emphasised the need for broad and cross-functional consultation with "*individuals*"*,* "*businesses*"*,* "*community*", "*not-for-profit* organisations, "*academia*", the "*quantum sector*", and "*government*" to develop successful national approaches to managing the growth of quantum-enabled technology and its security and societal impacts. The findings also highlight a need for more transparency in national approaches to emerging technology and cybersecurity, as expressed here by the NZ Government's *National Security Long-Term Insights Briefing*, "*New Zealanders are concerned too and want to know more, and some want to be more involved in how we respond*" (Department of the Prime Minister and Cabinet [DPMC], 2023, p. 28). Some areas are responding to this need for greater transparency by explicitly setting transparent and measurable objectives in their strategies, such as seen in the *Cyber Security Strategy for Germany 202*1, which notes, "*government activity must be transparent if citizens are to trust the state*. *The 2021 Cyber Security Strategy therefore addresses the issue of making objectives transparent and measurable for the first time"* (FMIBC, 2021, p. 26).

A "*10-year horizon*" or "*10-year plan*" is used in most national quantum strategies analysed, with some extending a vision out 20 years. For example, *Growing Australia's Quantum Technology Industry* roadmap suggests a longer-term focus, "*the roadmap is focused on actions that can begin immediately to enable the successful development, demonstration and commercialisation of emerging quantum technologies over the next 20 years*" (CSIRO, 2020, p. 3). The strategic timeframes outlined encompass several common national or regional goals. Firstly, a widespread goal seen in the findings is building a fault-tolerant quantum computer capable of quantum acceleration. For example, the European Parliament's 2030 *Digital Compass: The European Way for the Digital Decade* states, "*By 2025, Europe will have its first computer with quantum acceleration, paving the way for Europe to be at the cutting edge of quantum capabilities by 2030"* (European Parliament, 2022a, p. 8). Multiple nations are also setting an even larger goal of building a full quantum internet. The European Quantum Flagship *Strategic Research Agenda* describes this goal as, "*the long-term vision for the Quantum Flagship initiative is for a "Quantum Internet": quantum computers, simulators and sensors interconnected via quantum networks…to secure our digital infrastructure*" (European Quantum Flagship, 2020, p. 6). Several nations believe successfully achieving the goal of developing a "quantum internet" will secure their global technical leadership and their digital sovereignty, as expressed by Canada's *National Quantum Strategy*, "*completing this mission would create a made-in-Canada quantum communications solution that would secure the Canadian economy and digital sovereignty*" (Government of Canada, 2022, p. 13).

In addition to a full quantum internet, a near-term goal is described, which is to implement QKD networks. For example, the *German Cyber Security Strategy 2021* states the intent to demonstrate these as follows,

"*the potential increase in security occasioned by QKD will be demonstrated not only in research prototypes, but also in real deployment situations, to show that it works in practice"* (FMIBC, 2021, p. 69), and finally, interim goals that specify the development and implementation of hybrid systems are highlighted in national strategies as key to "*transition smoothly from pre-quantum to post-quantum*" systems and algorithms. France's Agence Nationale de la Sécurité des Systèmes D'information (ANSSI), in their technical briefing document, describe the role of hybridisation as "*crucial*" for cryptographic security in the transition to a quantum-computing-enabled landscape (ANSSI, 2022, p. 4).

Detailed implementation plans are required to achieve the strategic quantum and cybersecurity goals outlined in national strategies. Nations are developing these "*execution plans*" now to ensure "*identified approaches*" and "*policy opportunities*" are met. For example, Canada's *National Quantum Strategy states*, "*in the near term, the Government of Canada is planning a more detailed rollout…These roadmaps will include detailed objectives, milestones and actions required*" (Government of Canada, 2022, p. 10). Low-level plans with milestone targets are already described in detail in some national roadmaps to achieve the development of these solutions. An example of such detail in the European Commission's Quantum Flagship *Strategic Research Agenda* is, "*demonstration of a chain of physically distant quantum repeaters enabling quantum communication over at least 800km using telecom fibres; Demonstration of a quantum network node of at least 20 qubits connected to a quantum network*" (European Quantum Flagship, 2020, p. 6).

Along with a strategy and plan, the findings show that national governance mechanisms for quantum and cybersecurity must be established to achieve strategic goals and enhance national digital sovereignty. For example, Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the *Digital Decade Policy Programme 2030* describes the need for governance that is "*comprehensive, robust, reliable, flexible and transparent*" (European Parliament, 2022b, para. 22) to achieve digital transformation goals, and the Government of Ireland's *National Cyber Security Strategy 2019–2024* highlights the need for a "*governance framework and structure*" (Government of Ireland, 2019, p. 50) to deliver the national cyber security strategy successfully.

Governments are, therefore, beginning to establish governance mechanisms such as "*quantum advisory councils*" and appropriate alternate structures to drive coordinated governance and deliver "*impartial advice*" to governments implementing quantum strategies. An example of this is given by the UK's *National Strategy for Quantum Technologies* in describing the purpose of the Quantum Technologies Strategic Advisory Board as follows "*(Qt SAB) was set up to provide a visible focus for quantum technologies in the UK and to act as a co-ordinating body for UK interests. It has an oversight of the UK National Quantum Technologies Programme*" (Quantum Technologies Strategic Advisory Board, 2015, p. 2).

Some limited proposals for international governance of quantum technologies were found, with the WEF developing a set of initial governance principles that nations can follow to ensure the responsible development and use of quantum computing. The WEF (2022b) believes establishing these principles will ensure a safe transition to the technology, stating, "*the proactive establishment of governance principles is key to building trust in quantum and to pre-empt possible risks before the technology is commercialized*" (p. 5)

5.3.1.1 Build and provide quantum infrastructure and solutions

The achievement of strategic goals in quantum computing and cybersecurity will depend upon the availability of quantum and supporting infrastructure. New and improved national infrastructure is required to enable quantum ecosystems that realise the opportunities and protect against the threats associated with quantum computing, as the findings show that a lack of infrastructure is currently limiting the growth of secure quantum ecosystems. For example, the Australian Government's *National Quantum Strategy* highlights this in reporting, "*growth is constrained by limited access to advanced infrastructure such as: – noisy intermediate-scale quantum computers and prototyping facilities – quantum materials and tools such as precision machining equipment*" (DSIR, 2023, p. 14).

Governments have recognised the need for new infrastructure, and the findings show widespread initiation of plans to invest in this area. For example, Europe's Quantum Flagship *Strategic Research Agenda* describes, "*to further develop this area as a whole…research and innovation priorities need to be accompanied by major European infrastructure investments such as those for Quantum Communications, Quantum Computers and Simulation or Quantum Sensing and Metrology*" (European Quantum Flagship, 2020, p. 6). However, there is a need to audit existing national infrastructure to identify where new infrastructure to support quantum-enabled technologies is required. The findings show this action is planned across all national quantum strategies analysed and is described by Australia's National Science Agency, who state their aim to, "*assess the industry capabilities and infrastructure facilities that will be critical to the success of a domestic quantum industry and develop business cases to address any gaps*" (CSIRO, 2020, p. 30).

It is universally recognised that developing the infrastructure needed to support quantum-enabled technologies is "*capital intensive and expensive*" and that the infrastructure is also required "*immediately*". Therefore, nations and regions are implementing "*strategic investment programs*" to address this need. National investment programmes in quantum and cybersecurity infrastructure are also anticipated to grow further. As described by Australia's National Science Agency, "*investment in quantum communication networks and related cybersecurity solutions can be expected to grow as the next generation of quantum technologies emerge*" (CSIRO, 2020, p. 24).

Supplying this new infrastructure is critical to enabling the adoption of quantum technology, as expressed by the US Government's *National Strategic Overview for Quantum Information Science*, "*a targeted expansion of the relevant Federal and industrial infrastructure…is needed to accelerate progress and prepare Federal agencies and industry to adopt the ensuing quantum technologies*" (National Science & Technology Council [NSTC], 2018, p. 9). It is also necessary for nations to enable greater access to quantum infrastructure to advance quantum and cybersecurity research and development, as there is currently insufficient infrastructure to support innovation. An example of this challenge is described in *Growing Australia's Quantum Technology Industry* roadmap, which states, "*Australian start-ups and research groups can face difficulties in accessing the infrastructure required for device prototyping and fabrication*" (CSIRO, 2020, p. 12).

The document analysis found the following critical infrastructure is required and planned to be built by nations to evolve global quantum ecosystems:

- Quantum computing hardware and software (including algorithm design). For example, "*the development of quantum processors...novel algorithms for machine learning and optimization; and transformative cyber security systems including quantum-resistant cryptography*" (NSTC, 2018, p. 2)

- High-performance classical hardware components. For example, "*ultra-cold cooling systems, …precision electronic and optical systems, basic components like cables appropriate for carrying quantum signals*" (NSTC, 2023, p. 31)

- Materials characterisation and fabrication facilities (NSTC, 2023, p. 38)

- End-user tools, platforms, and testbeds. For example, "*developing quantum computing test-beds – demonstrating the advantage of a quantum computer over a classical one*" (DSIT, 2023a, p. 9)

- Quantum supporting technologies. For example, "*the program has identified nitrogen-vacancy diamonds for magnetometry applications and single photon emitters for secure quantum communications as priority technologies*" (CISRO, 2020, p. 23)

- Quantum network infrastructure. For example, "*an optical communication backbone, routing, switching, detection, interconnects and quantum repeaters*" (CISRO, 2020, p. 24)

5.3.1.2 Build a skilled and diverse quantum technology and cybersecurity workforce

"*Education opportunities will be a significant point of differentiation between nations and institutions involved in quantum technologies*" (CISRO, 2020, p. 8)

Building and maintaining a skilled and diverse workforce is seen as essential for establishing healthy quantum ecosystems and ensuring a secure future in a quantum computing-enabled world. Building a "*quantum-smart*" workforce was a common goal across all documents, and the importance of this can be seen in this example from the UK's *National Quantum Strategy*, which states, "*building a diverse and thriving workforce that can drive the growing quantum industry will be vital to unlocking economic and societal benefits in the future*" (DSIT, 2023a, p. 26). The key actions being proposed globally to drive the development of national workforces skilled in both quantum and cybersecurity include identifying future quantum workforce needs, enhancing education at all levels, supporting broader engagement in quantum computing, developing skill taxonomies, improving quantum literacy, and creating quantum role models.

Most nations acknowledged the need for a diverse and broad range of expertise to support emerging quantum technology, such as expressed in Canada's *National Quantum Strategy*, "*future success requires harnessing expertise in a wide variety of fields, such as social science and humanities, business, and engineering*" (Government of Canada, 2022, p. 18). However, limitations in the current education systems are found where the focus is primarily on "discrete" disciplines rather than the "cross-disciplinary" study required to develop the skills required to answer complex challenges across quantum information science. All documents agree, therefore, that improvements are necessary throughout national education systems to support a future quantum-enabled society. For example, the European Commission's Quantum Flagship *Strategic Research Agenda* describes the changing requirements of the learning ecosystem as follows,

"*the conventional formal introduction to quantum physics, based on the concepts of 20th-century physics, will not meet the needs*" (European Quantum Flagship, 2020, p. 106).

Various initiatives were found to be proposed to address current limitations and enhance the education systems in many nations to support a future quantum ecosystem. Early education is being addressed by introducing STEM and quantum science awareness throughout the school curriculum in some nations. For example, the US *National Strategic Overview for Quantum Information Science* states they will "*address education in the area of quantum science at an early stage, including elementary, middle and high school levels*" (NSTC, 2018, p. 3). The Quantum Flagship Strategic Research Agenda also reinforces this idea by suggesting high school students are, "*engaged with modern didactic methods to explain the concept of a qubit, teleportation, and to explore quantum technologies in simple programming exercises*" (European Quantum Flagship, 2020, p. 31).

Even greater efforts to improve quantum education are observed at the tertiary level throughout the findings. For example, some national universities are establishing specific quantum education offerings, including master's programmes and short courses as described by the European Commission to, "*develop educational tracks on quantum technologies and its applied fields, including quantum communication, at universities throughout Europe*" (European Quantum Flagship, 2020, p. 44). Furthermore, universities are encouraged to add "*tenured or tenure-track faculty*" within interdisciplinary fields associated with quantum science and consider it a "*discipline for future concentration*". This additional effort is summarised by Canada's *National Quantum Strategy* as, "*recognizing the importance of all levels of quantum talent on industrial success, universities have bolstered efforts to develop the talent pipeline by equipping students with industry-relevant quantum competencies*" (Government of Canada, 2022, p. 19).

The findings highlight that raising the skills and competencies of the existing workforce is also necessary to support a thriving and secure national quantum ecosystem. This includes increasing the understanding of senior leaders who will influence the success and uptake of quantum technology as described in the European Quantum Flagship *Strategic Research Agenda*, "t*he main issue for industry is to develop concepts for raising the awareness of the workforce to current quantum technologies and their potential*. *This involves decision-makers in industry* [CEOs, CTOs, SME organisations], *who need special training courses*" (European Quantum Flagship, 2020, p. 107*)*.

Building a skilled workforce that is representative of society and sufficient for the future will require addressing the current lack of talent diversity in quantum technologies. Currently, nations report a "*severe gender imbalance*", with women being in a "*clear minority*" in the quantum technologies field. A lack of diversity negatively impacts a thriving quantum ecosystem, as described by Canada's National Quantum Strategy, which states that, "*representation in key fields relevant to the quantum sector is currently imbalanced, so Canada is missing out on a critical supply of new ideas and talent*" (Government of Canada, 2022, p. 21).

Nations recognise the need to foster diversity in quantum technology and cybersecurity both to promote "*social fairness*" and, as the European Commission's Quantum Flagship *Strategic Research Agenda* describes, to "*have a positive impact on productivity and innovation*" (European Quantum Flagship, 2020, p. 97). Solving the challenge to increase diversity will require addressing "*systemic bias*" in current

education and workforce processes and significant, sustained effort and investment over time, as highlighted by the European Commission, "*with only one in six ICT specialists and one in three STEM graduates being women…this challenge requires massive investment"* (European Parliament, 2022a, p. 5). The findings show that there are activities already underway in some nations to access the current "untapped potential" of women, which include initiating "*unconscious bias training*" and raising the "*visibility*" of female scientists.

Skilled workers in both cybersecurity and quantum are scarce, and global talent competition is growing. The findings show that nations already suffer from a lack of available talent and recognise that this issue will only become more challenging. For example, the Government of Ireland's *National Cyber Security Strategy 2019–2024* discusses the current challenge in cyber security, "*a number of substantial skills gaps have emerged in cyber security, largely as a consequence of its rapid development as a societal challenge*" (Government of Ireland, 2019, p. 36). The UK's *National Quantum Strategy* describes how the small pool of global talent impacts businesses in their preparation for quantum computing, "a *recent survey found that the top challenge for businesses in preparing for quantum computing was being able to access the right skills and talent*" (DSIT, 2023a, p. 26).

In response to skills scarcity, nations are now competing to attract and retain global talent in quantum computing, with most believing this to be "*critical*" to success. Many nations are focused on easing the immigration pathways for global talent to become destinations of choice for skilled workers. For example, as described by the *Growing Australia's Quantum Technology Industry* roadmap, "*it will be important to reduce barriers to efficient recruitment of global talent to support the short-term growth of the domestic quantum industry*" (CSIRO, 2020, p. 12).

Most nations are focused on driving quantum and cybersecurity talent to their individual countries in support of national digital sovereignty. This focus is further highlighted in finding only one document, Canada's *National Quantum Strategy 2022*, acknowledging how collaborating internationally on overcoming skill shortages could benefit all by "*growing the overall global talent pool for our mutual benefit*" (Government of Canada, 2022, p. 20).

5.3.1.3 Creating dynamic national quantum industries

To support the growth of quantum ecosystems, governments must enable innovation and quantum research commercialisation. However, challenges exist today for nations attempting to commercialise emerging technology as described by Australia's National Science Agency as, "a*ssessments of Australia's innovation system have found that Australia performs well at knowledge creation but has a poor record on the transfer and application of this into new technologies and businesses*" (CSIRO, 2020, p. 13) and this difficulty is globally widespread. For example, the European Commission also highlights it as a key problem to overcome by stating, "*the main challenge is to move quickly from early research to industrial exploitation*" (European Quantum Flagship, 2020, p. 7).

Specific areas proving difficult when attempting to commercialise emerging quantum technology and grow the industry include gaining "*early-stage long term capital*" in a currently uncertain global investment climate and the need for greater coordination between "*researchers and industry*" to identify attractive quantum applications. Additionally, the various yet unstandardised systems driving quantum innovation

ensure hesitancy with potential investors. For example, Australia's *National Quantum Strategy* describes this by stating, "*investors are uncertain about development timelines and which technologies to support*" (DSIR, 2023, p. 14).

The findings show a need to "*build stronger pathways*" to commercialise quantum research and overcome these challenges. The ability of start-ups and entrepreneurs to access funding is seen as a critical factor determining the successful growth of an innovative quantum industry, as described by Europe's Quantum Flagship *Strategic Research Agenda*, "*access to capital is a crucial factor for nurturing a quantum industry in Europe*" (European Quantum Flagship, 2020, p. 15). Nations are, therefore, looking to find "*efficient and effective*" funding mechanisms to support the growth of quantum businesses at all stages in their evolution. For example, the UK's *National Quantum Strategy* highlights the importance of this funding availability, "*to develop a globally competitive quantum technologies sector we must ensure UK companies can access finance at all stages of growth*. *Quantum technologies can require large amounts of investment before they produce a return and have lengthy research and development cycles to reach the market, requiring more patient capital than some other technology sectors*" (DSIT, 2023a, p. 38).

All cyber security and quantum strategy documents described a greater need for collaboration between industry, academia, and government to succeed in establishing and growing successful quantum technology ecosystems. For example, Canada's *National Quantum Strategy* describes the need for this collaboration as follows, "*Expanded partnerships between academia, industry, government are essential to translate quantum research into societal benefits*" (Government of Canada, 2022, p. 18) and a specific focus on improving and expanding "*public-private cooperation*" and "*industry-academia*" collaboration is seen throughout the findings. For example, the benefits of improving industry-academia collaboration are described as follows, "*increasing industry-academia collaboration was noted as a way to draw research talent into industry, increase commercialization, and ensure strong readiness to engage and create value from quantum applications*" (Government of Canada, 2022, p. 7).

Additional mechanisms found to be used globally to support and grow national quantum industries are presented in Table 7.

Table 7

Growing Quantum Industry and Innovation

Mechanisms to grow innovation and quantum industry	Example document extracts
Running programs to fast-track quantum projects for a variety of use cases	"*Design new programs to incentivise the continued growth of quantum use cases in sensing, communications, and computing. The goal of these programs should be to fast-track projects using quantum and other advanced technologies to solve significant national challenges*" (DSIR, 2023, p. 22) "*Drive commercialisation through new programs to incentivise the continued growth of quantum use cases*" (DSIT, 2023a, p. 10)
Enabling greater funding and investment in innovative quantum research	"*Create pipelines for investment in industry-ready quantum technologies through the National Reconstruction Fund*" (DSIR, 2023, p. 10). "*incentivise private investment, including through roadmapping and demonstration*" (Quantum Technologies Strategic Advisory Board, 2015, p. 4) "*lifting business investment in research and development*" (DSIR, 2022, p. 9)
Establishing dedicated organisations to focus on growing innovation	"*establish a Canadian innovation and investment agency. This agency will work to help new and established Canadian firms innovate, commercialize research, and create new economic opportunities for workers and businesses in Canada*" (Government of Canada, 2022, p. 7) "*establishing industry associations such as Quantum Industry Canada. The technology mentoring program Creative Destruction Lab has spurred growth in the quantum sector by helping launch more than 50 quantum firms through its four quantum streams*" (Government of Canada, 2022, p. 22)
Providing greater support for quantum technology-specific businesses	"*support early adopters of these new technologies as they emerge over differing timescales*" (Quantum Technologies Strategic Advisory Board, 2015, p. 4) "*supported the incubation, start-up and scale-up of leading quantum businesses of all sizes*" (Government of Canada, 2022, p. 23). "*R&D procurement spending (contracts) and grants to support the growth and scale-up of firms*" (Government of Canada, 2022, p. 24) "*leveraging and expanding existing research commercialisation programs and initiatives, to grow business acumen in emerging quantum start-ups*" (DSIR, 2022, p. 9) "*Explore efficient and effective funding mechanisms to support the demonstration and commercialisation of quantum technology applications and enable the growth of emerging quantum businesses*" (CSIRO, 2020, p. 30) "*Support entrepreneurship and accelerator programs that enhance the commercialisation skills of deep technology start-up*" (CSIRO, 2020, p. 30)

Mechanisms to grow innovation and quantum industry	Example document extracts
Enabling access to quantum infrastructure	"*enable access to world leading infrastructure – including quantum computers – and manufacturing capabilities that will allow researchers and companies to flourish*" (DSIR, 2022, p. 4) "*National quantum technology and flexible fabrication facilities that enable collaborative R&D, engagement with end-users, and product prototyping for global value chains*" (CSIRO, 2020, p. 16) "*The next ten years of innovation will require access to the right research and innovation infrastructure to test, pilot and demonstrate the value of these technologies in the laboratory and real-world settings so that we can accelerate their path to market*" (DSIT, 2023a, p. 35)
Fostering collaboration	"*delivered funding to Canadian small and medium-sized enterprises to undertake collaborative R&D and technology matchmaking missions with foreign industrial partners in the quantum space*" (Government of Canada, 2022, p. 23) "*showcasing benefits to emerging and established industries, and fostering stronger linkages between academia, industry and government*" (DSIT, 2023a, p. 9) "*increasing coordination, investment and awareness in Australia's quantum ecosystem, including: developing and promoting use cases for existing and emergent quantum capabilities (for example, sensing, security, communications, simulation and optimization)*" (DSIR, 2023, p. 40) "*sharing of knowledge and resources between quantum researchers and practitioners across industry, government and academia*" (DSIR, 2022, p. 9)

Finally, enabling and driving the early adoption of quantum technologies, including quantum-safe solutions, is found to be an important outcome of many national strategies to assist in growing a viable quantum industry and gaining an early advantage over other nations. Countries refer to the need to "*stay ahead of the technology curve*" and be "*early movers*" and "*pioneers*", and the findings show early adoption is promoted to harness the economic and security benefits of a quantum-enabled world, as stated in the UK's *National Quantum Strategy* as a goal to, "*drive the adoption and use of quantum technologies in the UK to deliver benefits for the economy and society, as well as our national security*" (DSIT, 2023a, p. 10).

5.3.1.4 Fostering quantum research

Fostering world-class research in both cybersecurity and quantum technologies is also seen as vital when looking to grow a quantum industry and support the transition between education, innovation, and industry. Where nations are found to be successfully launching a quantum industry, a history of long-term investment in quantum research is present. For example, Australia's *National Quantum Strategy* consultation paper highlights this enabling factor by stating, "*world-leading quantum research and talent is the result of over 20 years of investment establishing strong scientific and technical foundations…this long-term investment in foundational research is now enabling the growth of exciting new start-ups and ventures*" (DSIR, 2022, p. 6).

Funding and promoting research into basic and applied quantum computing technologies is a goal in all quantum strategies analysed. The need for research to be genuinely cross-disciplinary is highlighted. For example, an action from Australia's growing quantum roadmap is to, "*establish a multidisciplinary and multi-institution research initiative focused on the development and evaluation of software applications and quantum control techniques for noisy intermediate-scale and large-scale quantum computers"* (CSIRO, 2020, p. 31).

National investment in quantum technology research and development is found to be critical for forming and maintaining effective international partnerships in the evolving global quantum technology ecosystem. For example, Canada, in their *National Quantum Strategy*, highlights how other countries have "*ramped up their efforts*" to develop quantum technology and how it is necessary for Canada to "*build on its quantum advantage*" to "*partner effectively*" in an environment of growing international investments (Government of Canada, 2022).

Nations currently leading in developing quantum technologies are explicitly outlining conditions of international partnerships that require equal contribution, as described by the EU's Quantum Flagship *Strategic Research Agenda* whereby they describe international partnership in quantum research and innovation only to be suitable and undertaken where, "*the expertise of the partners complements each other…is of similar levels*" and "*Europe should benefit at least as much as its partners from the international cooperation*" (European Quantum Flagship, 2020, p. 92).

The findings show that increasing the level of collaboration in international research is a goal of some nations where the opportunity is deemed "*mutually beneficial*"; however, currently, much less emphasis is placed on this activity than on strategic domestic research initiatives.

5.3.1.5 Supply chain security and accessibility

There is significant concern around the security and accessibility of the quantum technology supply chain, and the findings demonstrate that nations are concerned about the overreliance on non-sovereign technology and resources in an environment of increasing cybersecurity threats. For example, the introduction of cyber risk due to the reliance on foreign technology is described in the US *National Cybersecurity Strategy*, which states, "*we depend upon a growing network of foreign suppliers*. *This dependency on critical foreign products and services from untrusted suppliers introduces multiple sources of systemic risk to our digital ecosystem*" (The White House, 2023, p. 32).

Most documents also highlight how important it will be to gain stable access to critical components for building quantum computers to ensure innovation and development can continue at pace. For example, GESDA (2022) describes this issue as follows, "*the expertise, materials and enabling technologies required to build quantum computers could become a major bottleneck*. *Countries that control certain resources or core technologies, such as rare earth metals or the helium needed for refrigerating quantum computers, could gain significant economic and geopolitical advantage*" (p. 8).

Therefore, ensuring broad access to quantum and supporting technology that enables the pathways required for transitioning to quantum-enabled systems is stated as an important aim in most documents. For example, this is expressed by the UK's *Cyber Security Strategy 2022* in their written goal to secure a robust supply chain as follow, "*secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply*" (HM Government, 2022, p. 14).

Finally, the findings demonstrate that the need to ensure a reliable quantum supply chain and avoid introducing cyber risk from foreign sources further drives the goal to develop sovereign capacity and enhance national digital sovereignty. For example, the US National Cybersecurity Strategy states, "*Critical inputs, components, and systems must increasingly be developed at home*" (The White House, 2023, p. 32).

5.3.1.6 IP protection

Appropriately "*protecting*" and "*mobilising*" IP will be important to ensure that the benefits of quantum technology can be realised globally. Owning and protecting the IP that underpins commercial quantum applications is seen by individual nations and regions as an important step to "technological independence" and commercial success, as described by the European Commission's Quantum Flagship *Strategic Research Agenda*, and "*to build a flourishing quantum industry, Europe needs to protect its ideas and strategically build up intellectual property to compete with other regions…it would be alarming to see Europe falling behind in the race for IP in quantum technologies*" (European Quantum Flagship, 2020, p. 15).

The findings show that the use of education, frameworks, patents, trade secret protections, and contractual obligations are being encouraged as tools to ensure IP protection. The UK's *National Quantum Strategy* describes the new protection measures as follows, "*we have put in place measures such as the National Security Investment Act 2021, export controls, responsible research programmes, grant agreements and*

advice on IP protection to help companies and academic institutions to protect themselves from hostile actors who may seek to exploit their technology or knowledge" (DSIT, 2023a, p. 49).

Despite implementing these measures, the need to "*strike an appropriate balance between restrictiveness and openness*" is also reported as necessary when addressing IP, as the findings caution that overly restrictive or conservative approaches to IP laws may create "*unintentional barriers*" to development and investment, and hinder research commercialisation.

There is some limited awareness of the need to question IP management on a global scale due to the international nature of many businesses and the need to maintain an equilibrium between "*free trade*" and "*protectionism*". The European Commission highlights this consideration, stating, "*IP rules are an important issue while constructing international collaborations on quantum technologies and should be questioned in a global context*" (European Quantum Flagship, 2020, p. 91). However, most documents only suggest implementing IP measures to secure national interests.

5.3.1.7 Growing government capacity and capability

The documents show that it will benefit nations to grow government capabilities, awareness, and expertise in cybersecurity and quantum technology. Greater government capability and expertise in cybersecurity are believed to be required for multiple reasons, including to "*respond to the growing cybersecurity threat*", better support businesses to "*meet cybersecurity standards*", and improve the "*resilience*" of the public sector.

Increasing government cybersecurity capacity is already underway in many nations. For example, the US *National Cybersecurity Strategy 2023* describes its government's efforts in this space as follows, "*the Federal Government has increased its capacity to respond to cyber incidents; arrested and successfully prosecuted transnational cybercriminals*" (The White House, 2023, p. 14). However, more nations are recognising that greater investment is still required to lift capacity with the advent of quantum computing technologies and ensure the government is knowledgeable and equipped to understand the challenges this technology poses and to lead and manage impacts. For example, the UK *National Cyber Strategy 2022* aims to ensure "*government is better able to analyse new and developing science and technology and understand the implications for UK cyber policy and strategy"* (HM Government, 2022, p. 81).

National goals to "*de-risk*" emerging quantum technologies, provide "*technical leadership*", advance quantum applications that support "*government priorities*", and "*enhance the readiness*" of society for quantum technologies are all found to require enhanced government understanding, expertise, and capacity to succeed.

5.3.1.8 Creating international partnerships

Despite a heavy emphasis on developing national technical sovereignty throughout the findings, the need to form strategic international partnerships and collaborate is acknowledged as useful for quantum technology progress. As expressed in Canada's *National Quantum Strategy*, "*the surest way to succeed in the quantum technologies race is to work together*" (Government of Canada, 2022, p. 29). Mechanisms found to be promoted to drive international collaboration include "*bilateral*" partnerships*,* "*regional and*

bilateral agreements", and working with "*international institutions*" and "*multilateral processes*" such as "*the United Nations (UN) Group of Governmental Experts and Open-Ended Working Group*".

Currently, international collaboration is found to be primarily driven by the need to ensure accessibility to scarce global quantum technology experts, research and technology, as described by the US *National Strategic Overview for Quantum Information Science* in stating they will, "*identify and prioritize strategic bilateral partnerships to ensure that the United States…has access to international technologies, research facilities, and experts in QIS*" (NSTC, 2018, p. 13). However, Canada's *National Quantum Strategy* also recognises the value of international collaboration to ensure the "*interoperability*" of the technologies and as a means to "*leverage international markets*" (Government of Canada, 2022, p. 8).

5.3.1.9 Subtheme – Influence and protect behavioural norms in technology

There is widespread acknowledgement within the documents that digital technologies can underpin and support national values such as "*democracy*", "*equality*", and "*freedom*" and that they should contribute to the achievement of these values, as described in the Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022, "*digital technologies should contribute to achieving broader societal outcomes that are not limited to the digital sphere, but have positive effects on the everyday lives and well-being of citizens*" (European Parliament, 2022b, para. 22).

Ensuring national values are maintained in the online environment is an outcome of successful national digital sovereignty, and the need to influence and protect the values and behaviours that nations see as "*norms*" is a core concept seen throughout the documents analysed. For example, the European Commission communicates, "*digital policy is never value-neutral, with competing models on offer*, *the EU now has an opportunity to promote its positive and humancentric vision of the digital economy and society*" (European Parliament, 2022a, p. 18).

The findings demonstrate a desire to develop an agreed set of ethical use principles for quantum technology to ensure it is universally embraced. For example, the Australian Government's *National Quantum Strategy* explains, "*the public is increasingly aware of the ethical and social implications of new technologies, and we should not assume they will enthusiastically embrace quantum technologies*. *By building principles for responsible development and use, quantum researchers and developers can develop technologies that align to Australian values and expectations and protect human rights*" (DSIR, 2023, p. 41).

In addition to creating guidelines for the ethical use of quantum technology, there is still a need to develop international standards to ensure the "*security*" and "*interoperability*" of this technology. For example, the Federal Office for Information Security (FOIS) in Germany describes this need in one area of quantum technology, "*the standardisation of QKD protocols with associated security proofs is particularly important in the context of certifications and approvals to be able to assess their security*" (FOIS, 2021, p. 63). The findings show that nations are exploring ways to "*better support*" the development of appropriate international standards in technology, and most have explicit goals to actively participate in the creation of these standards, such as seen in the Australian Government's *National Quantum Strategy*, which states the aim to "*be an active participant in global standards-setting bodies to promote the development of standards that support a thriving, accessible and safe quantum ecosystem*" (DSIR, 2023, p. 9).

The document analysis found that more international standards are required both for "*cybersecurity*" and for the specific building blocks for quantum applications, such as described by the German FOIS, "*the future interoperable use of quantum communication requires the standardisation of…the protocols used, the authentication methods used, key management, the integration of repeaters and network aspects*" (FOIS, 2021, p. 53). The findings also highlight the need for these new international standards to be created through a "*transparent*" global process, and that they must be "*strong*", "*mutually advantageous*", and support "*responsible and inclusive*" quantum development and use.

Leading the development of technology standards is deemed important to some nations to ensure their interests, norms, and values are encompassed within these, thereby supporting their national digital sovereignty. For example, the UK's *National Quantum Strategy 2023* states their aim to lead this process as follows, "*demonstrate UK leadership in international standards…creating standards that are compatible with our norms and values*" (DSIT, 2023a, p. 57). Similarly, contributing to and shaping global thinking on ethical and secure emerging technology development and use is stated as a goal for nations wishing to ensure their values are upheld in the digital world. For example, Australia intends to shape global thinking as stated in the *2023–2030 Australian Cyber Security Strategy Discussion Paper*, "*Australia is a respected voice in addressing the challenge of making the world a safer place online. We can leverage this voice through tangible steps to shape global thinking, particularly in relation to new and emerging technologies*" (Department of Home Affairs, 2023, p. 17).

The findings show that nations are primarily focused on upholding values around security and safety, openness, freedom and democracy, and stability in the development and use of emerging quantum technology and cybersecurity, as seen in Table 8:

Table 8

National Values Expressed in Quantum Strategies

National values focus	Example evidential extracts
Safety and security	"*a more secure cyberspace and upholding fundamental rights online*" (FMIBC, 2021, p. 27)
	"*the protection of privacy*" (DPMC, 2019, p. 9)
	"*an Irish society that can continue to safely enjoy the benefits of the digital revolution*" (Government of Ireland, 2019, p. 11)
	"p*romotes secure and trusted data flows, respects privacy*" (The White House, 2023, p. 30)
Openness, freedom, democracy	"*a democratic, value-driven approach*" (European Parliament, 2022a, para. 2)
	"*the right to freedom of expression*" (DPMC, 2019, p. 13)
	"*champion a free, open…internet*" (DPMC, 2019, p. 8)
	"*ensure that cyber space remains open, secure, unitary, free*" (Government of Ireland, 2019, p. 12)
Stability	"*promote peace and stability in cyberspace*" (DPMC, 2019, p. 13)
	"*able to facilitate economic and social development*" (Government of Ireland, 2019, p. 22)

Additionally, the findings show some focus on ensuring equality and "*a level playing field*" is upheld nationally and globally in the digital world. An existing digital divide is recognised by many of the documents

analysed, such as the European Commissions: 2030 Digital Compass: the European Way for the Digital Decade, who explain, "*a new digital divide has also emerged…between those who can fully benefit from an enriched, accessible, and secure digital space…and those who cannot*" (European Parliament, 2022a, p. 2.). The closing of this digital divide is found to be a stated desire of some nations. For example, the European Commission states, "*The European vision for 2030 is a digital society where no one is left behind*", and most documents describe an opportunity to focus on promoting national values, including equality, when developing quantum technology for the betterment of society. For example, this is described in the Strategic Research Agenda of the Quantum Flagship as follows, "*Tackling the challenges of equality, equity and inclusion in the quantum technologies domain as we begin to structure this emerging industry represents a timely opportunity*" (European Quantum Flagship, 2020, p. 97).

The primary way nations intend to drive their values into cyber security and emerging technology development, as seen in the findings, is to collaborate with other nations in proactively exploring and defining the risks of this technology and developing principles for "*responsible and secure*" development and deployment. For example, Australia's National Science Agency publication - Growing Australia's Quantum Technology Industry, describes this intent in the following strategic action points, "• *Embed responsible innovation practices into quantum technology R&D • Foster dialogue with international governments and partners to understand practical policy responses to any emerging risks* (CSIRO, 2020, p. 35)". Some documents also highlight the possibility of funding research specifically into the ethical use of quantum technology. For example, Growing Australia's Quantum Roadmap states they will "*Proactively explore and address any unknown ethical, social or environmental risks that may arise with the next generation of quantum technologies*" (CSIRO, 2020, p. 30); however, this idea is not expressed universally in the documents analysed.

Upholding desired behavioural values and norms in cyberspace involves addressing those acting in contrast to these. The findings show a need to hold those responsible for poor behaviour in cyberspace accountable, and it is clear from the documents analysed that proactively disrupting cybercrime is becoming more prioritised globally. For example, the US *National Cybersecurity Strategy 2023* intends to "*hold countries accountable for irresponsible behavior in cyberspace and disrupt the networks of criminals behind dangerous cyber-attacks around the globe*" (The White House, 2023, p. 1).

The findings highlight how nations emphasise the need for greater "*powers*" and "*capability*" to protect their citizens in cyberspace and that all are looking to strengthen their response to global threat actors. However, national approaches vary in the intended scope and degree of strength when discussing the use of government power. For example, Australia, in their *National Quantum Strategy: Consultation Paper,* describes the need for powers to be "*fit for purpose*" (DSIR, 2022, p. 15), whereas the US National *Cybersecurity Strategy 2023* states they will use "*all instruments of national power*" to "*dismantle*" threat actors (The White House, 2023, p. 14). The UK also expresses a stronger stance in stating in their *National Cyber Strategy* how they will use "*all means available*" to act against cybercrime (HM Government, 2022, p. 34).

Some documents recognise that international collaboration will be essential for quantum-enabled technology to flourish. For example, as stated by GESDA, "*Quantum computing is incredibly challenging and unless the collective intelligence of the world's best minds is leveraged, the chance will be lost to make*

rapid progress and achieve the transformative potential" (GESDA, 2022, p. 8). Specifically, the findings show that a complete set of use cases for quantum-enabled technology does not exist as described by Canada's *National Quantum Strategy* in saying, "*the full range of potential applications to real-world problems remains uncharted*" (Government of Canada, 2022, p. 11), and that identifying and defining a full suite of use cases to accelerate the interest, awareness, and understanding of quantum-enabled technologies and their potential impacts requires global participation. The inclusion of wide consultation (yet unrealised) is considered particularly important when negotiating the ethical use and impacts of this technology and attempting to ensure that development goals are met. For example, GESDA (2022) describes, "*those developing the technology are not in touch with the realities of the countries in most need and facing the greatest societal challenges*. *Building real use cases requires input from these countries, which at present is limited due to lack of both awareness and access*" (p. 8).

However, the findings also show that global technology cooperation is challenging due to differing national standpoints, described as a "*clash of competing interests*, *values and visions*" by the UK's *National Cyber Strategy* (HM Government, 2022, p. 10). While increasing collaboration and cooperation with international allies is seen as important to ensure emerging quantum technology delivers benefits and aligns with national ideals and values, most documents only promote collaborating with "*like-minded*", "*trusted*" nations or "*established partners*" due to the potential national security and economic impacts of this technology. Only one document expressed an intention to continue open dialogue with nations that differ in their values and views around the use of emerging technology, as seen in the US *National Cybersecurity Strategy*, "*we will continue to engage with countries working in opposition to our larger agenda on common problems*" (The White House, 2023, p. 29), thereby making it clear that the perceived national security implications of quantum technologies threaten open global collaboration. GESDA summarises the impact of this potential concern as follows, "*concerns around the security implications of the technology could also see the field drift away from the open collaboration that has powered advances to date towards more siloed efforts, which could slow innovation*" (GESDA, 2022, p. 8).

5.3.2 Protect National Security and Economy from the Impacts of Quantum Technology

Increased geopolitical tension and cyber threats are driving the need for nations to increase their cybersecurity efforts. For example, New Zealand's *Cyber Security Strategy 2019* states, "*technological changes are not happening in a vacuum: the geopolitical picture has also shifted, with a greater range of state actors making the most of cyber-enabled tools to steal information, spread disinformation and launch attacks*" (DPMC, 2019, p. 3).

It is believed that "*the number of state-sponsored cyber operations is rising*", and the findings demonstrate that nations feel increasingly threatened and recognise a need to strengthen their cybersecurity. For example, the US *National Cybersecurity Strategy* states, "*The governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms*. *Their reckless disregard for the rule of law and human rights in cyberspace is threatening US national security and economic prosperity*" (The White House, 2023, p. 3).

Rising geopolitical differences are also influencing the ways nations are responding to emerging quantum technology. National governments increasingly see quantum computing as a "*prestige technology*", which may have significant geopolitical and security implications. The findings show widespread recognition of the need for nations to develop and use quantum technology to ensure future national security and economic stability. The UK's *National Quantum Strategy* demonstrates this by stating that, "*quantum is a priority technology for the government, and one that will remain critically important for our economic growth, economic security, national security and defence*" (DSIT, 2023a, p. 8).

5.3.2.1 General cybersecurity

The findings show that cyber capabilities in many nations are not keeping up with the escalating cyber threat environment. For example, Australia's *Cyber Security Strategy 2020* states, "*Growth of cybercrime is outstripping our ability to respond*" (Department of Home Affairs, 2020, p. 15), and nations acknowledge they need to be "*better prepared*" to face cyber threats.

Creating "*fit-for-purpose*" cyber incident response and mitigation plans is seen as one way to ensure nations are more prepared to respond to and recover from incidents. This need is stated as a goal by the UK, who aims to be, "*more prepared to respond to and recover from incidents, including through better incident planning and regular exercising*" (HM Government, 2022, p. 74). Creating specific mitigation and response plans that address cyber threats resulting from quantum computing will additionally help "*enhance the readiness of governments, society, and end-users*" for next-generation quantum technologies.

Lifting awareness and providing information on the cyber threats that may result from quantum technology is also documented as a high-priority activity for national governments to ensure better preparation. Plans are in place in many areas to achieve greater cybersecurity awareness; for example, New Zealand's *Cyber Security Strategy 2019* describes an action to create "*practical, targeted and regular awareness campaigns to build awareness and resilience among different groups of people*" (DPMC, 2019, p. 11).

It is clear from the findings that current national cybersecurity measures of a voluntary nature are insufficient to drive meaningful change and that increased cyber resiliency is needed to combat threats. The US *National Cybersecurity Strategy* proves this by stating, "*the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes*" (The White House, 2023, p. 8). The findings also highlight various issues with current cybersecurity regulatory measures, including inconsistencies, unclear obligations, and missing or insufficient standards. For example, the Cyber Security Strategy for Germany 2021 describes this situation, "*The regulatory framework for the cyber security of products and services is inconsistent at national and international level…Binding standards in some cases do not exist or are insufficient*. *Moreover, ascertaining the relevant regulation can be time-consuming and error prone*" (FMIBC, 2021, p. 61).

There is a need to enhance existing regulatory frameworks to ensure they are "*fit-for-purpose*" and sufficient to protect nations in the current environment and into the future when quantum technologies will drive greater risks. For example, the *2023–2030 Australian Cyber Security Strategy Discussion Paper* states, "*it is clear from stakeholder feedback and the increasing frequency and severity of major cyber incidents, that more explicit specification of obligations, including some form of best practice cyber security*

standards, is required across the economy to increase our national cyber resilience" (Department of Home Affairs, 2023, p. 17). Defining and implementing "*minimum security requirements*" along with creating regulation that guides the responsible development and use of quantum capability are identified in most documents as critical areas requiring action. For example, the UK's *National Quantum Strategy 2023* describes this action, "*Create a national and international regulatory framework that supports innovation and the ethical use of quantum technologies*" (DSIT, 2023a, p. 10).

The findings stress that new regulations must be "nimble" enough to change with evolving technology, allow public-private collaboration, be easy to understand, be sensitive to implementation costs, and be tailored for risk profiles. For example, the UK *National Quantum Strategy 2023* describes the regulatory requirements as, "*Quantum regulation will need to be: • Stable, coherent and predictable • Agile enough to move quickly with technological development • Simple to understand and inexpensive to implement • Where possible, co-designed with industry • Focused on innovation and industry-needs • Champion the transparent and ethical use of quantum technologies*" (DSIT, 2023a, p. 47). An early example of legislation that supports the quantum ecosystem is seen in the US *Quantum Computing Cybersecurity Preparedness Act*, which outlines clear guidelines for preparing for quantum technology, such as, "*Not later than 180 days after the date of enactment of this Act, the Director of OMB shall establish, by rule or binding guidance, a requirement for each executive agency to establish and maintain an inventory of each cryptographic system in use by the agency*" (US Government Publishing Office, 2022, section 4).

Nations are starting to see the necessity of addressing cybersecurity as both a "task for the present" and a vitally important task for the future to "*get ahead of changes in the risk environment*". The need to focus cybersecurity efforts more strategically and prioritise "*emerging and enabling technologies*", including quantum computing, is described across the documents analysed. The US *National Cybersecurity Strategy* describes this change to a more strategic approach as follows, "*We will realign incentives to favor long-term investments in security, resilience, and promising new technologies*" (The White House, 2023, prelim).

5.3.2.2 Protecting national security from the impacts of emerging quantum technology

It is believed that quantum technology will be transformative and have wide-reaching impacts on society. For example, the Australian Government *National Quantum Strategy* states, "*The impact of the quantum revolution will be comparable to the digital revolution that brought us transistors and lasers, which are the basis of all our modern electronics, computers and communications*" (DSIR, 2023, p. 5). However, most documents also highlight how the full impacts of evolving quantum technology and QIS on national security and the economy are as yet unknown, as described in the US *National Strategic Overview for Quantum Information Science*, "*significant uncertainty remains regarding the overall economic and national security impact of QIS*" (NSTC, 2018, p. 5).

The findings show most nations anticipate both beneficial and detrimental impacts on their national economies and national security due to emerging quantum technology. For example, most documents highlight how the evolution of quantum computing may drive positive advances in various areas and supply benefits to society, such as those described here by Canada's *National Quantum Strategy*, "*Emerging quantum innovations will underpin major advances in fields from computing to artificial intelligence (AI) to health care…developing life-saving drugs and vaccines, locating critical minerals and other natural*

resources, making transportation safer…secure communications, defence applications" (Government of Canada, 2022, p. 4)

However, all documents also caution against the potential negative impacts of this technology, particularly the new cybersecurity risks it presents to cryptography, as this is described as an essential tool used to protect the global economy. The recognised threat that quantum computing poses to cryptographic systems is highlighted in all documents as a risk to national security postures. The *National Quantum Strategy* of Canada describes this stance as, "*Quantum computing presents a significant cyber security risk, as it has the potential to break current security algorithms*...*Quantum computing-enabled malicious cyber activity could put personal information, financial systems, utility grids, infrastructure and national security in peril*" (Government of Canada, 2022, p. 8).

There is international acknowledgement that a stance of "*when not if*" should apply when addressing quantum computing, and the threats this technology presents to cryptographic processes must be addressed today. For example, the European Commission: Quantum Flagship Strategic Research Agenda discusses this need as follows, "*Although it may take many years for a large-scale quantum computer to be realised, quantum security techniques are important today for protecting information that must remain confidential for many years, such as industrial secrets of companies or the genome data and medical records of individuals*" (European Quantum Flagship, 2020, p. 20).

The primary ways national security will be maintained in response to quantum technology evolution are via the development of quantum technology solutions for defence and the development and implementation of quantum-resistant cryptography.

Development of quantum technology

The findings show nations and regions are planning to develop and use quantum technology to protect national security by building secure quantum communication networks as described in a goal in Canada's *National Quantum Strategy* to "*invest in a parallel infrastructure for secure communications for highly sensitive information using quantum technologies, including critical space-based infrastructure*" (Government of Canada, 2022, p. 8).

The development and use of quantum cryptography, particularly QKD, is indicated as a future solution to secure systems in many documents. Nations are actively pursuing its research, development and use as described by Germany's FOIS, "*quantum key distribution (QKD) is also attracting strong interest worldwide*. *Both in the EU and in Germany, intensive work is being done on QKD networks*" (FOIS, 2021, p. 3). However, the findings also show that nations are aware of QKD's limitations around cost, security, and distance and are therefore not relying on this as a sole solution. The ANSSI *Technical Position Paper: QKD* describes these limitations, including "*the complex and cost-intensive acquisition, the large number of demonstrated side-channel attacks against QKD devices, the limited range and the lack of end-to-end security over longer distances are considered problematic*" (ANSSI, 2020, p. 1), and in recognition of these QKD limitations, all documents advocate for the use of quantum-resistant cryptography as the "*preferred way*" to ensure protection.

Transitioning to quantum-resistant algorithms

All documents describe the necessity and intent to develop, test, and implement quantum-resistant cryptography to ensure the future security of national information and communication systems. For example, ANSSI's document, *Views on the PQC Transition*, states, "*a profound change of today's public key cryptography towards quantum-resistant algorithms should be globally initiated to anticipate a possible collapse of our current cryptographic infrastructure*" (ANSSI, 2022, p. 2). Transitioning to quantum-resistant cryptographic algorithms is highlighted throughout the findings as critical to ensure data protection now and into a quantum computing-enabled future, as stated here by the FOIS, "*Due to the urgency of migrating to quantum-safe solutions, migration to post-quantum cryptography should therefore be a priority*" (FOIS, 2021, p. 63).

The findings also confirm that quantum computing will have a small impact on symmetric algorithms and that nations should start using longer keys for symmetric encryption to mitigate this threat now. For example, the FOIS's publication *Quantum-Safe Cryptography – Fundamentals, Current Developments, and Recommendation*s includes the following advice, "*if long-term protection of data is important, a key length of 256 bits should therefore be provided for new developments in which a symmetric encryption algorithm is to be implemented*" (FOIS, 2021, p. 27).

Encouraging the adoption of PQC in vulnerable areas is described as a key priority for all national governments. For example, Canada's *National Quantum Strategy* states this intention as, "*Work…to support the adoption of post-quantum cryptography in technologies vulnerable to future quantum-enabled threats*" (Government of Canada, 2022, p. 14). However, it is also seen that transitioning to post-quantum algorithms will raise challenges. Firstly, the impact transitioning to quantum-resistant algorithms will have on developing further quantum technologies is unknown, as discussed by Australia's National Science Agency in *Growing Australia's Quantum Technology Industry*, "*Experts are currently divided on whether these algorithms will complement or disrupt the opportunity for QKD in the long-term*" (CSIRO, 2020, p. 24). Secondly, the time it will take to transition is highlighted by several documents as possibly problematic due to the need to operate legacy systems alongside new technology. Canada's *National Quantum Strategy* describes this challenge, "*The interoperability of existing and new systems will also be a major issue, as transitioning to new cryptographic technologies may take years*" (Government of Canada, 2022, p. 8).

Therefore, there is a need to prioritise the replacement of legacy hardware, applications, software, and IP with those that support cryptographic agility, and hybrid implementations are promoted in most national strategies. For example, the US *National Cybersecurity Strategy* describes this need to replace existing systems to support transitioning as, "*We must prioritize and accelerate investments in widespread replacement of hardware, software, and services that can be easily compromised by quantum computers*" (The White House, 2023, p. 25).

The findings show that the need to use hybrid solutions for a period of time while transitioning to a quantum-safe world is now universally accepted. These hybrid solutions are proposed in several ways:

1. The findings show a period of expected overlap whereby current and post-quantum algorithms will be used. For example, “The ANSSI recommends an overlap of current and post-quantum algorithms, with a progressive phase-out of the former” (ANSSI, 2022, p. 4).

2. Combining QKD with classical cryptography as a viable hybrid solution is proposed throughout the documents, as using QKD or quantum cryptography alone is not recommended. For example, “QKD should only be used in hybrid mode with classical and post-quantum key agreement schemes” (FOIS, 2021, p. 55).

3. Running two separate parallel networks (classical and quantum) in tandem is also seen as a possible solution, for example, “invest in a parallel infrastructure for secure communications…using quantum technologies” (DIST, 2023, p. 8).

The findings indicate an urgent need to start transitioning to quantum-safe systems now to avoid the known potential threats that quantum computing may pose, as described by Germany’s FOIS, “*BSI believes that it is already urgently necessary to take appropriate measures to switch to quantum-safe schemes”* (FOIS, 2021, p. 54). In response, a minority of nations have chosen not to wait for post-quantum algorithms to be standardised and have already issued recommended transition steps to post-quantum algorithms. For example, the FOIS state, “*Since the protection of long-term secrets may require timely action, BSI decided in late 2019 not to wait for NIST’s decision…BSI has initiated the migration to post-quantum cryptography and published initial recommendations*” (FOIS, 2021, p. 62).

While most nations are more conservative in their approach to transition and have yet to begin this process, all findings agree that it is possible to start the preparation required for a smooth transition immediately. For example, the New Zealand NCSC *MSP Supplier Panel Update* (2022) includes one step for immediate action, “*Use longer keys for symmetric encryption…Can do this now!*”. Another initial step outlined for nations to take when securing against quantum computing-enabled threats is the identification of the most vulnerable national systems and data as described in a proposed action here by Canada’s National Quantum Strategy, “*Identify information currently held by the Government of Canada at greatest risk if quantum technologies break currently used encryption protocols and develop and implement a plan to secure it”* (Government of Canada, 2022, p.14).

Investigation of the security aspects of emerging quantum technology both to mitigate any negative impacts and to take advantage of their potential ability to protect national infrastructures is seen as important, and some research is underway. For example, the European Commission’s Strategic Research Agenda of the Quantum Flagship highlights the need to look further at QKD security for defensive reasons as, “*Research on the security of implemented systems (both fibre and free-space), including methods of attacking QKD systems and how to prevent such attacks, is…very important”* (European Quantum Flagship, 2020, p. 25), and the *Cybersecurity Strategy for Germany 2021* describes how they will research the deployment of systems based on quantum technology to provide a high level of IT security, “*Research will be carried out into the effects of quantum computing on cyber security and technological innovations will be used for greater cyber security”* (FMIBC, 2021, p. 69).

To ensure national security, it is clear from the findings that further research is required in all areas of quantum technology purporting to secure systems. This includes post-quantum algorithms, QKD, and

quantum algorithms, as they are all still largely untested. The security of these solutions against implementation attacks is uncertain, and many unresolved questions require further investigation to instil confidence in their ability to secure future systems efficiently. For example, Germany's FOIS discusses some unanswered questions,"*are there cryptographically relevant quantum algorithms that require fewer qubits? Can cryptographic attacks be accelerated using special-purpose quantum computers?*" (FOIS, 2021, p. 63).

5.3.2.3 Protecting the economy from the impacts of emerging quantum technology

The findings show a need for nations to protect their economies from the impacts of emerging quantum technology. Safeguarding the stability of the global economy from the cybersecurity risks to cryptographic algorithms is clearly emphasised as enabling secure digital environments is critical to economic stability and success, as shown in the Government of Irelands *National Cyber Security Strategy*, which states, "*Our economic success is therefore closely bound up with our ongoing ability to provide a secure environment*" (Government of Ireland, 2019, p. 9).

However, the risk of being left behind and missing out on the economic benefits of quantum computing is also prevalent throughout the documents analysed, as nations believe that science and technology innovation are "*cornerstones*" to national prosperity and emerging technology is recognised as a significant opportunity for economic growth. For example, *Te Rautaki Matihiko mō Aotearoa – The Digital Strategy for Aotearoa* states, "*digital and data-driven technologies offer huge opportunities to grow Aotearoa New Zealand's economy in equitable, sustainable, and world-leading ways*" (NZ Government, 2022a, p. 29).

All documents acknowledge the potential for quantum technologies to significantly impact national and global economies. The belief that quantum will drive innovation and subsequent economic growth is widespread. For example, the UK *National Quantum Strategy* states, "*quantum technologies will offer a step-change in performance across a wide range of applications and are enablers to wider innovation across the economy, with £100 billion of expected benefits estimated globally in the coming decades*" (DSIT, 2023a, p. 42).

There is a sense of "*urgency*" and great "*ambition*" expressed when discussing the need to "*realize the promise of quantum technologies*". For example, the Australian Government's *National Quantum Strategy Consultation Paper* states they have, "*ambitions, urgency and commitment*" when discussing building a quantum ecosystem, and the findings also show many nations are investing in quantum technology and quantum science research to "*future-proof*" their economies and "*encourage economic opportunities*" in this space (DSIR, 2022, p. 8).

Protecting the stability of the cyber insurance industry is another consideration highlighted in the findings to ensure economic stability should a "*catastrophic cyber incident*" impact any nation. For example, the US *National Cybersecurity Strategy* describes how preplanning support for that industry would allow market certainty in the event of a large-scale incident and make the nation "*more resilient*" as follows, "*in the event of a catastrophic cyber incident, the Federal Government could be called upon to stabilize the economy and aid recovery…The Administration will assess the need for and possible structures of a federal insurance response to catastrophic cyber events that would support the existing cyber insurance market*" (The White House, 2023, p. 22).

The findings demonstrate that quantum technology is evolving rapidly. All documents recognise the quick speed and growth of the quantum evolution and describe an "*expectation that this trajectory will continue*". Australia's *National Quantum Strategy Consultation Paper* explains this fast growth, "*Quantum is growing quickly, with the market for some technologies projected to grow at a compound annual growth rate of more than 30% over the coming years*" (DSIR, 2022, p. 14).

Nations believe that now is the time to escalate the "*scale of effort*" and "*commitment*" in developing quantum technologies both to harness the economic benefits and address the cyber threats that quantum may pose. As described by Canada's *National Quantum Strategy* in stating, "*enhanced scale of effort and collaboration are critical to realize the promise of quantum technologies"* (Government of Canada, 2022, p. 17). However, the findings also caution that the economic benefits of quantum technology development must be balanced with the new risks this technology may pose to society, as stated by the US *National Strategic Overview for Quantum Information Science*, "*an appropriate balance between growth and risk can provide long-term benefits*" (NSTC, 2018, p.11).

5.4 Conclusion

Chapter 5 reported the findings derived from interviewing NZ cybersecurity and business leaders to determine levels of organisational preparedness to face potential quantum computing-enabled cyber threats and the analysis of a group of documents determining possible stances that the NZ Government could take domestically and internationally when addressing these threats.

The findings describe several main themes that will influence cybersecurity preparedness in a quantum computing-enabled world. Chapter 6 will further discuss these findings, linking them to the literature review and existing theory and using the results to answer the main research question and sub-questions posed by this study.

Chapter 6: Discussion

6.1 Introduction

Chapter 5 presented the findings from the interview and document analysis processes. These findings were obtained using an RTA method, as presented in Chapter 4. The aim of Chapter 6 is to discuss the findings presented in Chapter 5 and describe their relationship to the issues of quantum computing-enabled cyber threats outlined in the literature review. The main research questions and sub-questions introduced in Chapter 1 are also answered.

This chapter comprises six sections. Section 6.2 answers the first research question and discusses how the findings reflect, advance, or contradict previous relevant research and theories presented in the literature review. Section 6.3 answers the second research question, and Section 6.4 satisfies the aims of this study by answering the third and final research question. Additionally, in alignment with a study undertaken through the lens of classical pragmatism, Section 6.5 presents a discussion on practical preparation guidance for NZ organisations based on the study results.

6.2 Research Question 1

Sub question 1. How aware of quantum computing cybersecurity threats are critical NZ organisations?

Answer:

The findings show that NZ organisations have a low level of awareness of the cyber threats posed by quantum computing and any potential mitigations for these threats.

Lifting the awareness levels of NZ organisations should begin immediately in alignment with the international efforts underway in this area, as seen in the document analysis results. Sufficient awareness levels are the first necessary step in adopting new technology. It will be critical for NZ organisations to adequately undertake preparation to respond to the potential threats and take advantage of economic benefits and new security technology that quantum computing may enable.

Sub question 2. How are NZ organisations currently planning for quantum computing cybersecurity threats?

Answer:

The findings show that NZ organisations are not currently planning for the potential cyber or ethical threats posed by quantum computing.

The current overwhelming levels of cyber risk in the landscape mean cybersecurity functions operate predominately reactively in NZ organisations. There is little to no cybersecurity resource available within these organisations to proactively plan or prepare for future threats despite knowing that a more proactive stance would be ideal. Immediate cyber threats and system vulnerabilities take priority over strategic or long-term preparation, and the sheer number of immediate threats and new daily vulnerabilities seen in 2024 ensures that little capacity remains for anything other than a reactive response to these challenges.

While most NZ organisations have cybersecurity planning in place, they do not prescribe improvement activities that extend beyond the short to medium term. Additionally, these improvement activities are not executed robustly due to the high levels of daily reactive response work that consumes all available resources.

The literature review highlighted how the nature of quantum computing threats may lead to a level of inertia from organisations and prevent preparation (DigiCert, 2019), and the results of this study strongly confirm this. However, the findings also suggest NZ organisations may be even further behind than others globally, as while only 40% of businesses internationally were found to be preparing for these threats, no participants in this study were aware of any NZ organisations currently preparing or planning to prepare for these threats.

The lack of preparation for quantum-enabled cyber threats puts some NZ organisations at risk today as sensitive data encrypted using standardised algorithms such as RSA may already have been harvested by adversaries for later decryption by quantum computers. Furthermore, failing to start the preparation for these threats may mean NZ organisations run out of time to protect themselves adequately. The literature review confirms that preparation will entail significant changes to current systems and may take up to 10 years to implement fully. Although the timeframe for these threats to eventuate in the wild is unknown, the literature and data analysis findings both concur that there are clear indications that this could occur within the next decade.

Research Q1. How prepared are NZ organisations to face quantum computing-enabled cyber threats?

Answer:

NZ organisations are not currently sufficiently prepared to face quantum computing-enabled cyber threats. Existing strongly skilled but scarce cybersecurity resources in NZ may ensure a reactive response mitigates some potential negative impacts; however, many NZ organisations have yet to adequately prepare for quantum computing-enabled cyber threats. If further efforts to reduce current cyber risk and prepare for these cyber threats are not undertaken shortly, the resulting impacts may include widespread business disruption, increased personal and professional stress levels, harm from sensitive data breaches, and significant financial loss. Existing ethical concerns, such as the increasing digital divide and reduction of individual data privacy, may also be exacerbated.

The prevailing high-risk landscape ensures NZ organisations are underprepared for future threats as they struggle to manage the current levels of cyber risk. A lack of strong governance mechanisms, including unclear accountability and responsibility for cybersecurity and ineffective risk management processes, has resulted in an overall level of cyber maturity that is too low to combat either current or future threats. Not applying enough of a strategic lens to cybersecurity planning, a belief in the inevitability of cyber-attacks, and a low-trust environment all contribute to NZ organisations' limited ability and drive to prepare for the threats that emerging technology, such as quantum computing, may pose.

The results of this study find an urgent need to address the high levels of cyber risk in the NZ landscape. NZ organisations cannot comfortably keep up with the threat levels they are operating in, and NZ cybersecurity professionals are overwhelmed in trying to keep NZ organisations protected under current

conditions. Reducing the current cyber risk levels while simultaneously lifting organisational resiliency across NZ will be critical before the emerging issues of tomorrow, such as quantum computing-enabled cyber threats, arrive to complicate the landscape further.

Numerous factors were found to be contributing to the high levels of cyber risk in NZ, including the volume and novelty of cyber-attacks, the rate of technology change, skill shortages, the reliance on legacy technology and third-party providers, and insufficient cyber governance and cyber maturity levels. However, all of these contributing factors can be addressed to improve the overall landscape and enable greater protection for NZ organisations today and in a quantum computing-enabled world.

All findings from this study suggest that the NZ Government must strongly advocate for organisations to begin preparing for the threats posed by quantum computers immediately, and consider mandating this preparation for nationally significant organisations to protect national security and the economy from harm. Securing a strong and secure digital future will also require investing in greater quantum capacity and capability, including ensuring the accessibility of quantum infrastructure and supporting foundational quantum research and industry initiatives.

6.2.1 Addressing the High-Risk Landscape and Lifting Cybersecurity Maturity

This study found that the current high cyber risk operating levels have impacted NZ organisations in several ways, including limiting the ability of organisations to sufficiently address longer-term threats, ensuring an uneasy reliance on third-party providers, creating a sense of helplessness around combatting cyber threats, and contributing to elevated levels of personal burnout in the cyber industry. To reduce risk, grow cyber resiliency, and prepare to effectively defend against the cyber threats that quantum computing may bring, NZ organisations and the NZ Government must focus on getting minimum basic cybersecurity controls implemented sustainably, lifting overall cyber maturity, increasing quantum threat awareness, and finding ways to disseminate timelier and more contextually relevant threat intelligence to cybersecurity professionals.

6.2.1.1 Getting the basics right

Cyber security maturity levels across NZ organisations are currently too low. Participants in this study felt NZ took longer than other nations to recognise the seriousness of cyber threats, and whilst cyber is now recognised as a top risk in most organisations, the maturity levels needed to ensure they are adequately protected from these risks have not caught up. While there is an urgent need to move organisations from a reactive to a proactive stance in cybersecurity and drive more effective planning for the threats that quantum computing will bring, this cannot occur without addressing the current overwhelming high-risk landscape and lack of sustainable basic security hygiene. Therefore, the initial focus must be increasing minimum basic security hygiene across the NZ landscape. While many NZ organisations have already implemented significant cybersecurity mechanisms within their environments, it is clear from the findings of this study that some of the basics are not universally or sustainably implemented.

The findings of this study suggest that organisations must go back to the basics and invest more time, people, and money to improve the quality of baseline cyber controls. Foundational security controls, such as creating inventories of all hardware, software, and data within an organisation, are critical to understanding what assets require protection and where they are located (CIS, 2021). If these steps are

not undertaken well, how much is spent on further technology protections downstream becomes irrelevant as the investment may be focused on the wrong areas. Additionally, if these actions are implemented in a non-sustainable way, as described by this study's findings, they are quickly rendered inaccurate and time-consuming to maintain. This ongoing maintenance adds to an already overwhelming workload for security teams. Security professionals in NZ are currently struggling in environments with limited visibility of risks and will continue to act purely as firefighters on the front line if implementing basic controls that increase the visibility and manageability of the environment is deprioritised. Security resources must be allocated sufficient time to complete tasks such as maintaining an accurate view of technology inventory to ensure a sturdy foundation is created for building further cybersecurity maturity.

The document analysis findings concur with the literature review in outlining initial steps organisations can undertake immediately to start preparing for quantum computing-enabled cyber threats. These steps start with identifying and documenting where cryptographic algorithms are currently used within an organisation (NIST, 2020), which can be undertaken prior to the threat being seen in the wild or any solutions being standardised. However, no study participants knew of an existing cryptographic inventory in the organisations they had worked for in NZ.

Creating greater visibility of environments through technology and process inventories is a foundational activity specified in most cybersecurity frameworks and guides seen in the literature review (CIS, 2021; ISACA, 2021; NIST, 2020). Emphasising a return to focusing on getting these basics in place would assist in reducing the current overwhelming cyber risk and equally aid in starting to address emerging threats, including the cryptographic threat posed by quantum computing. Identifying and thoughtfully implementing activities that provide immediate and future cyber resilience is critical in the current resource-constrained environment. Therefore, foundational actions such as fit-for-purpose employee training, robust backups, contingency plans, and robust inventories that simultaneously address immediate cyber risk in NZ organisations and promote preparation for quantum computing-enabled threats should arguably be the initial focus of cyber improvement investment.

6.2.1.2 Lifting cybersecurity and quantum technology awareness

The document analysis highlighted the high priority that some nations place on lifting general knowledge and awareness of quantum-enabled technology and its cybersecurity and societal impacts. This study found that NZ will also need to prioritise this activity immediately to successfully enable organisations to remain secure from the cyber threats these technologies may pose, as awareness and understanding of these threats are currently too low. While some participants were tangentially aware of the potential impact of quantum computing on cryptography, many participants had no knowledge in this area, and most could not describe the threat in any detail or discuss any potential mitigations for it.

Greater awareness of quantum-enabled computation and communication will also be necessary for NZ organisations to take advantage of the economic benefits and cyber security protection these technologies could offer. The literature describes how it will be necessary to use quantum technology to fully protect against quantum technology threats (Wallden & Kashefi, 2019); however, the interview results highlighted extremely limited awareness of using specific quantum technologies for cyber defence in the NZ landscape. The use and development of quantum solutions are still evolving globally; however, the document analysis clearly outlined how other nations are already promoting and investing in these

solutions, such as QKD networks, for secure data communication. These findings suggest NZ will be left behind other nations in adopting emerging cyber defence technology if greater awareness of these solutions is not pursued.

The theory of DOI outlined in Chapter 1 describes how organisations must progress through five stages to fully adopt new technologies. Understanding and awareness must come first before positive or negative opinions can be formed about the use of the technology, and then a decision is made to adopt it or not. When viewing these results through the lens of the theory of DOI, it is obvious that NZ organisations are only at the first of the five necessary steps to quantum technology adoption. Greater awareness around all aspects of quantum computing, including the cybersecurity threats and the potential defence options it presents, will therefore be critical to ensure organisations progress further through this adoption process and arm themselves sufficiently for a future landscape where quantum computing is active.

This study found several specific areas requiring focus in the NZ landscape to enable cybersecurity and quantum computing awareness and knowledge. These included increasing board-level cyber knowledge, improving the translation of research outcomes, and changing the way quantum computing and related technology threats are framed.

6.2.1.3 Board/senior leadership understanding of quantum and cybersecurity risks

The literature review highlighted the importance of senior leadership understanding in ensuring adequate support, resources, and budget are allocated to cybersecurity (Chang et al., 2020). However, the interview findings in this study clearly show limited knowledge and skills in cyber at the board level of NZ organisations. Even more concerning is that there does not appear to be any intent to grow knowledge or representation of cybersecurity professionals at this level in NZ despite the increase in the severity of cyber risk, which is a leading business risk.

Organisations are increasingly expected to have cyber expertise at the board level internationally. For example, The United States Congress has put forward legislation requiring publicly traded companies to disclose whether any board member has “expertise or experience in cybersecurity” or, if not, how the board has taken cybersecurity into account in support of the business (Cybersecurity Disclosure Act, 2021). Boards and senior leadership need to fully understand the benefits and risks of emerging technology, such as quantum computing, to drive an organisational culture that supports long-term economic success and ensures that emphasis is placed on security. As the boards of NZ organisations are not voluntarily gaining this expertise, the NZ Government may need to enact similar legislative pressure to drive cybersecurity skills to the highest and most influential parts of NZ organisations.

6.2.1.4 Translating knowledge from academia to industry

The literature in Chapter 2 demonstrated that the negative impacts quantum computers will have on current cryptographic schemes have been well understood and documented for many years (Cloud Security Alliance, 2018; Mailloux et al., 2016; Wallden & Kashefi, 2019). It also highlighted how various solutions to these threats, such as QKD and alternative algorithms, have been explored for almost 20 years (Elliott et al., 2005; NIST, 2020). However, despite this documented history, the findings of this study show that this knowledge has not fully transferred to the people who need to understand and prepare for these risks in NZ organisations. This delay in translating and communicating research outcomes to practical knowledge

is problematic as it results in a lack of action from the areas of society, such as private organisations, that could benefit from understanding and implementing these insights.

It is clear from the findings in this study that the journals through which current academic research is primarily communicated are not a source of information for industry professionals. Rather, cybersecurity professionals in NZ organisations report receiving much of their information through vendors. This means a significant portion of the information they use for decision-making is likely biased as it is limited to research that can be commercialised in products for a profit. Not all research is ready or appropriate for industry consumption; however, many valuable and validated insights, such as the confirmed threat to cryptographic algorithms by quantum computers, are. Closing this knowledge gap by finding alternative methods to disseminate key research may allow the industry to be more prepared and benefit from cybersecurity advancements early.

Solutions such as introducing liaison roles either in universities, centres of excellence, or through government agencies, whose sole purpose is to communicate to industry the outcomes of verified research that may impact these areas, could assist in ensuring the important messages are received. In this study, NZ organisations strongly preferred personal interaction and communication of information, ideally in their place of operation and in a language that makes sense to them. Responding to this need for different mechanisms and mediums of knowledge transfer will be important to promote a wide understanding and adoption of safety solutions for emerging quantum computing technology in NZ.

6.2.1.5 Making quantum computing and cybersecurity understandable

This study found that the technically savvy participants struggled to comprehend the fundamental concepts of quantum computing technology, finding it confusing, overly theoretical, and ultimately difficult to understand. This lack of understanding means NZ cyber professionals are reluctant to discuss the new threats or advantages of quantum technology with other senior leaders in their organisations who may be less technically savvy. Therefore, to enable greater awareness, acceptance, and adoption of this technology and the cyber threats it presents, new language techniques to demystify it and make it a more familiar part of the everyday linguistic palette are required.

As discussed in the literature review, the oft-quoted analogy of “Schrodinger’s cat” attempts to describe the paradox of quantum superposition in a friendly manner, but in turn, it highlights quantum’s more unfamiliar behaviour and may make it seem even more esoteric (Grinbaum, 2017). Therefore, participants in this study suggested that referring to quantum computing as a “resource” that enables certain solutions may drive more productive conversations. However, while simplifying quantum computing concepts may be helpful to reduce perceived barriers to understanding the technology, it is not the full solution as resources such as “entanglement” and protocols such as “QKD” must be understood in terms of what they can offer organisations. Driving these new concepts into the realm of common technology discourse rather than avoiding them will be necessary for the immediate conversations that will enable NZ’s preparation for a quantum-enabled computing world; however, how these new concepts are communicated needs further consideration to ensure they are approachable.

To engage NZ organisations and the broader society in the implications of quantum technologies, a common and accessible language is clearly required. Finding innovative methods to disseminate scientific

knowledge about quantum phenomena and how this phenomenon is applied to technological advancements requires further investigation as it is an under-researched area; however, the results of this study indicate some potential guidelines for communication in this space. Quantum technology and threats should be presented in an honest and easy-to-understand manner with thoughtful use of scientific terms where necessary. Discussions should focus on specific technologies and resources, such as QKD and known quantum-resistant algorithms, rather than general quantum science phenomena. This focus may ensure greater interest and engagement by making quantum computing solutions "real" rather than just "incomprehensible ideas" to the NZ organisations who must ultimately implement them. Additionally, all communication should be contextually relevant to the audience by focusing on impacts, advantages, disadvantages, and solutions applicable and available to NZ organisations. Describing use cases specific to each industry context may help to make the technology more relevant to the day-to-day operations of cyber professionals.

The findings also show that taking a balanced approach when discussing the potential disruptive potential of quantum computing will be important. NZ organisations may ignore unsubstantiated claims or unrealistic proposals to defeat potential threats if they feel they do not have the agency or ability to act on these. Finally, trust is seen to be crucial in the findings of this study, and therefore, fully transparent communication about all the possible benefits, limitations, and threats quantum technology may bring is essential to build trust and allow organisations to act autonomously on this information.

6.2.1.6 Gaining timelier and more relevant cyber threat information

Reducing the current reactive cybersecurity workload of NZ organisations and effectively enabling the preparation for quantum computing-enabled cyber threats require reliable cyber threat intelligence. The interview findings heavily stressed the value of quality information, with participants describing it as critical to preparing for and defending against cyber threats. However, this study found that solutions to provide NZ organisations with timelier, trusted, and contextually relevant information about both current and future cyber threats in the landscape require work. The current sources of threat intelligence available are seen to be either biased or too slow to be effective and allow organisations to adequately protect themselves.

One solution posed by the participants was to develop a consolidated and near real-time view of current attacks in the NZ landscape. This portal could display all available information about the nature of the attacks, potential mitigations, and ongoing impacts, and it could be shared as widely as possible to assist those attempting to stay prepared. However, developing such a resource would only be possible if private and public organisations, including the government agencies responsible for national cybersecurity, committed to openly sharing threat information as quickly and transparently as possible. Enabling this would require a significant cultural shift from the current low-trust environment seen through the findings in this study to one of much more openness. Security concerns are often cited (CERTNZ, 2024) as a reason for not allowing the wide publication of cyber-attack information. This concern is valid as all online information can be hacked and used for negative as well as positive outcomes; however, balancing the potential gains of widespread, timely and contextually relevant information against the potential downsides a security breach of this information may pose should be considered.

Another option to improve this area would be to increase the capacity of government cybersecurity agencies and subsequently allow a greater range of organisations to access the information and resources

currently supplied to only nationally significant organisations (NSOs) or MSPs with an existing relationship with the NCSC. For example, in 2023, the NCSC issued a brief communication highlighting the threat that quantum computing poses to current cryptographic algorithms and their high-level expectations of how organisations should respond to this threat (GCSB, 2022a). However, this communication was sent to an extremely limited subset of individuals and organisations, and a much broader dissemination of critical information about future threats is needed.

Ensuring sufficiently broad capacity in government agencies to cover all the various industry nuances required to supply more contextualised and useful threat intelligence for NZ organisations may be challenging. Therefore, it may be necessary to grant trusted industry individuals appropriate government security clearances to interpret critical cyber intelligence for their industry context effectively. Once again, this change requires additional trust; however, allowing greater industry input may increase the value and timeliness of the cyber information transfer from national and international intelligence to domestic organisations.

6.2.1.7 Practical information on implementing quantum-safe solutions

Current literature, along with the document analysis findings, also shows that more information is required regarding the practical implementation of quantum-safe solutions. Necessary actions for generating this practical information and ensuring it is useful for NZ organisations include the continued support and funding of quantum technology research in NZ, keeping abreast and fully engaged in international research, and providing wide access to test beds for sufficient experimentation of use case implementations.

Conducting further research into exactly how proposed quantum-safe solutions would integrate into NZ's organisational infrastructure is also required so that successful case study examples are available for wide dissemination. For example, the findings show there is currently no understanding of exactly how much technology currently resides within NZ organisations that will struggle to run newly proposed quantum-safe algorithms. Therefore, conducting low-risk test implementations and collaborative studies of these specific features in NZ organisations would be incredibly useful in minimising disruption and helping a wide range of industries and organisations to clearly understand the logistics of implementing quantum-safe solutions.

In summary, NZ could increase the value of cyber threat information and enable more effective preparation for current and emerging quantum computing cyber threats by focusing on growing trust in the NZ cybersecurity landscape, looking for new solutions to disseminate cyber intelligence, developing more and closer relationships between NZ Government cyber agencies and organisational representatives, and supporting quantum computing research.

6.2.2 Strengthening National and Organisational Cyber Governance

The literature review highlights how strong cybersecurity governance is important to increase cyber resiliency (Manning, 2020; Trager, 2022). Therefore, effectively governing cybersecurity and emerging technologies, such as quantum computing that may impact cybersecurity, must be a priority concern. However, this study found that current governance mechanisms in NZ organisations are insufficient to support increasing cyber resiliency or cyber threat preparedness. The findings highlight how greater governance can be achieved both at national and organisational levels in NZ by focusing on driving clearer

accountability and responsibility for cybersecurity, improving cybersecurity framework use, valuing the cybersecurity function more, creating a culture of quality and challenging existing cyber incident acceptance levels, demonstrating strong leadership, and improving current risk assessment and management processes.

6.2.2.1 Clarifying and growing cybersecurity accountability and responsibility

This study highlighted a lack of clear responsibility and accountability for cybersecurity within the NZ landscape, driving greater cyber risk and resulting in successful cyber-attacks. This also extended to a lack of ownership when discussing the preparation for quantum-enabled cyber threats. The complexity of the technology landscape, which involves a full ecosystem of interdependent systems including multiple third-party providers and product supply chains, makes assigning accountability incredibly difficult. However, this critical cyber governance aspect must be improved in NZ to reduce cyber risk and the inappropriate assigning of blame for failures.

Levers highlighted in this study that could drive greater cybersecurity accountability in the NZ landscape include clarifying cybersecurity roles and responsibilities, managing third-party contractual agreements, introducing greater government, industry, and regulatory obligations, and framing and communicating cyber risks mindfully.

6.2.2.2 Clarifying organisational cybersecurity

One function of cyber governance is to ensure clear roles and responsibilities exist for managing cyber risk. Overall accountability for business risk sits with the board or senior leadership team of an organisation, and therefore, they must understand their duties regarding cyber risk and ensure cyber risk is governed, managed, and reported on appropriately within the business. This includes the specification and sufficient support of organisational roles to manage cyber risk appropriately.

Cyber security roles and responsibilities are commonly communicated via tables that map individual roles and systems against the categories of responsible, accountable, consulted, and informed (RACI). While some NZ organisations report using basic RACI for cybersecurity, this area requires a more granular focus, as the study findings show that current RACI governance is insufficient to ensure that everyone in an organisation is held accountable for cybersecurity.

NZ organisations must make more effort to assign ownership of all relevant systems to individual roles within their organisations to achieve greater clarity on cyber security responsibilities. All actions that protect these systems must be clearly defined, monitored, and delegated to the role responsible for undertaking them. An example of how RACI may be defined to protect individual systems from the threat to cryptographic algorithms that quantum computing poses is provided in Table 9. In this example, the head of customer care is accountable for ensuring the transition to quantum-safe algorithms in the customer relationship management system. However, the IT analyst is responsible for undertaking this task.

Table 9

System Name: Customer Relationship Management System

System owner: Head of customer care

Action	Responsible	Accountable	Consulted	Informed
Maintain data inventories	IT analyst	Head of customer care	HR analyst Customer care team leader	Risk manager Chief information security officer
Maintain cryptographic protections	IT analyst	Head of customer care	HR analyst Customer care team leader	Risk manager Chief information security officer

The findings of this study agree with the current literature in determining that cybersecurity must be the responsibility of everyone in an ecosystem. However, to achieve this level of ownership, each role must be contractually obligated to perform their duties in this space and understand the consequences of not performing them. Only in this manner, with true visibility and ownership across all areas of the technology architecture, can cyber risk be effectively managed.

6.2.2.3 Defining third-party contractual agreements

There is evidence that outsourcing IT contributes to greater cybersecurity risk exposure (Grody, 2020) and additionally complicates the assignment of accountability and responsibility for cyber risk in organisations. These unclear cyber risk boundaries were apparent in the findings of this study, where participants attributed recent cyber breaches to unpatched technology systems that spanned internal and third-party environments and where no one could determine ultimate security responsibility. Instead of, or in addition to, government mandates for MSPs, organisations must have strong contractual agreements in place with their providers that outline minimum acceptable security standards, responsibilities for implementing, maintaining, and reporting on these security standards, and the penalties for failing. Demanding that vendors and partners show evidence of security certification and clearly agree on levels of transparency and communication around cyber incidents is also necessary to build trust and ensure clear lines of accountability and responsibility are in place for securing the wider environment. With respect to quantum-enabled computing threats, outlining which party is responsible for ensuring secure cryptographic protection remains in place and how emerging threats and their mitigation actions are communicated and reported on requires clarification in all agreements. NZ organisations are disappointed in the level of service received from their cyber partners, and therefore, proactive efforts from all parties to lift the quality of service and set and agree clearer expectations and realistic service level agreements are required to improve this situation.

With clearer cybersecurity RACI throughout the entire technology supply chain, there is an opportunity to further reduce the “blame” culture that still exists in the cyber environment in NZ, which is apparent in the aftermath of successful cyber-attacks. Setting clear expectations around the protection standards that must be met, who must meet these, and who must ensure they are met would enable the accurate assignment of appropriate judgement and penalties should failures occur, thereby reducing widespread finger-pointing when failures happen. Therefore, along with strengthening organisational RACI governance, the NZ Government also has a clear role in setting minimum standards for the national cyber security ecosystem.

6.2.2.4 Introducing greater regulatory obligations

It was overwhelmingly clear in the findings of this study that NZ does not have sufficient regulatory levers in place to effectively change organisational behaviour and promote the increase of cyber maturity required to reduce cyber risk. Asking NZ organisations to voluntarily attempt to implement cybersecurity frameworks and controls without providing sufficient additional support has only been partially successful, as seen by the low basic security hygiene levels described by some of the study participants. Additionally, where organisations in NZ have obtained a more secure cyber posture, it was seen to happen because of the need to comply with mandatory international regulations. More concerningly, many participants of this study felt that NZ organisations would not proactively take preparatory steps to protect against cyber threats, such as the threat to cryptographic algorithms that quantum computing poses, without these steps being mandated by the government.

Introducing more cybersecurity legislation is a trend seen internationally, as evidenced in the document analysis findings and the literature review. The findings of this study suggest that following this trend by introducing greater regulation for cybersecurity in NZ that specifies more punitive penalties for noncompliance would be largely supported as a measure to lift overall cyber maturity and support greater cybersecurity accountability.

Although strengthening national cyber governance and introducing legislative measures are being approached in varied ways internationally, some common areas are clear. Many governments are starting to regulate general cyber resilience more heavily. For example, Australia now requires critical infrastructure providers to adopt a risk management programme in which cyber resilience is a key component of overall operational resiliency. Greater regulation of cyber resilience is also reflected in the UK, the US, and the European Union (DORA Digital Operational Resilience Act, 2022), signalling that cybersecurity is now seen as a critical business issue and must be addressed holistically.

There has also been a significant increase in global organisational and senior leadership regulatory obligations. Examples such as the EU's DORA and the proposed US Securities and Exchange Commission (SEC) regulations (DORA, 2022; SEC, 2023) focus more on board and senior executive accountability for cyber risk. For example, in DORA, the board holds ultimate accountability for ICT risk, and this legislation specifies penalties for both the organisation and the individuals in these roles should they fail to ensure that the organisation is protected by appropriate security controls and processes. DORA also mandates employee training and requires organisations to measure and evidence their cyber risk. Similar obligations are required in the NZ landscape to drive greater accountability for cyber risk, and directors need a clear interpretation of cybersecurity accountability. Senior organisational leadership must not be able to delegate or deflect the ownership for cyber risk or cyber security management to technology teams. The NZ Government must clearly articulate specific cyber governance requirements for organisations that ensure senior leaders maintain oversight of all cyber risk and are obligated to ensure organisational operations remain protected. Introducing these measures may also drive the appointment of more individuals with cybersecurity skills at the board level and help increase the overall understanding and awareness of these issues at the top of NZ organisations.

In addition to emphasising board and senior executive accountability, governments internationally are imposing stricter controls on critical sectors and expanding the scope of industries regulated to include

MSPs and other third parties, such as payment providers (Australian Institute of Company Directors [AICD], 2023). The findings show that NZ organisations heavily rely on third-party managed services for cyber security, and therefore, NZ must follow the lead of other Western democracies by targeting critical industries and technology-managed services for further regulatory controls that specify minimum security maturity targets. This would assist in reducing the supply chain risk and increasing accountability for cybersecurity across the full landscape. The interview findings in this study describe how NZ organisations are already anticipating an increase in cyber regulation as no one feels that sufficient cyber maturity uplift will occur voluntarily, and therefore, actions to strengthen regulatory obligations should be prioritised.

6.2.2.5 Mandates for protecting against quantum computing-enabled threats

This study found that NZ cannot rely on organisations to voluntarily implement the measures needed to prepare for quantum computing-enabled threats, such as transitioning to quantum-safe algorithms. Therefore, it would be advisable for the NZ Government to mandate the transition to these algorithms, particularly for NSOs. As seen from the document analysis, this is already occurring overseas due to widespread recognition that transitioning to quantum-resistant cryptography will be important for maintaining national security and avoiding any negative impacts of quantum attacks on digital economies. Clear guidelines around the timelines to transition and the agreed standardised solution options should be articulated to all NZ industries as soon as the NIST standardisation process has signalled a firm solution direction. Further, a widespread mandate to transition should be considered, including every party operating in NZ's digital ecosystem.

Introducing greater mandatory requirements in cybersecurity may not happen smoothly, and the findings show that introducing more regulation will require mechanisms to evaluate and enforce these. The costs to implement new regulations may also be a hindering factor across many NZ industries; however, those industries that may struggle, such as healthcare, are also seen in the findings to need a strong push to lower cyber risk and ensure they are secured into the future (Robinson, 2023). Wide industry consultation will be important to ensure that any regulation introduced is understood and accepted. Additionally, the development and introduction of new mandates must also move at a pace fast enough to set initial high expectations and allow sufficient time for compliance to occur before penalties are imposed.

While the introduction of legislation can introduce challenges and is never perfect, previous research supports the findings of this study in describing that top-down regulatory mechanisms may be the most effective tool to enact change quickly (Tverskoi et al., 2022). This level of fast intervention is required in the NZ cybersecurity landscape to address the current overwhelming nature of cyber risk, and ensure organisations are prepared for a future driven by even greater computing power from quantum computing.

6.2.2.6 Framing quantum-computing enabled cryptographic threats

The findings describe how the responsibility and accountability for protecting the NZ landscape from quantum computing-enabled threats is currently seen as primarily a government issue due to the perceived scale of the threats and a belief that individual organisations cannot protect against them. The NZ Government must take ownership of protecting New Zealanders from quantum computing-enabled cyber threats to maintain national security and the country's economic stability. However, just as the responsibility for cybersecurity must be distributed throughout an organisation, it must also be distributed

between all public and private agencies operating in the NZ environment for a successful defence. Therefore, NZ organisations must also be accountable and responsible for preparing to defend against quantum computing-enabled cyber threats. To change the current prevailing attitude in organisations from "it's the government's responsibility" to "it's our responsibility", this study finds that how quantum-enabled cyber risks are framed must change.

This study confirms the findings from earlier research using CPT that suggested understanding and addressing risk, particularly under conditions of uncertainty, is challenging and impacts decision-making. For example, many participants described how the uncertain nature of quantum computing-enabled cyber risk made it too hard to consider.

The findings also support early research using CPT that described how the negative framing of potential risks led to decision-makers acting in a manner that was more risk-seeking (Bazerman, 1984). This was demonstrated in this study by interview participants exhibiting a clear inclination not to act and prepare for quantum computing threats when the outcomes of these threats were framed negatively. For example, when quantum computing threat impacts were described as extremely large or potentially existential in nature to the organisation, participants adopted an attitude of it being someone else's problem, and a lack of ownership was expressed. These findings suggest that using scare tactics to drive preparation for cyber threats and communicating the risks associated with quantum computing with negative terms or phrases such as "cryptopolypse" (Adams, 2013) or "quantum computing could break the internet" (Learner, 2023) seen in popular publications, will not work. Rather, framing the risk using positive outcomes and outlining the achievable and practical steps organisations can take to reduce the risk is indicated. This does not involve minimising the potential impacts, but rather avoiding outlining the potential threat scenarios too negatively.

An example of how the communication of the risk to cryptographic algorithms could be changed from a negative to a more positive framing to increase the organisational ownership for preparation is given as follows: Negatively framing the potential risk may be communicated by stating, "If quantum-resistant algorithms are not implemented, quantum computers will break all current PKI and render all of your transactions insecure", whereas positively framing this same risk could be communicated by stating, "Quantum computers will have the ability to break all current PKI; however, if your organisation transitions to quantum-resistant algorithms, your transactions can remain secure". According to this study, framing the risk more positively may drive more ownership of the issue and a more proactive response from NZ organisations.

6.2.2.7 Improving cybersecurity framework use

Both the literature review and the findings from this study highlight how the use of popular cybersecurity frameworks can help organisations increase cyber threat preparedness and lift cyber maturity. Cybersecurity frameworks, particularly the NIST CSF, were reported as widely used in NZ organisations. Unfortunately, despite this wide use, there is a lack of confidence in the practical benefit of using these frameworks to achieve greater organisational cyber resilience.

The interview findings concurred with the literature review in describing how the broad nature of the guidance within frameworks is challenging for NZ organisations to act upon. The frameworks specify

hundreds of high-level cybersecurity controls that must be contextualised and prioritised for each unique organisation. Additionally, they do not outline specific detailed actions and controls for emerging cyber threats such as those that quantum computing may pose. Most frameworks also measure progress by the number of controls implemented rather than by measuring the more meaningful business goal of cyber risk reduction. This study finds that this characteristic makes the tangible benefit of implementing each control unclear and difficult to communicate to decision-makers in NZ organisations.

NZ organisations are already finding it impossible to keep up with the number of daily urgent security updates and recommendations they receive from government advisories and vendors. Therefore, measuring cybersecurity success using a large framework with hundreds of potential security controls is reported as overwhelming, unachievable, and sometimes hard to justify. These findings suggest a need to rethink how NZ organisations promote and use these cybersecurity frameworks. Re-enforcing the wide use of a framework such as the NIST CSF is still warranted to ensure alignment with global standards and to drive awareness of the full cybersecurity domain, which requires consideration at a governance level. However, more specific and targeted guidance is required for NZ organisations to achieve greater cyber resiliency and drive cyber improvement programmes. Additionally, the measurement of cyber maturity must move away from assessing how many controls have been implemented against these frameworks and evolve to focus on measurable and visible risk reduction. This requires further investigation and developing skills and support tools that do not exist today.

Despite not being perfect, the findings also show that if a well-recognised framework such as the NIST CSF were to include specific preparatory actions for quantum computing, these would not be ignored. Expanding these frameworks to include a more strategically focused domain that specifies actions to combat quantum-enabled and other future threats may be one way to ensure that organisations focus on preparing for the future while simultaneously addressing active threats.

6.2.2.8 Valuing, supporting, and growing the influence of the cybersecurity function

Constantly defending against relentless cyber threats with scarce skilled resources and less control over outsourced security mechanisms, combined with a pervasive attitude of cyber breach inevitability, has led to increasing levels of burnout in NZ cyber professionals. Literature has highlighted the short tenure of cybersecurity professionals internationally due to unmanageable levels of overwhelm and fatigue (Nominet-Cyber, 2019; Tines, 2023). This study showed that increasing levels of fatigue and frustration are also present in the NZ environment. NZ has smart, skilled cyber professionals, many of whom have been in the industry for a long time. However, the findings show that some NZ cyber professionals feel undervalued and under-supported in their organisations and are suffering tangible personal impacts from attempting to keep up with the high-risk environment. If the culture of undervaluing the cybersecurity function in NZ organisations remains, organisations will risk losing more experienced professionals in a market already suffering from skill shortages.

This study found that security professionals in NZ organisations know where the greatest vulnerabilities lie; however, they require greater organisational support and influence to address these sustainably. Cybersecurity professionals must be seen as allies, partners, and leaders at the senior and board levels of NZ organisations. Framing cybersecurity as a strategic investment and as a positive differentiator that can grow customer trust and retention when effective may assist in gaining this necessary support.

Achieving a high level of organisational influence will require cybersecurity leaders to act as strategic partners by listening to organisational challenges and becoming as familiar with operational risks as they wish operational teams would be of cyber risk, demonstrating how to adopt a “whole of business” lens across risk. Additionally, if the cybersecurity function can move from a predominately defensive and reactive position to a proactive one that enables innovation, it may become more influential.

6.2.2.9 Creating a culture of quality in cybersecurity

Mediocrity is defined as “of only moderate quality; not very good”, and its synonyms include tolerable, middle-of-the-road, average, and indifferent (Collins English Dictionary, n.d.). This study found an acceptance of mediocrity across the NZ cyber security landscape. Mediocrity was demonstrated by the study participants in expressions of cyber threat acceptance, lack of ownership around cyber risk, and a blame culture. Some participants expressed frustration over the status quo; however, others did not seem aware of it. This suggests greater recognition of the problem and steps to encourage a change in culture to one of greater quality and excellence, which is required in the NZ cybersecurity landscape.

Many participants in this study stated how important customer data security was to their companies; however, there was also a strong report of “just doing enough” or even “not doing enough” when protecting against current and future threats to this data. This indicates that quality and security are not, in fact, embedded as core values in NZ organisations despite the recognition that cyber risk is now a significant business issue.

Quality initiatives may be placed behind maintaining continuity when organisations are under pressure (Shah et al., 2021). However, this approach is detrimental to NZ organisations’ long-term adaptability and resiliency to survive in an increasing threat landscape. During the COVID-19 pandemic, it was found that organisations that had strong cultures of quality navigated the unexpected and fast-moving landscape more successfully than those that did not have a strong quality foundation (Shah et al., 2021). Therefore, embedding a culture of quality may allow NZ organisations to better respond to the fast-moving technology changes and increased cyber threats they will face in a quantum computing-enabled world.

NZ must change its culture of mediocrity to one of excellence in cybersecurity and technology to achieve a more resilient cyber posture. While greater regulations should push cyber security maturity up, there is also a need for quality to be embedded in organisational culture to ensure any compliance-driven changes are implemented well. Leaders must support the notion that quality is important when securing technology by establishing standards of excellence and supporting continuous improvement. Additionally, employees must be empowered to deliver quality. Finally, organisations must apply pressure across their peer networks to reinforce high-quality expectations in cybersecurity, as this study demonstrates that peers can strongly influence NZ organisational behaviour.

6.2.2.10 Challenging cyber incident acceptance levels

This study’s participants exhibited a surprising and concerningly high sense of helplessness around addressing cybersecurity and protecting against cyber-attacks. NZ organisations appeared to be resigned to the inevitability of constantly suffering from cyber-attacks and their resulting harmful impacts, with some seeing it as the price to be paid for operating in the digital world.

The view that it is inevitable that all organisations will suffer a security breach is summarised in the oft-quoted phrase, “it’s not if, it’s when”. This phrase has been touted by cybersecurity experts internationally (AICD, 2024; Kolochenko, 2016) for many years to drive awareness in the landscape that nobody is immune to cyber threats. This message appears to have been successful, as evidenced by multiple participants in this study repeating the quote when describing the current NZ cyber threat landscape.

The resulting acceptance of cyber threats as ubiquitous has led to some positive shifts in NZ’s organisational culture, whereby the blaming and punishment of IT professionals for cyber-attacks is reported in the findings as somewhat, although not entirely, reduced. However, the findings also indicate that this message may be contributing to a perceived lack of agency in NZ organisations, and its continued use may be driving a reduction in proactive action to combat cyber threats. For example, rather than encouraging greater preparation and investment in preventative measures, the message of “it’s not if, it’s when” is seen in this study to be strengthening a shift away from the pragmatic acceptance that cyber-attacks are possible towards a more widespread feeling of helplessness against cyber-attacks. This sense of helplessness is seen to be leading to apathy and even less drive to prepare for future threats. For example, as described by some study participants, “Why bother?” preparing for a threat if an organisation cannot prevent the attacks from impacting them. This feeling of resignation was even stronger when discussing the possibility of quantum computing attacks, as many participants believed their organisations could not defend against threats of this scale.

Rather than working harder to prevent attacks and aiming for very high levels of cyber resilience, this study found that most NZ organisations are settling for a cybersecurity posture just slightly ahead of their peers and relying on cybercriminals to target the weakest organisations. While this may be an effective short-term strategy and may even be seen as taking a prioritised, risk-based approach to cybersecurity, it is ultimately negative for the overall business landscape. Adopting such high levels of cyber-attack acceptance and demonstrating mediocrity in defence continues to fuel a lucrative industry for cybercriminals and will guarantee continued high-risk for all.

Accepting “it’s not if, but when” an organisation will have a cyber breach is arguably equivalent to announcing to customers that “it’s not if the medical data you gave us will be stolen, it’s when”. Society does not advocate for this level of acceptance in any other areas of criminal activity; for example, individuals do not buy a car assuming it will be stolen or go for a walk, assuming it is not if they will be attacked but when. Therefore, cybersecurity professionals must reconsider this message to drive awareness and preparation in some areas as it may not result in positive outcomes as intended and may even be potentially detrimental to NZ’s organisational cyber preparedness.

6.2.2.11 Improving organisational cyber risk assessment and management processes

A risk-based approach to managing cybersecurity investment is necessary for most organisations addressing the current threat landscape with limited resources. As seen in the findings, most risk assessment processes today involve a simple probabilistic calculation that considers impact and likelihood to determine whether actions should be taken to mitigate a potential cyber risk. This predominately qualitative approach to risk assessment is seen in this study to be imperfect at best and involve significant guesswork at worst. Therefore, more effort is required to develop contextualised cyber risk assessment

tools and processes that allow greater quantitative input and output and enable a clear and objective view of organisational cyber risk.

Enabling a more quantitative cyber risk view in NZ organisations will require higher quality and more complete input data from the wider cyber landscape and the internal IT infrastructure. This is critical as having a complete view of an organisation's greatest areas of value and vulnerability, along with what may target these areas, is key to effectively prioritising risk. While individual organisations cannot immediately control external aspects of landscape visibility, internal visibility could be improved by focusing on ensuring quality audit tools and processes are established and used. Additionally, more training in formal risk management could benefit NZ organisations, as the findings described a lack of confidence in this area.

Using a risk-based assessment approach that only considers "point in time" impact and the likelihood of threats ensures that NZ organisations are not preparing to address any emerging or future cyber threats. This is because threats not currently seen "in the wild" will never score highly on the likelihood axis. Therefore, it is important to be aware that not all threats are sufficiently addressed by these traditional risk assessment processes. The conflict this current approach creates when prioritising risk management actions is seen in the findings of this study where participants both acknowledged that organisations must prepare for quantum threats immediately whilst simultaneously stating the quantum threat was not imminent enough to act on. Including a strategic risk view in organisation risk matrices where emerging threats can be captured, evaluated, and reevaluated has therefore become vital due to the existence of known but as yet unrealised cyber threats, such as those that quantum computing will pose. However, the findings show that this record is currently absent in many NZ organisations, and only active cyber threats are included in risk registers. Therefore, the observed conflict around whether organisations act on a longer-term risk will remain unresolved until this process is enhanced.

The impact of quantum computing-enabled threats is not well understood, and the findings from this study show that NZ organisations view the likelihood of this risk to their organisations as almost null in 2024. Therefore, this risk is not currently included in any risk assessment, planning, or management processes. However, as described in the literature review, this view is not completely accurate as there is already one threat posed by quantum computing, coined the store now, decrypt later (SNDL) attack, that is currently active. An SNDL attack could impact any organisation that handles information requiring confidentiality beyond 5–10 years and involves adversaries capturing the encrypted data today to decrypt it as soon as a quantum computer is available. Assessing whether an SNDL attack poses a true risk to an NZ organisation involves clearly understanding all of the data an organisation manages. For example, if schematic plans of sensitive buildings (such as prisons) or critical infrastructure equipment (such as powerplants) are stored and these are unlikely to change in the next decade, then the likelihood and impact of this being stolen now and decrypted in several years may be high. Finding alternative ways to protect this information is, therefore, immediately required. However, until organisations incorporate emerging cyber risks into their frameworks, attacks such as these may go unaddressed.

The need to start transitioning all systems to use quantum-resistant algorithms many years before a quantum computer is even available highlights how it is now also critical to include the additional element of "lag time" in the risk view. Lag time is essentially a calculation of the time it would take to mitigate a threat against the time it would take for a threat to eventuate. This calculation is represented in the literature

review example by Michael Mosca (2018). If lag time is not considered during risk assessment, the risk may be deemed low and preparation to ensure the threat can be mitigated once it eventuates is not adequately considered. This will ultimately result in much higher cyber risk once the threat does eventuate, with organisations scrambling to address the high-risk reactively and potentially being too late to prepare and avoid serious impacts.

Highly contextualised and more quantitative and complete risk assessment methods are required in NZ organisations. Additionally, having a more comprehensive view of risk and embedding the assessment of emerging threats into existing business risk management frameworks could aid in ensuring NZ organisations proactively assess and manage the preparation for quantum computing-enabled threats.

6.2.3 Making Room to Apply a More Strategic Lens Across Cybersecurity

A primary theme found throughout this study was the need to apply a more strategic lens when managing cyber and emerging technology risks. The results show that NZ organisations are not strategically planning for cyber threats. Current organisational planning frameworks do not look beyond the next 2–3 years, making them inadequate to sufficiently prepare for emerging threats with longer-term or uncertain impacts.

This lack of strategic focus is reflected at the NZ Government level, where the findings show the National Cybersecurity Strategy is not fit for purpose and does not look beyond 2023. The current strategy also lacks any reference to planning or managing quantum computing-enabled threats. There is also a distinct lack of transparency and clarity around the cyber risks that may impact NZ at a national level and how these risks are being managed and addressed to ensure a safe online future.

These findings support and reflect recent literature (Gluckman & Bardsley, 2021, 2023) that describes the current lack of adequate preparation for all kinds of high impact rare event (HIRE) risks in NZ. This research highlights the disconnect between the scientific awareness of high-impact risks and the investment actions required to prepare for these risks. While the current literature is focused on inadequate general HIRE risk management at a national government level, this study adds to this understanding of the landscape by showing inadequate strategic cybersecurity risk management at both government and organisational levels within NZ. This short-term focus harms NZ as long-term planning and investment in the resiliency of all technology infrastructure and environments is necessary to ensure a secure and prosperous future.

Participants gave uncertainty around the true impact and timeframes of future cyber threats associated with the development of quantum computing as a primary reason for not planning or preparing for these. However, it is important that organisations acknowledge that there will always be elements of uncertain risk and learn to tolerate this uncertainty. Encouraging and supporting planning sessions that look for common business impacts and mitigations regardless of the level of existing threat knowledge should be normalised. When discussing general risk preparation in conditions of uncertainty, Gluckman and Bardsley (2021) suggest considering what the common impacts may be from a variety of possible threats and making plans to mitigate these common impacts rather than focusing on the unknown or uncertain specific impacts from a particular use case. This idea could easily be applied to the possible but uncertain threats that may result from using quantum computing. For example, organisations could identify wider potential business impacts that may occur due to various cyber or natural disaster incidents, such as the inability to perform online payments for an extended period. Strategically planning to minimise the general impacts

identified, such as designing alternative methods of operating without online payments, may be beneficial for minimising the negative consequences of any one of multiple threats, including those that arise from using quantum computers. This method effectively reduces the need to fully understand “how” or “when” this impact may occur before addressing it.

In addition to creating a leadership culture where uncertainty is more acceptable, there is also a need for additional capacity at the government and organisational levels in NZ to allow long-term planning and strategy. However, making space for a strategic lens across cybersecurity and emerging technology may require ensuring this capacity sits somewhat outside of the traditional operating environments both in the government arena, where a political focus of 3 years is inadequate and in organisations where the current strategic planning and funding processes drive shorter-term objectives and deliverables.

Adding capacity to allow the “what if?” scenarios to be mapped out and understood would enable cyber risks that require early intervention to be uncovered and actions to mitigate these risks to be clearly communicated promptly. Additionally, adding this capacity for strategic thinking and ensuring the outcome of this process is transparent both at a national level and at an organisational level may build trust in cybersecurity functions and increase the understanding of future cyber risk in NZ.

6.2.3.1 Contingency planning

One strategic planning process that the findings show some NZ organisations already use and value is creating and regularly testing cyber incident response plans. Current literature supports the usefulness of these plans in successful cybersecurity response (Apgar, 2021; NIST, 2020), and all NZ organisations would benefit from creating a plan of action that describes how they will respond to a quantum-enabled cyber threat should it impact their organisation. The process of creating specific contingency plans may drive greater awareness and more effective preparation for quantum computing threats and ensure future attack impacts can be minimised.

An incident response plan to address the threats from quantum computing is also required at the national level, as the findings describe how any large attack from a quantum computer wielded by a hostile nation-state may have national security impacts. National security resources should develop a national response plan in collaboration with representatives from critical infrastructure organisations to ensure the protection and recovery of essential services is possible and prioritised after any attack. However, no participants in this study were aware of these plans, and participants felt that the government’s cybersecurity function lacked transparency in this area. Therefore, whether NZ is adequately prepared to respond to a widespread quantum computing cyber-attack at a national government level is unclear.

A cyber incident response plan must be widely tested to ensure it is fit for purpose and understood by all parties required to act on it. However, as this study found low awareness of quantum computing-enabled threats at the senior levels of many NSOs and no study participants were aware of a collaborative national response plan, it is unlikely that the nation could respond promptly or efficiently to a widespread attack of this nature. Australia’s recent cybersecurity strategy expressed an intent to conduct exercises across critical industries to test their cyber incident response plans (Commonwealth of Australia, 2023a), and this study found that NZ would benefit from a similar commitment to ensure a coordinated and effective response is possible to any significant cyber-attack with widespread impact at a national level.

6.2.4 Developing National Capacity for an Emerging Threat Landscape

This study highlighted several areas where national capacity could be grown to ensure NZ is better prepared to face the emerging quantum computing cyber threat landscape. These focus areas include lifting public capacity to respond to cyber incidents and investigate and prosecute cybercrime, growing a cybersecurity and quantum technology skills pipeline, building quantum-supporting infrastructure, and developing a domestic quantum industry.

6.2.4.1 Greater capacity and capability for cybercrime response, investigation, and enforcement

Increased organisational cybersecurity measures alone will not be enough to drive NZ's cyber risk down. Consequences for cybercrime or failing to secure an IT environment must exist as a deterrent alongside effective incident response, investigation, and enforcement measures. Currently, the findings show that the consequences of poor cyber hygiene or of committing cybercrime are too minimal in the NZ environment to act as an adequate deterrent, and there are also limited investigations or enforcement measures undertaken after a cyber incident has occurred. This study also found that NZ organisations require greater support to respond to and investigate cyber incidents, and that the government agencies currently tasked with supporting NSOs are viewed as neither skilled enough nor resourced sufficiently to provide this support. Quantum computing and related emerging technologies have the potential to rapidly lift the scale and impacts of cybercrime, making this issue even more imperative to address.

An enormous and well-recognised enforcement gap exists between the volume of cybercrime committed globally and the successful investigation and prosecution. Studies have attempted to understand this gap, why it is happening, and what must be done to change it (Vasiloiu, 2023; Walsh & Love-Grayer, 2023); however, developing the capabilities required to close this gap is woefully slow. NZ must begin by increasing the capabilities and capacity of agencies accountable for cybersecurity, including law enforcement. Ensuring police, prosecutors, and cyber incident responders fully understand digital crimes and have the tools, capacity, and mandate to investigate and prosecute those responsible and support the victims of these crimes is essential.

The literature review highlighted how nations are starting to dedicate large amounts of funding to tackle both cybercrime and emerging technology issues in recognition of the seriousness of this area. For example, the latest Australian Government budget has lifted the annual funding of the e-Safety Commission fourfold to A$131 million and is creating a new National Anti-Scam Centre, allocating another A$86.5 million to establish this. The US and the EU are also significantly lifting investment in measures to combat cyber threats (WEF, 2024). However, at the time of writing, NZ has yet to commit to lifting investment in national cyber capacity despite needing greater cyber response, investigation, and enforcement to lower the high-risk environment. Some positive steps have recently been taken to consolidate the government agencies responsible for cybersecurity and technology issues (NZ Government, 2023b). This action should start to address concerns raised in the findings that the response to cyber issues in NZ was scattered across too many disparate departments; however, those agencies responsible for addressing these issues may remain inefficient should greater investment in capacity and capability not be made.

Much stronger public and private collaboration is also required to fight cybercrime as the private sector holds much of the skills, data, and capability required to investigate within the corporate domain. Ensuring that future digital crime is adequately addressed in NZ will require stronger partnerships between the police, government cyber agencies, and the private industry. Agreeing common investigative frameworks and growing trust between these entities to incentivise data sharing will be critical; however, this will require concentrated effort as there is only limited trust and sharing between these parties today.

6.2.4.2 Addressing skill shortages in cybersecurity and quantum technology

The findings from this study concur with the literature review in concluding that there are critical skill shortages in cybersecurity and quantum technology globally and in NZ. Organisations and nations who cannot source and retain adequately skilled talent are hindered in their attempts to secure against cyber threats and harness the positive benefits of emerging quantum technology. Therefore, NZ organisations, the NZ Government, and academia must address these skill shortages and plan for a future where skilled individuals in cybersecurity and quantum technology will be essential to protect critical assets and economic markets. Lifting the availability of skilled resources will require the creation of an education pipeline that provides ample opportunities to learn and grow diverse knowledge and skills in cybersecurity, quantum science, technology, ethics, and business. It will also require increasing the diversity of quantum science and cybersecurity professionals and growing the skills of the existing workforce.

6.2.4.3 Quantum and cybersecurity education

The findings demonstrated that nations such as Canada, the US, the UK, and Australia all support changing and enhancing their national education systems to ensure they support the future needs of a quantum computing-enabled society. This requires a move away from teaching “discrete” disciplines and toward a more multidisciplined approach that heavily weaves quantum scientific concepts and STEM topics into learning systems from an early level. This new approach also encourages considering these disciplines through various lenses, including business, ethical, philosophical, and humanities.

Recently, the NZ school curriculum has faced heavy criticism for its lack of effective science programmes at the primary level (The Education Hub, 2022b; Wiggans, 2023a), with the Education Review Office stating in the last report conducted that less than one-third of NZ primary schools effectively educate students in fundamental sciences such as physics (Education Review Office, 2013). Additionally, the NZ Ministry of Education (MOE) published a draft review of a revised secondary school science curriculum in 2023, that, according to the New Zealand Institute of Physics, lacks any fundamental education in physics, let alone broadens the way physical sciences are taught to enable future quantum scientists or technologists (New Zealand Institute of Physics, 2021). The MOE emphasises that the new curriculum is needed to ensure a more holistic view of science is taught, enabling the solving of complex global problems such as climate change and those that emerging technology will bring. This need for more cross-functional skills across science and technology is strongly backed up by the findings of this study; however, NZ must carefully consider how it achieves this goal and ensure that both fundamental and further quantum physics concepts are included as foundational learning for all. It is critical for NZ’s future that changes are made to our learning systems to ensure NZ has a sufficient supply of critical thinkers that can address the emerging challenges organisations will face when quantum computing and related technologies become widespread. To achieve this, the NZ Government will need to gain the support and grow the confidence of

the teaching professionals to deliver this knowledge in a way not previously explored. However, support for a new approach is not widespread in NZ (Wiggans, 2023b), and stronger communication about the drivers for changing the curriculum needs to be undertaken.

The literature review acknowledged the existence of limited tertiary academic programmes focused on quantum technology research (NSA, 2020). However, the document analysis findings suggest that various nations are significantly increasing their investment in education programmes dedicated to quantum computing as they recognise the importance of developing a pipeline of skilled resources to support the cybersecurity and quantum landscape in their countries. The findings from this study suggest NZ professionals are aware of the importance of educating the future workforce as they are already feeling the pain of skill shortages and are disappointed in NZ's lack of commitment to improving education.

When discussing the theme of varied cyber maturity levels, participants expressed a wish for cybersecurity and ethical considerations to be become second nature in the next generation. With cybersecurity often still an afterthought today and education options limited, this is unlikely to happen without significant change that includes prioritising cyber security and quantum technology education to lift overall national capacity. In conclusion, NZ would benefit from introducing more quantum technology tertiary options and tertiary technology programmes that include ethics, policy, law, and business and innovation components.

6.2.4.4 Increasing diversity

Study participants did not raise or acknowledge a lack of diversity in technology or quantum sciences in NZ organisations. This lack of consideration is concerning as the document analysis findings clearly show that talent diversity is poor in both the fields of cybersecurity and quantum technology globally and within NZ. This lack of awareness may be because, on the surface, the technology departments in many NZ organisations appear to be very diverse as they are made up of many skilled immigrants from all over the globe (New Zealand Technology Industry Association Incorporated, 2022). These immigrants are needed because very few New Zealanders graduate in technology, and those who do are not diverse (Ministry of Business, Innovation & Employment, n.d.). This balance must change as while gaining skilled technology workers via immigration is valued, the increase in global competition for technology professionals may mean that this pipeline is not as easily available moving forward, and more reliance on domestic skills and talent will be necessary. This issue is amplified in quantum computing, where global talent diversity is extremely poor, and the findings show that nations are aggressively pursuing and attempting to retain global quantum talent.

As the findings show, female participation in quantum sciences and cybersecurity is particularly poor. In NZ, the inclusion of Māori and Pasifika in digital careers is also poor (New Zealand Digital Skills Forum, 2021). Ignoring such a large percentage of the potential future workforce will not make sense in a market increasingly impacted by skill shortages; therefore, greater numbers of women, Māori and Pasifika must be encouraged and supported into technology and quantum science careers in NZ. To achieve this greater diversity, the true value of a diverse workforce must be understood and promoted in NZ businesses. The literature shows that people with different backgrounds and experiences have different ideas and ways of solving problems (GESDA, 2022), which is especially valuable in technology fields such as cybersecurity and quantum computing that require innovative solutions. This diversity of thought will become even more crucial when the complex ethical issues of tomorrow's technology arrive. Without diversity, quantum

technology solutions that perpetuate current societal biases and do not harness the benefits for all areas of society may be all that are developed.

Lowering the barriers to entering a career in quantum computing by building internships and graduate programmes may assist in driving diversity. Recognising that future technology leaders will require a greater range of soft skills and multidisciplinary understanding may also reduce the barriers to entering a career traditionally seen as requiring high technical proficiency. Educating existing leaders on the value of promoting diversity will help promote change. Linking inclusivity and diversity to performance metrics may also be necessary to drive meaningful change where the value is not yet recognised, and offering targeted mentoring programmes and promoting diverse role models may also help.

Introducing unconscious bias training for employees may assist in creating workplace environments that are more welcoming and inclusive. Critically, this training should occur at senior leadership levels as resources at the senior levels must model an organisation's desired culture and behaviours. This study showed a successful cultural change in cybersecurity when organisations spent time and effort talking to employees about cybersecurity from their first day in an engaging and fun language and format. Similar effort and consideration can be applied to successfully encourage diverse workplace cultures by ensuring inclusive language is used, and the value and voice of all parts of society are acknowledged and respected. Additionally, enabling inclusive workplaces by offering flexible work hours, parental leave, on-site childcare, equal salary, and opportunities to lead and be heard will increase retention, as it is also clear that diversity reduces even further at the more senior levels of NZ organisations.

Creating a workforce that is more representative of the diversity of NZ's society is critical to reducing skill shortages, easing the reliance on international immigration, and driving innovative solutions that reflect all of society's needs. Diversity can be improved through various mechanisms, but as acknowledged by the findings, significant long-term investment and effort are required for change to occur.

6.2.4.5 Attracting international talent

Along with highlighting the availability of domestic talent, this study finds that NZ must ensure it remains an attractive option for international talent. The findings described how governments globally are taking various policy measures to encourage and retain international quantum and cybersecurity talent. The NZ Government has also started to respond to this trend by promising new technology-based visas to ensure a continued pipeline of skilled international workers (Keall, 2023), and further measures of this nature will be important to ensure NZ organisations have access to sufficient talent while domestic skills are still being built.

6.2.4.6 Lifting workplace skills and competency

Along with growing general and senior leadership skill levels in cybersecurity and quantum technology, the current general workforce skill level must be raised to ensure quantum threat challenges are understood and can be managed.

The current tools used by NZ organisations to train their teams in cybersecurity awareness, such as phishing tests and simulations, may not be sufficient to combat advanced social engineering threats created by emerging technologies such as AI fuelled by quantum-computing processing power. As

described in the literature review, AI-enabled adversaries can create threats that are harder to identify, and adding quantum power could make these threats even more targeted, pervasive, and powerful (Manning, 2020). Therefore, investment in lifting general workforce cybersecurity and quantum technology skills is critical to ensure NZ organisations remain safe.

6.2.4.7 Developing infrastructure and ensuring quantum technology accessibility to protect national security and the economy from negative quantum technology impacts

The literature reviewed in Chapter 2 demonstrated that quantum technology could threaten national security, particularly for those countries that do not possess the capabilities required to defend against quantum computing cyber-attacks. This view was confirmed by the findings of the document analysis, which suggest some nations are developing quantum technologies for protection.

To date, NZ has not invested heavily in infrastructure to support quantum technology and, therefore, is highly unlikely to be among the first nations to develop a quantum computer. Despite this, there are several compelling reasons why NZ should now accelerate national capacity development in these areas. Firstly, many defence mechanisms to protect against quantum computing-enabled cyber threats will come from quantum-enabled computing and networks. Access to these defences will be critical for NZ at a national and organisational level to ensure ongoing cyber threat protection. As seen in the findings, significant competition may exist for all the components necessary to implement quantum-enabled systems and access to these international supply chains is not guaranteed. Therefore, NZ must investigate and identify what components and materials it will require to utilise quantum networking, determine whether any components could be produced domestically, and start to secure the early supply of critical components.

Secondly, developing the infrastructure required to implement quantum systems will help drive the adoption of these technologies. Trust in new technologies requires time to establish. Therefore, the sooner NZ can test and evolve quantum and hybrid systems, the sooner NZ organisations will be prepared and able to use this technology to protect against any threats originating from the international use of quantum computers.

Finally, it can be argued that those who innovate and build quantum computing systems will create tools that deliver their desired outcomes, which will likely inherently embed their values (Pew Research Center, 2021). Therefore, ensuring quantum technology reflects NZ values will require NZ to be part of quantum technology innovation.

The literature review and the document analysis findings show that QKD networks are being explored and implemented globally (Mosca, 2018). At this stage, NZ has not started to prototype these potential solutions; however, this study found that this would be a viable and sensible next step for NZ. Investing in QKD networks may advance familiarity with and use of quantum technologies and help NZ organisations prepare to protect sensitive data and communications from quantum computing-enabled threats.

Public and private organisations in NZ must collaborate to drive the research and development into critical infrastructure to support future quantum technologies that could aid in protecting all New Zealanders. Continued support from the government is needed to maintain and grow the levels of current quantum research and development expertise through centres of excellence such as the Dodd–Walls Centre;

however, participation and investment from all areas will be necessary to ensure these technologies can be tested and accessible for use here in NZ by NZ organisations.

6.2.4.8 Establishing a domestic quantum industry

Establishing a sufficient domestic quantum technology industry to support the introduction of quantum infrastructure is necessary if NZ wishes to remain protected from cyber threats in the future. The findings clearly show that supporting the growth of domestic quantum industries is a strong priority for nations such as Australia, the US, Canada, and Europe; however, NZ has not begun this process. Therefore, effort is required in NZ to start establishing a stable quantum industry presence that has the resources and expertise to assist NZ organisations in incorporating and using quantum systems, networks, and technology. Supporting a domestic quantum industry in NZ will require more business incubation and investment opportunities, a greater cultural drive and support to innovate, maintaining a stable political system and recognising that quantum technology will be important for the nation's future security and economic opportunities.

The literature review confirmed that a stable political system is required to support a trusted economy, allow industries and markets to thrive, and, therefore, grow a local quantum technology presence. In recent years, NZ has scored highly in tools such as the Short-Term Politic Risk Index (Fitch Solutions, 2023), which measures national political stability. Unfortunately, NZ's score in this space has recently dropped to its lowest level in a decade, indicating greater local ideological division in politics. Critically, this greater division is predicted to slow down the formation of new policy (PWC, 2023), which may decrease the ability of NZ to grow a successful quantum presence. Increasing negotiation, diplomacy, and communication skills are therefore even more vital in the NZ Government to ensure timely agreement of national technology strategy, policy, and action.

Greater business incubation and funding support are also required for a fledging quantum industry to develop in NZ. Currently, however, investment for start-ups in NZ is falling (PWC, 2023), and investors are demonstrating risk-averse behaviour by choosing to invest in known companies rather than new technology companies. This current climate may adversely impact the ability of a quantum technology industry to form in NZ. To be successful, the government would need to provide greater support and backing for new start-ups in quantum and drive investor confidence into this area. However, suggested initiatives such as tax breaks for venture capital investments that may drive investment into innovative industries such as quantum technology were not included in the 2023 NZ Government mini-budget (NZ Government, 2023a), and it is unclear whether this will be a focus for the 2024 budget.

6.2.5 Strengthening and Enabling Trusted Relationships

The foundations for a resilient national cyber posture in a quantum computing-enabled world will rely heavily on forming and maintaining trusted relationships in all areas of the cyber landscape. The current NZ operating environment described by the findings in this study is one of low trust that drives secrecy and limits the sharing of threat intelligence, vulnerabilities, and lessons learned. Improving this detrimental culture will require significant courage and effort from cybersecurity and NZ organisational leaders.

One previous study considered in the literature review described how the nature of third-party relationships could impact a nation's technology readiness (Lees et al., 2018). The findings of this study strongly

reinforce this view and further extend it by highlighting the criticality of trusted relationships across all aspects of the cybersecurity landscape. Strong, trusted relationships must be built between cybersecurity and technology peers, organisations and vendors, industry competitors, and public and private organisations to improve the ability of NZ organisations to prepare for and respond to a quantum computing-enabled threat landscape.

The findings clearly show that interpersonal relationships and learning opportunities are vital to growing confidence in cybersecurity, and this must be harnessed to their full potential if NZ organisations are to succeed in protecting against a growing threat landscape. Formal opportunities for peer interaction between industry professionals could be strengthened. Currently, these events are mainly created by vendors; however, organisations would benefit from hosting these types of networking and sharing events themselves. Additionally, introducing formal mentoring programmes in organisations may help to grow the collective skills and knowledge of the cybersecurity landscape.

The findings indicate that building trust between NZ organisations and their technology and cybersecurity vendors could begin with vendors investing more time and effort into understanding their client's unique business contexts and challenges. Additionally, NZ organisations must recognise and acknowledge that competition and a fear of showing vulnerabilities to a competitor currently stand in the way of greater intelligence sharing that would benefit the whole industry.

The literature review, document analysis, and interview findings all concur in stating that cybersecurity is a team sport, and all community areas must work together to create a safe digital environment. Public and private collaboration was also seen as important in achieving innovation and developing a cyber-resilient nation; however, the findings show that NZ organisations have little trust in current public and private collaboration and little faith that more of this will occur.

This lack of trust has led some participants in this study to believe that cybersecurity management would be best left to private organisations only. This seems to be a recent trend, as participants reported minimal cybersecurity support offered or given to private industry by public agencies. However, leaving full responsibility for the protection, management, and equal dissemination of information in the hands of commercially driven organisations may be flawed, as they are often driven by commercial goals that may not reflect the best outcome for societies.

Historically, public institutions such as public libraries, universities, and postal services were created to manage data or information storage and dissemination. These mechanisms are still in use; however, arguably, the private sector now stores, handles, and sometimes protects most critical societal data. Therefore, the private sector must be given greater support to ensure adequate cybersecurity is implemented, and strong public agencies must be given accountability to offer this support and ensure commercial goals are not achieved at the expense of data security. Achieving this balance of responsibility for cybersecurity will require building much greater trust and stronger relationships than exist today between the public and private sectors in NZ.

Neither the literature review nor this study found easy or quick solutions for enabling more trusted relationships in cybersecurity. However, it is very clear that greater effort, more research, and a willingness for NZ cybersecurity practitioners to show vulnerability and share more openly are needed to ensure the

current low-trust culture does not limit NZ's ability to innovate and respond to new threats in a quantum computing-enabled world.

6.2.6 Slowing Down to Speed Up?

The pace of technology-driven change is now incredibly fast, and this study shows that many NZ organisations cannot respond to this rate of change and implement the technological and behavioural changes required to maintain a secure operating environment. Most NZ organisations also face the need to upgrade or replace significant amounts of legacy technology to remain secure in the quantum computing-enabled landscape. These necessary infrastructure improvements will require significant ongoing resources and time to complete. In parallel, security teams must also continue to patch new vulnerabilities in systems and change business processes to combat the latest cyber threats. However, as acknowledged by the study participants, organisations have a limit on how fast they can absorb change. This limitation restricts the number of changes cybersecurity teams can implement in organisations at any one time, and therefore, regardless of the size of their budgets or teams, the ability to keep users and data safe has become almost impossible in a landscape that shifts so quickly.

The idea that things are changing too fast to keep up with is not new. As early as 1922, an American sociologist observed how technology rapidly advances while social norms and values often resist change and "lag" behind. This phenomenon was named the "cultural lag" (Ogburn, 1957). Therefore, it is well-recognised that innovation moves faster than humans adapt to change. This cultural lag can be seen in current societal issues. For example, scientists have long highlighted that a climate change crisis is underway that requires cultural and behavioural change to combat; however, many nations, organisations, and individuals continue to act in ways that negatively impact the climate. The findings of this study show the potential negative impacts of quantum computing evolution may share some characteristics with the impacts of climate change, such as global scope and scale. The findings also clearly demonstrate that current organisational behaviour will not change to mitigate these impacts unless significant intervention is made to reduce cultural lag.

The disconnect between the pace of technological change and the ability to adjust and adapt to these changes is already demonstrated in the inability of organisations to secure against current cyber threats. This disconnect will be reflected and potentially amplified in the evolution to a quantum computing-enabled world. Therefore, there are some arguments to support slowing down the pace of new technology development and rollout across society.

Firstly, slowing down may allow time for organisations to catch up with implementing basic security hygiene in a sustainable manner that focuses on quality and ensures current technology environments are secure. Secondly, slowing down may allow greater time for technology developers to genuinely consider questions such as why and how emerging technology, such as quantum computing, should be developed and used.

It is important to determine who will benefit from new quantum technology and at what collateral cost is necessary in a society where it is arguably no longer optional to interact with it. As new technology is often used in ways that diverge from the original use case or intent envisioned by developers (Wolff, 2021), this process would require technologists to be trained to think creatively and strategically. New frameworks that embed conscious steps encouraging developers to consider the potential impacts of the technology

are required. Deciding who is responsible for the impact review process and ensuring these impacts are mitigated would also be critical. Finally, leaders must recognise the importance of these steps and allow slower development timeframes to ensure it happens. Slowing down the development lifecycle to incorporate these important facets may allow time for organisational culture and behaviour to remain aligned with any security challenges the technology may bring.

Despite the findings indicating a need to slow down the rate at which society and organisations introduce new technology and, therefore, the rate at which they must absorb security changes, the notion that constant change and innovation are a good thing in technology is pervasive. If you can innovate and change, you will succeed. The contemporary framing of technology seen in the literature review draws on the language of progress, development, and advancement with new technology positioned as necessary and inevitable (Chen, 2020). This language is also pervasive in the findings of this study which emphasise how quantum technology will equal national strength and is necessary for growing a thriving economy in the future.

Changing societal norms and behaviour is difficult, as shown by humanity's reluctance to alter behaviour in response to climate change. This study clearly shows it is unlikely that humanity will slow the pace of technological innovation and change by much, as although there is recognition of the need to catch up, there is an equally strong desire to innovate and advance technology. Therefore, the solution to overcoming cultural lag in addressing quantum computing may require a combination of slowing the rate of technology change slightly by using the levers of regulation, changing culture to value the need for quality over pace in getting foundational aspects of cybersecurity in place, and prioritising technological equality and ethics in society over pure economic growth, whilst also simultaneously seeking practical methods to increase the rate of new technology adoption and behavioural change.

6.3 Research Question 2

Q2. What role should the NZ Government play in global conversations and policy development focused on the cybersecurity and ethical implications of emerging quantum-enabled technology?

NZ must play an active role on the global stage to encourage and promote NZ's view of the ethical development and use of quantum technologies. Showing strong diplomatic skills, the NZ Government must champion open international collaboration and cooperation in a geopolitical environment increasingly displaying more protectionist and national sovereignty rhetoric. The NZ Government should embrace a role that strongly advocates for globally agreed principles for ethical quantum technology development and use that are created and established using a wide collaborative and transparent process. Additionally, the NZ Government must build credibility to enable their constructive contribution on the global stage by acting as a role model and defining and applying domestic principles for ethical quantum research, development, and use.

The findings also indicate that several complimentary activities must occur to ensure that the NZ Government can play a leading role in global conversations in this area. These include developing a stronger domestic technology vision, enabling skilled policy advisors and diplomats, and investing in research exploring quantum technology's impacts on NZ society.

6.3.1 Developing an NZ Vision

The NZ Government must clearly understand, define, and transparently communicate exactly what stance NZ will take when addressing the development and use of quantum technologies domestically. In addition, they must communicate a clearer approach to all cybersecurity issues currently impacting the NZ landscape to ensure a digital future that reflects NZ's unique values is widely understood and upheld.

The results of this study show that NZ's position and plan to address cybersecurity and quantum technology issues are unclear. NZ organisations expect greater leadership from the NZ Government to ensure the definition and articulation of a national vision that reflects the country's cultural and ethical paradigm. Strong direction and practical guidance that support NZ organisations in enabling this vision are also needed. The study results describe how various nations have invested in creating detailed national quantum and cybersecurity strategies and plans to address emerging technology issues. In contrast, the findings show that NZ's cyber planning is insufficient regarding technology scope, detail, and planning horizon. The current NZ cybersecurity strategy does not adequately reflect the rapidly changing technology landscape, and there is no publicly available vision for quantum computing or related emerging technologies in NZ.

The findings describe how NZ has a unique position in the world, requiring it to think carefully about its approach to quantum technology development and use. There are also cultural values that require prioritisation when developing an NZ-focused stance and strategy. These values include equality, freedom, democracy, advocating and upholding human rights, and applying tikanga.

Study participants expressed a strong wish to see NZ uphold a commitment to build future technology in a way that "benefits all" of society. However, there is often conflict between the use of technology for individual good versus societal good, which requires careful consideration. For example, using a quantum computing search of health data may simultaneously aid society's understanding of current health challenges while negatively impacting an individual's right to privacy. These challenges must be fully understood and require widespread debate to ensure a range of views contribute to any resulting stance or formation of policy.

Deeply exploring NZ's position on emerging quantum technology issues is also required to understand and address the nature and preservation of data sovereignty for all New Zealanders. The results of this study align with the literature in expressing how there is a need for meaningful consideration of the impacts of decisions about digital technologies on the land and broader environment. Māori culture recognises how all things are interconnected, and as expressed by Kukutai et al. (2020), the ethics of manaakitanga and kaitiakitanga must be considered to ensure that a quantum computing-enabled world upholds the dignity of individuals, promotes equality, and protects all areas of NZ society from harm.

Another important dimension to consider when embracing tikanga is shifting any planning focus beyond short-term benefits and harm and adopting a view across generations. The results of this study strongly highlight how this long-term dimension is sorely lacking in the current cybersecurity and technology landscape in NZ, and any process to develop a cybersecurity and quantum technology vision for the nation must embrace a more strategic lens. Ensuring a multigenerational view is included in national strategy would also demonstrate the value of this approach internationally.

The literature review highlighted how more research investigating quantum technology's role in influencing current global democratic processes is required (Coenen et al., 2022). The interview findings show that strong democracy is valued in NZ; therefore, the government must support and undertake this research to ensure that any NZ strategy does not include actions and discourse that knowingly or unknowingly erode democracy. One factor seen to potentially influence quantum technology's role in democracy is our ability to hold constructive conversations on the ethical issues surrounding it.

The literature suggests that the discourse required around quantum computing and cybersecurity now spans a complex arena of human rights, domestic and foreign policy, economic stability and progress, and healthy democracy. A concern raised in the findings was the lack of technology professionals with sufficient multidisciplinary knowledge in the public service to discuss ethical concerns around emerging technology and translate these concerns into policy and direction. National governments such as in Australia are allocating funding to ensure skills and policies can be created to effectively govern emerging technologies (Commonwealth of Australia, 2023b), and the NZ Government must also invest in ensuring adequate skills are developed in this increasingly important area. The NZ Government must also encourage much greater and more widespread global public awareness and debate on the ethical and legal challenges of emerging technology, as this study demonstrated that many New Zealanders lack an understanding of these complex challenges.

Several studies in the literature review highlight the lack of a common language to discuss many of the complex ethical and technical issues that the evolution of quantum computing will pose (Coenen et al., 2022; Liman & Weber, 2023; Roberson et al., 2021) and there is also some rudimentary literature that acknowledges the impact that language is having on the global ability to engage in meaningful conversations around the ethical impacts of quantum technology (Burton & Christou, 2021).

The terminology used to describe the concepts, metaphors, and protocols of both cybersecurity and cryptography are typically related to the terms of warfare. For example, entities that listen in on communications are "malicious adversaries" that use "tactics" or a "cyber kill chain" to conduct "attacks" or "cyberwar". This study shows that this language style has also permeated the quantum computing discourse and dominates current national quantum strategies. Using militaristic terminology and conflict-driven framing of quantum technology may ultimately skew society's understanding of quantum computing. Domestically and in its role on the global stage, the NZ Government should refrain from engaging in quantum discourse emphasising power, national sovereignty, warfare, battle and dominance. Embracing and using the language of scientists and business to describe quantum computing and its potential impacts (both positive and negative) may encourage other nations away from global rhetoric that is starting to be recognised as unhelpful for building geopolitical relationships or for promoting quantum technology use cases for the greater societal good.

To ensure an inclusive and widely representative view is reflected in any national vision and strategy for quantum and emerging technology, the NZ Government must undertake wide consultation and act as an effective mediator to ensure constructive and open conversation. Any consultation process must be open and transparent, as, to date, this study shows NZ organisations feel excluded from information about cybersecurity issues at a national level.

6.3.2 Influencing an Increasingly Divided Geopolitical Environment

The findings of this study concur with recent literature in describing a growing sense of greater division in international politics and the strengthening of rhetoric centred around building and defending national digital sovereignty. The ongoing discussion of quantum computing increasingly frames it as a critical shaping influence for the global geopolitical landscape. The document analysis findings support literature showing how international security is now a key motivation for increased investment in quantum development (Der Derian & Wendt, 2020).

The literature view described how many nations see the evolution of quantum technologies as a new "space-race" (Johnson, 2019) and invest heavily in the development of quantum industries to lead this race. However, this study found that NZ will need to approach this issue differently due to the nation's smaller size and limited investment in this technology to date.

The growing emphasis on national sovereignty, the strategic competition, and the growing divide between China and the US are placing small- to medium-sized countries such as NZ in a challenging position whereby new strategies will need to be devised to ensure ongoing access to transformative technologies. The findings show that NZ increasingly treads a fine line between maintaining robust relationships with its traditional "Five Eyes" partners and keeping enough distance on contentious issues to maintain a positive trading partnership with China. Sustaining the status quo is becoming more difficult, however, and as these global powers are likely to have access to quantum technologies first, the decisions the NZ Government makes regarding responding to the more divisive current geopolitical environment may impact NZ's ability to prepare for quantum computing-enabled cyber threats.

Increasing geopolitical competition between the US and China and recognising the role emerging technologies will play in the geopolitical landscape is starting to motivate the formation of new security agreements that include quantum technologies, such as AUKUS (US Department of Defense, 2023). The AUKUS pact was entered into by arguably NZ's closest military allies, the UK, US and Australia, in 2021, raising concerns that NZ may be left behind regarding access to and information on quantum computing and related quantum technologies (Lanteigne, 2021). This concern was reflected in the findings from this study, along with the recognition that NZ will need to collaborate with strong partners due to the limited domestic investment in this technology.

There are genuine reasons for NZ to join the technology pillar of the AUKUS agreement. As NZ is not currently building quantum technology domestically, it will be critical for the NZ Government to find ways to secure access to emerging quantum technologies and ensure these can be successfully integrated into the digital environment to protect national security and ensure economic stability. Agreements such as AUKUS are one way to achieve this. Should NZ fail to access and use quantum technologies, it may mean the government and military cannot fully integrate systems with traditional allies, receive necessary signals intelligence, or contribute meaningfully to existing arrangements such as the Five Eyes intelligence sharing agreement. The findings also describe how the ability for mutual benefit is now a stated prerequisite for nations that are more advanced in quantum technology to collaborate with other nations in this area. Therefore, a lack of ability to meaningfully engage and contribute could potentially threaten NZ's long-term

membership of existing allied agreements and leave NZ out of any potential future collaborative quantum technology projects.

However, joining agreements such as the AUKUS pact may jeopardise positive relationships with other nations, such as China, who strongly oppose AUKUS (The Embassy of the People's Republic of China in New Zealand, 2024), and there is still much debate on whether joining is in NZ's best interests (Clark & Brash, 2024; Gillespie & Patman, 2023). This debate is reflected in the findings of this study, with participants divided in their opinion on whether the NZ Government should maintain a middle ground and fiercely protect the ability for "independent" foreign policy development or "choose a side" and gain stronger alliances.

In January 2024, the NZ Government expressed a stronger interest in exploring options for NZ to join the non-nuclear pillar of the AUKUS pact (Dexter, 2023), but at the time of writing, any final decision on this remains unclear. However, decisions such as these reiterate the need for the NZ Government to develop a strong vision and strategy for emerging technology so that these choices are not made purely to address immediate political or economic pressures and any path chosen results in outcomes that support an agreed and multigenerational vision for the digital environment in NZ.

If the NZ Government maintains the status quo of balancing its international relationships and avoids signalling any closer security relationships with existing military allies, gaining access to quantum technology may be more challenging. In this scenario, the NZ Government may need to invest much more to secure greater self-reliance and enhanced technical resiliency by significantly increasing domestic cybersecurity and quantum technology capability. There are challenges to this approach, such as materials sourcing and skill shortages, that cannot be overcome quickly; however, some level of greater investment in domestic capacity is warranted regardless of the geopolitical situation to ensure an acceptable level of national digital sovereignty and protection moving forward.

6.3.3 International Governance of Quantum Technology

The findings clearly demonstrated that failing to build safety and security into the first technology revolution has meant NZ organisations are constantly battling a high-risk environment and experiencing significant harm. It has also proven much more difficult to build security retrospectively to create a safe digital environment, and most of the currently available resources are focused on this activity. This suggests that safety and security must be an upfront consideration in developing and evolving any emerging technology, including quantum computing.

As observed in the literature review, there is currently a lack of agreed international standards to measure progress in quantum technology development. International standards are also lacking in multiple other areas, such as the safety, security, and performance of quantum solutions currently under development or recently developed. This study found that developing these standards will be critical and that many nations intend to be involved in this process to ensure their national views are represented. Along with technical standards, there is a growing call for creating new international norms of responsible behaviour in cyberspace and more collaboration to reduce the risk and rise of nation-state cyber conflict. The development of new frameworks, understandings, and restraints to govern emerging technologies

effectively and safely is required, and the findings show that while NZ is a smaller country, it is vital that the NZ Government plays an active role in creating these.

Although the literature review suggested regulating the development and use of quantum computing to mitigate potential harmful use (Atkinson, 2020), this process would not be straightforward. Regulating the use of technology is challenging as it requires alignment of agreed values across borders and commitment from all parties to agreed use cases that may limit the perceived growth of individual nations. This will be even more challenging in a geopolitical security environment that appears to be growing more divisive and focusing on national sovereignty rather than strongly valuing and developing platforms for international cooperation.

There is an ethical imperative to drive the development of quantum use cases that benefit all of society, ensure fair access to quantum computing resources, and promote the use of these resources for good and not harm; however, the findings show that regulating technology use is ultimately seen as too challenging to succeed. Recent history supports this view and demonstrates that regulating the ownership or use of emerging technologies is unlikely to occur until serious harm has already occurred. For example, despite AI now being used for cyber-attacks and to generate and use data unethically, most jurisdictions globally have yet to issue any formal guidance on lawful behaviour when using this technology. The European Parliament passed a precursor to the *Artificial Intelligence Act* in June of 2023 (WEF, 2023), which intends to limit the use of AI for activities that impact individuals' security and human rights; however, this regulation will be too late to protect many from the harmful impacts suffered as a result of the oversharing of data that is already occurring in this space. As there is currently much greater discussion on the ethical impacts of AI and the seeds of legislative activity, this may make a good case study for how the use of quantum computing may be managed. Acts to support ethical AI use and legislation may offer potential ethical frameworks and guidance that would cross over for use with quantum computing technologies and support a smoother adoption.

Despite global regulation not being seen as a practical option in the current global environment, the increased pace of change from technology will still require global decision-makers to respond faster when acting to mitigate any harmful impacts and directing technology for positive use. Therefore, one tool that may speed up a global response is agreeing on "principles" rather than rigid or detailed "rules" or "law". Study participants demonstrated a desire to uphold an ethical paradigm in technology that reflects NZ's norms and values. Therefore, the NZ Government must take an active leadership role on the global stage to promote and role model the development of agreed principles in quantum technology development and use to protect the values aspect of NZ digital sovereignty while simultaneously exploring the complex notions of the "greater good". Building on the current literature discourse, the findings suggest this may involve supporting the development of quantum technologies that are:

Open: Make research easily available beyond early adopters, start-ups, and big technology companies

As seen in the literature review and findings of this study, much research is not approachable or available for wide consumption. For example, the NZ Government has only recently distributed information about quantum-resistant algorithms to a limited number of Managed Service Providers, leaving all other

organisations unaware. Additionally, advocating for wider access to domestic and international research laboratories and quantum resources should be prioritised. Open development also extends to sharing important research on ethical use cases for quantum technology and global cybersecurity. Nations and societal groups who do not have the means to complete this research themselves must not be excluded from critical findings that may further drive an increasing digital divide.

Resilient: Drive sustainability and security into base design considerations

Research that investigates the long-term potential impacts of all quantum technology and looks ahead generations to mitigate potentially harmful impacts on society must be supported.

Inclusive: Drive participation and enable opportunities across cultural contexts. Research the impact of different cultural norms

NZ has unique values, including those driven by indigenous culture. These should be investigated to ensure future technology use supports and embraces societal values rather than acts in opposition to these, causing harm. Additionally, greater research and workforce diversity must be enabled. Women are grossly underrepresented in cybersecurity, especially quantum science and technology, and pathways to encourage more diversity in these fields are needed.

Meaningful: Steer development towards meaningful applications not only for industry and business but society as a whole

Study participants expressed significant concern for the future direction of technology and stressed how important it will be to consciously harness this technology for the overall good rather than purely for commercial purposes.

How we plan to research, develop, and use quantum technologies will ultimately impact NZ society and making conscious choices in these areas is critical to achieving an outcome where this technology is widely supported and benefits all. The NZ Government must play a role in strongly advocating for and modelling the evolution and agreement of development principles on the global stage.

6.3.4 Driving Greater International Collaboration

Fragmentation across global economic and social environments poses a risk of a future whereby common systems to ensure financial stability and develop governance frameworks for emerging technology, such as quantum computing, are impossible. As a smaller player on the global stage, NZ will increasingly need to engage in savvy diplomacy and rely on the strength of multilateral organisations, such as the UN. The NZ Government should, therefore, play a role that primarily champions international collaboration and cooperation in quantum technology development and use and strongly promotes open forums and structures to develop shared understanding, common language, and agreed ethical principles on quantum technology.

Funding and contributing to strong international structures that can agree on acceptable technology use principles and investigate and mitigate against the potentially harmful impacts of emerging technology could ensure a global change in how technology such as quantum computing is developed and used. Strong global collaboration could also positively change the cyberthreat landscape. For example, if nations

banded together to develop and deliver a major cyber defence programme to identify cybercrime and effectively counter the malicious use of technology, the global cybercrime landscape would change. Increased divisiveness and an overly strong focus on national sovereignty work against a safe global digital landscape that operates freely and without borders. Technology already supports a truly global vision; however, the traditional methods of dividing nations and political lines conflict with this, and cyber criminals are currently benefitting from this scenario.

The findings of this study highlight that NZ cannot successfully develop, access, use, or protect against quantum technology alone, and any success in this area will rely strongly on international collaboration, cooperation, and compromise. The smooth and safe operation of quantum-enabled technology will require nations to cooperate and coordinate to develop common standards and norms, and the NZ Government must engage in strong diplomacy to champion this cooperation. To contribute meaningfully to conversations around quantum technology development and use on the global stage, the NZ Government must also maintain investment in quantum research and lift the commitment to building capability in technology ethics, quantum science, and diplomacy.

6.4 Research Question 3

Q3. What factors will contribute to NZ's cyber threat preparedness in a quantum computing-enabled world?

National readiness, organisational readiness, quantum and cybersecurity industry readiness, and global readiness will all contribute to NZ's level of cyber threat preparedness in a quantum computing-enabled world.

The literature review highlighted how current cybersecurity frameworks and models are often too generic to be useful, and the findings from the interviews conducted for this study confirmed this view. Additionally, the literature review suggested the need to create preparedness models and frameworks for specific technologies to aid in assessing cybersecurity preparedness. Therefore, to fully present the factors that will contribute to NZ's cyber threat preparedness in a quantum computing-enabled world, a conceptual model of quantum computing cybersecurity preparedness tailored for the NZ landscape was created.

6.4.1 The Quantum Computing Cybersecurity Preparedness Model

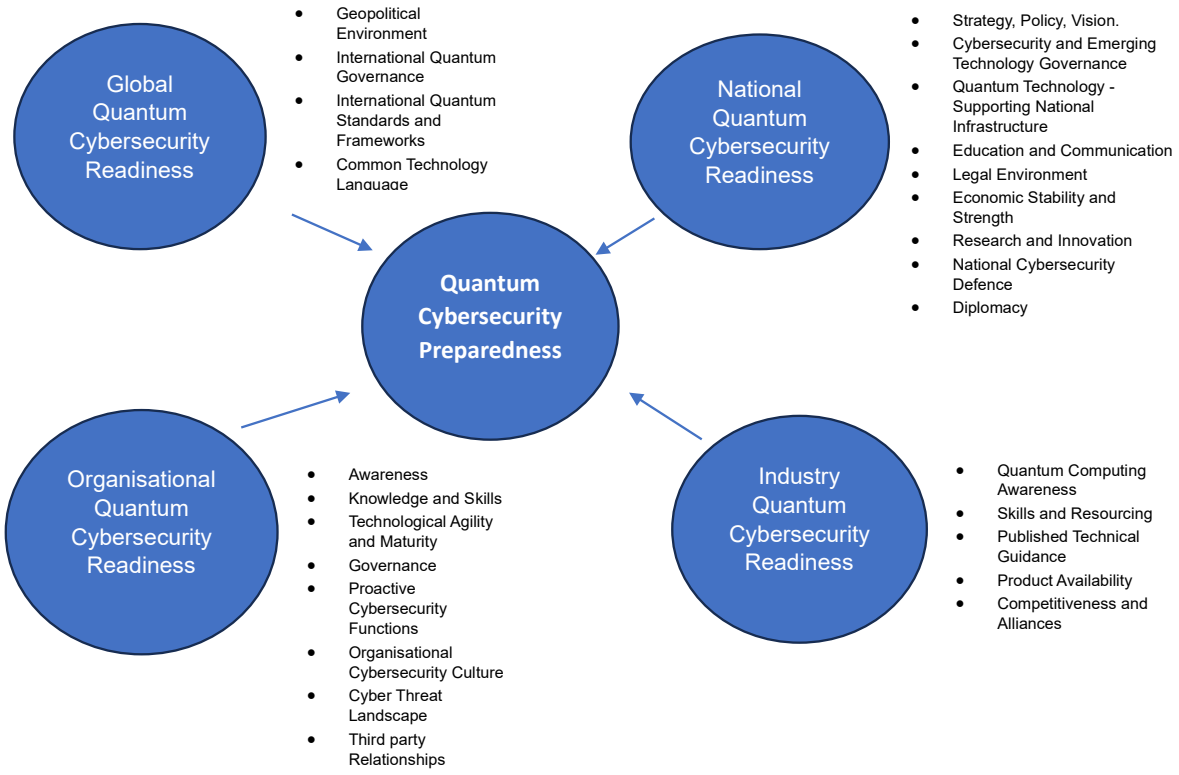
The QCCP model seen in Figure 16 encompasses relevant ideas of readiness, maturity, and resiliency from previous cybersecurity studies outlined in the literature review by Kurnia et al. (2009), Ogunyemi and Johnston (2012), and Bahuguna et al. (2019), whilst also including cybersecurity readiness suggestions that are unique to addressing quantum cybersecurity threats from recognised industry leaders such as NIST (2020) and Mosca (2018). Critical findings from the document and interview data analysis phases of this study are incorporated into the model to drive specificity and ensure contextual relevance for the current NZ landscape. The seven primary themes described in Chapter 5 of this study are reflected across the model and heavily influence the focus and priority of the factors represented within.

The literature review described three high-level areas that may impact preparedness to face emerging cybersecurity threats that quantum computing may enable: national readiness (Bahuguna et al., 2019), organisational readiness (Eilts, 2020; Wibowo et al., 2020), and industry readiness (Lees et al., 2018). The findings from this study concurred that readiness factors in all these areas would impact levels of quantum

cyber threat preparedness for NZ; however, the interview and document analysis findings also strongly demonstrated that factors of global readiness would contribute to NZ's preparedness for quantum computing enabled threats and therefore this aspect has been included in the model.

Figure 16

Quantum Computing Cybersecurity Preparedness Model



The quantum cybersecurity preparedness model comprises four primary areas in which the lower-level preparation factors are grouped. The overarching areas and each preparation factor are explained as follows:

6.4.1.1 Global quantum cybersecurity readiness

Global quantum cybersecurity readiness involves a collaborative geopolitical environment that promotes and upholds safety, security, and cultural norms in the digital world.

This includes creating and maintaining internationally agreed standards, successful collaborative forums for open global debate, secure supply chains and accessibility to quantum technologies, and the widespread adoption of quantum-safe systems that underpin global economies.

Table 10 describes the preparation factors underlying the area of global quantum cybersecurity readiness that make up the QCCP model and will contribute to NZ's preparedness to face cyber threats in a quantum computing-enabled world.

Table 10

Global Quantum Computing Cybersecurity Preparedness

Factors	Description	Related themes
Geopolitical environment	• Degree of open versus protectionist geopolitical landscape	• Develop quantum technology for digital sovereignty • Influence and protect behavioural norms in technology
International quantum governance	• Global forums for international collaboration in quantum technology development • Balanced IP laws • Clear quantum technology development strategy and pathways • Equal and freely moving supply chains for quantum technology infrastructure and resources	• Importance of trusted relationships • Influence and protect behavioural norms in technology • Protect national security and the economy from the impacts of quantum technology
International quantum standards and frameworks	• Standardised measurement system for quantum computing development progress • Availability of a complete and inclusive set of quantum technology use cases • Internationally agreed standards for quantum technology development and implementation • International frameworks for ethical use of quantum technologies • Availability of recognised cybersecurity frameworks that include specific quantum technology threat and mitigation detail	• Influence and protect behavioural norms in technology • Protect national security and the economy from the impacts of quantum technology
Common technology language	• Accepted global rhetoric on quantum computing (emphasis on positive and equal versus negative, powerful), including the positive framing of quantum and cybersecurity threats • Availability of a common language to communicate quantum technology and cyber threats	• High-risk environment • Varied cyber maturity levels • Influence and protect behavioural norms in technology

6.4.1.2 National quantum cybersecurity readiness

National quantum readiness is the ability of the NZ Government to provide an enabling environment for the detection of quantum-vulnerable systems and sufficient protection against quantum computing threats. This includes maintaining political and economic stability and ICT infrastructure; developing and publishing clear cybersecurity strategies and roadmaps for transitioning to a post-quantum world; supporting quantum research and development; contributing to international thought leadership; and developing and enforcing appropriate policy and law.

Table 11 describes the preparation factors underlying the area of national quantum cybersecurity readiness that make up the QCCP model and will contribute to NZ's preparedness to face cyber threats in a quantum computing-enabled world.

Table 11

National Quantum Computing Cybersecurity Preparedness

Factors	Description	Related themes
Strategy, policy, vision	• Transparent NZ vision and strategy for cybersecurity and quantum technology (reflects an understanding of NZ values and unique digital sovereignty) • Transparent quantum cyber threat national risk assessment • Clear published roadmaps for the adoption of quantum technology • Clear, published roadmaps for the adoption of solutions to defend against quantum cybersecurity threats • Strategic technology planning capacity and capability, including cross-functional skills to address ethical issues in emerging technology	• Applying a strategic lens • Developing an NZ approach • Varied cyber maturity levels • High-risk environment
Cybersecurity and emerging technology governance	• Cybersecurity and emerging technology governance procedures, including strongly defined national roles and responsibilities and transparent national reporting mechanisms • Capability for technology industry oversight • Demonstrated leadership in cybersecurity, including the display of minimum best cybersecurity practices, early transition to quantum-safe algorithms, and early adoption of quantum cybersecurity technology	• Insufficient governance mechanisms • Developing national capacity • Varied cyber maturity levels • High-risk environment
Quantum technology – Supporting national infrastructure	• Understanding and inventory of current and future national infrastructure needed to support quantum technology • Development and deployment of hybrid and digital infrastructure that supports quantum technology initiatives, including quantum cybersecurity, communication, and ICT systems such as QKD networks • Reliable access to quantum technologies, contributing supporting technologies, and international raw material supply chains • International drive to advance versus reject emerging cybersecurity and quantum technology-based solutions	• Developing national capacity • Develop quantum technology for digital sovereignty • Protect national security and the economy from the impacts of quantum technology

Factors	Description	Related themes
Education and communication	• Widespread cybersecurity awareness programmes that address emerging quantum computing threats • Formal education and qualification pathways (at all levels) in cybersecurity and quantum technology • Support to ensure greater diversity in technology programmes • Receipt and distribution of timely, transparent, and contextually relevant cyber threat intelligence • Ability to translate and widely disseminate appropriate research findings to industry	• Developing national capacity • Varied cyber maturity levels
Legal environment	• Sufficient regulation governing cybersecurity, including mandates for minimum security baselines and for transitioning to quantum-resistant algorithms • Applicable laws and legal guidance governing quantum technology use and misuse • IP law that considers relevant characteristics of emerging technology, such as quantum and NZ's unique position • Technology product cybersecurity certification standards • Capacity to enforce regulation, penalise nonadherence, and prosecute cyber criminals	• Developing national capacity • Varied cyber maturity levels • High-risk landscape • Protect national security and the economy from the impacts of quantum technology
Economic stability and strength	• An economy that is stable, open, and attractive for business investment • A stable political system • Sufficient domestic labour markets • Immigration and work environments designed to attract and retain global quantum and cybersecurity talent	• Developing national capacity • High-risk landscape • Protect national security and the economy from the impacts of quantum technology
Research and innovation	• Establishment, funding, and maintenance of quantum and cybersecurity research programmes and centres of excellence (such as the existing Dodd–Walls Centre). • Business and innovation incubators for quantum technologies (including mentoring and start-up funding initiatives) • Public/Private collaboration	• Developing national capacity • Develop quantum technology for digital sovereignty • Importance of trusted relationships
National cybersecurity defence	• Sufficient cyber emergency response skills and resources to protect national security and support NZ organisations in planning, preparing, and responding to cyber threats. • Tested incident response plans for significant cross-industry quantum computing-enabled cyber incidents	• Developing national capacity • Protect national security and the economy from the impacts of quantum technology

Factors	Description	Related themes
Diplomacy	• Skilled and valued diplomatic capacity • Access to and active participation in international forums and agreements focused on quantum technology (including forums on the ethical development and use of quantum technology and technical standards development for quantum technology) • Opportunities for open disclosure and international information sharing around quantum technology development and cyber threat impacts and mitigation • Opportunities to collaborate on international cybercrime investigation and response	• Importance of trusted relationships • Developing an NZ approach • Influence and protect behavioural norms in technology • Protect national security and the economy from the impacts of quantum technology

6.4.1.3 Organisational quantum cybersecurity readiness

Organisational quantum cybersecurity readiness is described in this model as sufficient people, knowledge, skills, technology, governance, and IT infrastructure within an organisation to identify, prepare, detect, protect, respond, and recover from quantum computing cybersecurity threats.

Organisational readiness includes the inventory of quantum-vulnerable systems and processes, cryptographic and hardware agility, threat understanding and analysis, cybersecurity awareness and culture, and quantum mitigation strategies and governance.

Table 12 describes the preparation factors underlying the area of organisational quantum computing cybersecurity readiness that make up the QCCP model and will contribute to NZ's preparedness to face cyber threats in a quantum computing-enabled world.

Table 12

Organisational Quantum Computing Cybersecurity Preparedness

Factors	Description	Related themes
Awareness	• General cybersecurity awareness levels at all levels of an organisation • Understanding and recognition of the potential cybersecurity threats posed by quantum computing at all levels of an organisation • Understanding of quantum technologies and terminology used in computation, communication, and security at all levels of an organisation	• Varied cyber maturity levels • Developing national capacity
Knowledge and skills	• Availability of cybersecurity and quantum computing (including networking and cryptographic) knowledge and skills • Appropriate levels of reliance on third-party skills and resources • Availability of timely and contextually relevant general and quantum cyber threat intelligence • Availability of timely and contextually relevant implementation guidance for quantum cybersecurity solutions • Opportunities and access to extended peer networking and cyber mentoring	• Varied cyber maturity levels • Developing national capacity • Importance of trusted relationships • Developing quantum technology for digital sovereignty
Technological agility and maturity	• Cryptographic agility • IT infrastructure agility • Capacity for hardware and software infrastructure to adopt new technologies and protocols, including the operation of quantum-resistant algorithms • Capacity for interoperability with quantum systems • Reliance on legacy technology • Access to quantum technology (infrastructure, products, services)	• Varied cyber maturity levels • High-risk environment • Protect national security and the economy from the impacts of quantum technology

Factors	Description	Related themes
Governance	• Strategic technology planning capacity • Relevant business and IT security policies that incorporate the development, use and defence of quantum computing • Cybersecurity budget aligned with long-term strategic plan • Formal cybersecurity framework alignment • Cybersecurity maturity level assessment • Oversight and management of third-party suppliers • Defined cybersecurity RASCI • Cybersecurity representation at the board level of an organisation • Regulatory landscape understanding and compliance • Formal quantitative and qualitative cyber risk assessment and management that incorporates emerging and uncertain risks, such as those posed by quantum computing	• Applying a strategic lens • Insufficient governance mechanisms • Varied cyber maturity levels
Proactive cybersecurity functions	• Cybersecurity improvement plans with agreed minimum security hygiene baseline • Documented and tested incident response playbooks for quantum computing-enabled cyber threats • Plans for transitioning to quantum-safe systems, including migration to quantum-safe algorithms	• Varied cyber maturity levels • Developing national capacity • Protect national security and the economy from the impacts of quantum technology
Organisational cybersecurity culture	• Understanding of organisational risk appetite (risk seeking versus risk-averse culture) and consideration in decision-making processes • Level of organisational acceptance (versus resistance) to change and uncertainty • Level of perceived value and trust in cyber security function • Accountability versus blame focus • Support structures for cybersecurity professionals • Quality focus in cybersecurity planning and operations • Cyber incident acceptance level	• High-risk environment • Insufficient governance mechanisms
Cyber threat landscape	• Volume and severity of active general cyber-attacks targeting NZ organisations • Level of quantum computing enabled threat impacts seen in the wild	• High-risk environment

Factors	Description	Related themes
Third-party relationships	• Confidence in the suitability and reliability of third-party/vendors' quantum and cybersecurity products, solutions, and service levels • Confidence in the threat intelligence information shared between public, private organisations, government, and academia • Formal opportunities for open disclosure and sharing (organisational and peer level) around quantum technology development and cyber threat impacts and mitigation • Peers, industry competitors, associated businesses, external organisations, and standards bodies drive to advance (versus reject) emerging cybersecurity and quantum technology-based ideas and products • Willingness to support recommended quantum and cybersecurity products and solutions • Defined and achievable service level agreements and security level agreements with third-party service providers • Supply chain reliability	• Importance of trusted relationships • Varied cyber maturity levels

6.4.1.4 Industry quantum cybersecurity readiness

Industry quantum cybersecurity readiness is seen as the presence of a vibrant and competitive quantum and cybersecurity technology market, delivering timely, cost-effective, and reliable products and services that identify and protect against quantum cybersecurity threats.

Industry readiness encompasses supply chain awareness and skills, published industry standards and guidance and innovative products for discovering quantum vulnerabilities and compatible new technology. It also requires a healthy competitive environment where consumers have choices and suppliers have strong partnerships to deliver quantum-resistant solutions.

Table 13 describes the preparation factors underlying the area of industry quantum cybersecurity readiness that make up the QCCP model and will contribute to NZ's preparedness to face cyber threats in a quantum computing-enabled world.

Table 13

Industry Quantum Computing Cybersecurity Preparedness

Factors	Description	Related themes
Quantum computing awareness	• Supply chain vendor awareness of cybersecurity threats posed by quantum computing • Supply chain awareness of suitable defence products and strategies for NZ organisations to combat quantum computing cyber threats	• Varied cyber maturity levels • High-risk environment
Skills and resourcing	• Cross-functional skills available to support quantum technology development • Availability of resources with skills required to support cybersecurity implementations in a quantum computing-enabled world	• Varied cyber maturity levels • High-risk environment • Developing national capacity
Published technical guidance	• Availability of published reliable and proven guidance on quantum cybersecurity suitable for widespread use • Access to published frameworks and standards for ethical quantum computing development	• Protect national security and the economy from the impacts of quantum technology
Product availability	• Availability of standardised and reliable products for securing existing IT networks and new quantum and hybrid networks • Opportunities for international collaboration in quantum and cybersecurity technology development • Access to funding and support for innovation and commercialisation of quantum and cybersecurity products • Timely quantum and cybersecurity product updates and support • Compatible product availability • International supply chain reliability	• Developing national capacity • Develop quantum technology for digital sovereignty • Protect national security and the economy from the impacts of quantum technology • Importance of trusted relationships
Competitiveness and alliances	• Open market to drive competition • Alliances to support quantum cybersecurity advances • Levels of collaboration, trust in third party and customer relationships	• Importance of trusted relationships • High-risk environment

The QCCP model clarifies the concept of quantum cybersecurity preparedness by outlining all factors identified in this study that will contribute to NZ's cyber threat preparedness in a quantum computing-enabled world. However, the QCCP model has some limitations. Aspects of personal individual preparation for quantum computing cyber threats are not fully represented. For example, while general societal awareness and knowledge building are included in the model as a necessary first step to quantum technology adoption and threat protection, there will potentially be further steps an individual computer user must undertake to successfully contribute to NZ's overall preparedness. However, as the investigation of individual preparation was not in the scope of this study, preparedness actions of this nature are

excluded. Additionally, as this model is conceptual, it lacks low-level detail and, therefore, is intended to give an overview of the primary factors that will contribute to NZ's preparedness, as found in this study only. The model is not intended to be an extensive strategy or detailed implementation guide for preparation.

6.5 Practical Preparedness Guidance for NZ Organisations

6.5.1 Introduction

In alignment with a lens of classical pragmatism and a pragmatic methodology that promotes the creation of knowledge deemed useful by those who must implement it, Section 6.5.2 provides initial guidance for NZ organisations attempting to prepare for the threats that quantum computing may pose. Due to clear findings that NZ organisations are currently overwhelmed by the volume of work the current high-risk landscape is driving, this guidance is tailored to address the immediate or near-term concerns that quantum computing may pose and is designed to be shared as a practical starting point for preparation.

6.5.2 Preparing for a Quantum-Computing Enabled Threat Landscape

The development of quantum computing and related quantum technologies will impact cybersecurity in NZ and NZ organisations. Many facets of this topic remain uncertain, and all use cases and scenarios involving these developments are yet to be explored; however, there are pragmatic "low regret" actions organisations can immediately consider undertaking to prepare for a quantum computing-enabled cyber threat landscape.

6.5.2.1 What are the cyber threats that quantum computing will pose?

The possible threats are varied. In addition to new technical attack vectors, quantum computing may also exacerbate current issues such as misinformation and the digital divide. However, the most relevant problem for immediate business consideration is that quantum computers are expected to break current public key cryptography. NIST anticipates that this may occur by 2030. This creates two cyber threats:

SNDL attacks

This threat is now active and refers to adversaries capturing and storing valuable encrypted data today and then decrypting it once sufficiently large, fault-tolerant (LFT) quantum computers are available. Note that this attack is only relevant to information that retains its value in the future.

Breaking of RSA and ECC cryptography

RSA and ECC remain the two most widespread public key algorithms used to currently encrypt data. Shor's quantum algorithm may break both once a sufficiently LFT quantum computer is available. This will allow attackers to forge RSA and ECC digital signatures and pose risks to functions such as secure web browsing and zero-trust architectures.

6.5.2.2 What are the solutions?

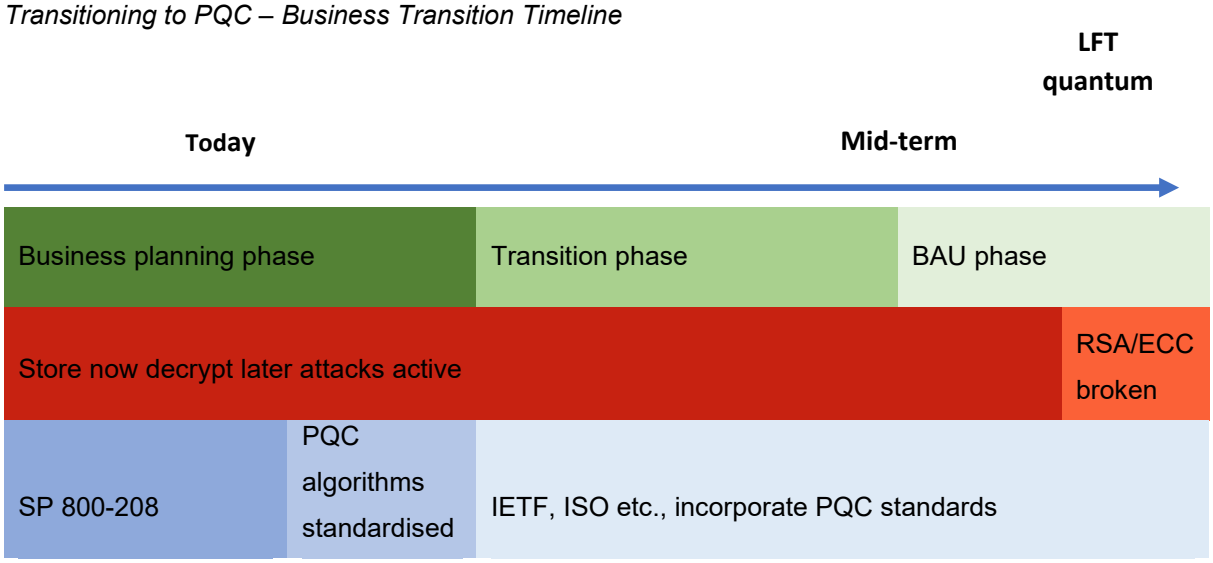
The two main solutions proposed to combat these threats are PQC and quantum cryptography (including QKD and quantum random number generation). While quantum cryptography looks promising in the long

term, transitioning to PQC is a more practical option for most NZ businesses due to its lower cost and the possibility of integrating it into existing infrastructure.

NIST has now standardised the first PQC algorithms, and therefore, a further push for adopting quantum-resistant technology will be seen over the next 2 years to promote preparedness.

Figure 17

Transitioning to PQC – Business Transition Timeline



Note. Adapted from "Transitioning Organisations to Post-Quantum Cryptography" by D. Joseph, 2021, *Nature*, *605*(5), 237–243. https://doi.org/10.1038/s41586-022-04623-2. Copyright 2022 Springer Nature Limited.

6.5.2.3 Do I need to act right now?

Whilst all businesses should create a robust quantum-safe strategy to migrate to a post-quantum cryptographic world, not all businesses need to address this issue with the same urgency.

If your business stores data with a value that exceeds 5 years (for example, trade secrets, IP, medical records):

- Consider a plan to transition to PQC immediately. In the context described above, the data you hold today may already be at increasing risk from SNDL attacks.

If you are designing and planning infrastructure that has an anticipated lifespan of 20–30 years plus (such as some operational technology, vehicles, etc.):

- Consider immediately creating a clear strategy around transitioning to PQC wherever possible.

If neither of the above scenarios is relevant to your business, you have more time to plan; however, there are still actions that you can take now to make the journey smoother.

6.5.2.4 Actions to take now

Follow developments on PQC and quantum computing

Subscribe to updates from NIST, CISA, and other agencies working to develop and encourage the adoption of new standards.

- Post-Quantum Cryptography | CSRC (nist.gov)

- NZISM – ISM Document (gcsb.govt.nz) (Specifically Section 17 – Cryptography)
- Homepage | CISA

Build awareness around the quantum threat

Quantum computing and its threats need to be demystified and understood at all levels of an organisation. Socialising this threat early will help ease the eventual transition and ensure your business has the skills and knowledge to assess your risk. Consider adding this risk to your general risk management framework for assessment as the likelihood of impact gets closer.

Build a cryptographic inventory

Identify where public key cryptography is used in your products, services, and infrastructure. Once this is completed, you can identify where your organisation uses cryptographic schemes that are at elevated risk, as these will need to transition to PQC first. For example, this is likely to be where key exchange algorithms are used in the context of confidentiality.

Maintain an inventory of your critical data, systems, and processes, as this will also assist in clear prioritisation for transitioning activities.

Plan for crypto agility (The ability to switch between cryptographic algorithms seamlessly)

It is predicted that organisations will need to change and layer cryptographic algorithms more frequently in the future due to the differing attributes and uncertain long-term security of PQC:

- Ask your vendors about the level of crypto agility in their products and services
- Adopt abstraction layers on centrally managed toolkits and services to minimise the effort required for further cryptographic changes
- Ensure tooling can manage adjusted data formats and sizes
- Create a centralised library of cryptographic services to abstract algorithms in use from the infrastructure
- Identify data field and size dependencies in protocols, software, databases, and data stores. Adjust any that assume current fixed field sizes

Ensure your IT policies mandate the swift adoption of TLS releases

External-facing TLS systems are often more flexible with respect to quick migrations. A quantum-safe TLS version should be ready before the negative impacts of quantum computing are felt, and businesses should commit to the swift adoption of upgrades to build up experience with PQC implementations.

Inventory devices and technology that may not transition smoothly

All known quantum-resistant algorithms being considered for standardisation have performance challenges, such as requiring longer key lengths and greater processing times, compared to those used today. This means some devices (particularly resource-constrained, older technology, operational technology, and some IoT devices) required to be online may not be able to adopt PQC. Understand whether you have any of these devices in your network so the use of hybrid solutions or replacements can be planned.

Create, update, and test cyber incident response and business continuity plans

All the potential outcomes of using a quantum computer to perform cyber-attacks are unknown; however, it is likely that combining quantum computing abilities with other advanced technologies, such as AI, will enable new or enhanced cyber-attack vectors and impacts beyond the known impact on cryptography. Despite limited detailed information on the nature of future cyber-attacks that utilise quantum computing power, all organisations can and should immediately undertake the proactive planning and creation of cyber incident response plans, playbooks, and business continuity plans.

Focus on identifying and planning for any potential shared business process impacts resulting from a large-scale cyber incident (such as the inability to make electronic payments or access system critical system resources) initially. Understand how (and how long) critical operational processes could be undertaken should a quantum attack impact just your organisation and then an entire industry or supporting industry (such as banking).

Areas to consider when formulating response plans include:

- Ensuring clear roles and responsibilities and escalation paths are identified for cyber incident response
- Engagement of other suppliers/alternative supply chains and resources in the event of national or industry-level incidents
- Communication and public relations methods and key messages
- Insurance requirements
- Engagement and notification of law enforcement, government, and other regulatory bodies
- Segregation of and access to backup systems
- Existence of “break-glass” solutions (i.e., Do you have a quick means for extending an agreed individual’s system access rights in exceptional cases (only to be used when normal processes are insufficient))?
- Who will own and update these plans as new information on attack methods becomes available?
- How you will regularly test your plans to ensure they are fit-for-purpose and up-to-date, that the team understands all roles, and that they work together seamlessly to respond quickly under pressure

Apply pressure on your peers and supply chain to adequately prepare

In the highly interconnected global digital landscape, all parties must prepare for quantum computing so that NZ can remain secure and minimise any potential impacts.

Encourage all industry peers, competitors, and third-party suppliers in the supply chain to have their own suitably detailed and tested response plans for large-scale threats.

Encourage all supply chain peers to join together and participate in discussions and simulated events that test potential cyber incident scenarios to gain clarity on cross-industry roles and responsibilities,

communication responses and prioritisation of operational activities and recovery. Consider hosting a simulation, discussion or education event involving multiple critical suppliers focused on brainstorming and agreeing on how all parties would respond in the event of a quantum computing-enabled cyber incident.

6.5.2.5 Why act early?

This cryptographic transition is wider and more complex than previous cryptographic migrations and, therefore, requires more time for both planning and execution.

Acting early will:

- Allow time to iron out bugs, train teams, and prepare for what could prove a lengthy process
- Ensure you are ahead of any regulatory pressures to adopt new standards
- Avoid investment in tools that may prove unsuitable in the medium term

6.6 Conclusion

Chapter 6 discussed the findings first presented in Chapter 5, and the main research questions and sub-questions were answered. The results described a low level of awareness around the cyber threats quantum computing may pose, along with no current preparation or intent from NZ organisations to prepare for these threats. A high-risk operating landscape with varied cyber maturity levels, poor strategic emerging technology planning, and limited quantum-supporting infrastructure, industry, and capability were all seen in this study, and it was concluded that NZ organisations were currently insufficiently prepared to face the cyber threats that quantum computing may pose.

This chapter discussed actions that NZ organisations and the NZ Government could take to increase NZ's cyber resiliency and enable greater preparation for quantum computing-enabled cyber threats. These actions included investing in quantum-supporting infrastructure and industry, improving the quantum and cybersecurity skills pipeline, introducing more cybersecurity regulation, considering the pace of technology development, focusing on quality, and reframing the way quantum technology threats are communicated.

The role the NZ Government could play internationally when discussing the ethical and security impacts of quantum computing was investigated, and the importance of clarifying a strong national stance on these issues and playing a role that strongly promotes and advocates for international cooperation and collaboration in quantum technology and cybersecurity was discussed.

The discussion also determined that organisational, industry, national, and global readiness factors will impact NZ's preparedness to address quantum computing-enabled cyber threats in the future, and a quantum cybersecurity preparedness model was presented to describe these factors. Finally, the chapter suggested practical ways in which NZ organisations can start to prepare for quantum computing-enabled cyber threats.

Chapter 7: Conclusion

Chapter 1 introduced the research topic of quantum computing-enabled cyberthreat preparation in NZ, outlined the thesis structure, and discussed the motivation behind conducting this study. The literature review presented in Chapter 2 then described the challenges in developing quantum computing technology, demonstrated the threats it poses to information technology systems and outlined potential solutions. Chapter 3 outlined existing theories in the literature that provide a framework for analysing the data derived from this study.

The concerns and issues described in Chapter 2 led to the formation of the research questions for this study, focusing on the awareness and preparation of NZ organisations and the NZ Government to face quantum computing-enabled cyber threats. Chapter 4 described a suitable methodology for investigating the research questions and outlined the interview and document analysis methods used for this study.

The findings derived from following these methods were presented in Chapter 5. These findings demonstrated low quantum computing-enabled cyber threat awareness levels and no proactive preparation for these threats. The results also described the need for the NZ Government to actively champion strong international collaboration in forming globally accepted quantum technology development principles. Chapter 6 further analysed and discussed the findings to link them to the literature review and, importantly, answer the study's main research questions and sub-questions. Recommendations were provided for NZ organisations to prepare for quantum computing-enabled cyber threats. A model that described the key factors that will influence cybersecurity in NZ in a quantum computing-enabled world was presented.

This chapter concludes the thesis by summarising the research, highlighting its contributions to the broader area of quantum computing-enabled cyberthreat preparation, describing the research limitations, and providing suggestions for further research.

7.1 Summary of Research

This research aimed to determine whether NZ organisations were aware of and prepared for the potential cyber threats that emerging quantum computing technology may pose. It further aimed to explore the role the NZ Government could play when discussing and forming international policy on the ethical and secure development and use of quantum technologies. Finally, it aimed to clarify the key factors contributing to NZ's cybersecurity preparedness in a world enabled by quantum computing.

This study targeted NZ cybersecurity professionals and experts in technology and policy to understand their lived experiences and levels of quantum risk awareness and preparedness in NZ organisations. Additionally, publicly available documents presenting global strategies and viewpoints on quantum technology and cybersecurity were analysed to determine the NZ Government's role on the global stage in this space and identify further factors that may influence NZ's cybersecurity preparedness in a quantum-enabled world.

Overall, this study demonstrated that NZ organisations were insufficiently prepared for the cyber threats that quantum computing may pose. NZ organisations' awareness of these potential threats was low, and

no organisations were found to be proactively preparing for these threats. These findings are concerning as the evolution of quantum computing and its supporting technologies are now widely seen as having the potential to disrupt economies and impact national security. The threat quantum computers pose to cryptographic algorithms is theoretically proven, and national governments globally are starting to encourage and mandate the transition to quantum-resistant solutions to prevent harm.

The findings highlight that NZ organisations are already at risk from quantum computing cyber threats. SNDL attacks are likely underway, capturing sensitive data from critical NZ organisations for later decryption with a quantum computer. Additionally, even if a quantum computer sufficiently advanced enough to break current cryptosystems is more than 10 years away, the findings highlight that the time frame necessary for transitioning to new secure cryptographic schemes is sufficiently lengthy that there is an urgent need for NZ to prioritise the development, standardisation, and implementation of post-quantum cryptographic systems to avoid the severe global consequences and privacy disaster that the fall of the PKI could bring.

The findings conclude that NZ organisations are operating in an environment of high cyber risk with cybersecurity maturity levels insufficient to mitigate these risks. This situation negatively impacts organisations' ability to address current cyber threats and, combined with a lack of strategic cyber planning, will severely limit proactive preparation for emerging quantum computing-enabled threats.

This study recommends increasing cyber maturity and national cyber capacity to reduce risk to manageable levels and enable available resources for strategic cyber threat preparation. A theme of insufficient cyber governance was seen throughout the findings, and more robust mechanisms to govern cybersecurity and emerging technology at national and organisational levels are required. There is little clarity around accountability and responsibility for cybersecurity or cyber incidents in the increasingly complex and interconnected NZ landscape. Greater effort will be necessary to define responsibility and accountability for all parties, ensure security obligations are clear, and reduce a culture that still looks to attribute blame after a cyber incident. The findings also described the need for and the potential acceptance of more regulatory levers to lift cyber maturity levels and lower cyber risk in NZ. Following international trends seen in this study, the NZ Government could introduce more legislative measures across several areas. These include greater general cyber resiliency requirements, defining organisational and senior leadership risk accountability, and introducing more mandates for technology-managed service and critical infrastructure providers. The findings conclude that introducing mandates to ensure critical NZ organisations transition to quantum-safe algorithms in a timely fashion is required immediately, as this action is unlikely to occur voluntarily.

Cybersecurity and quantum computing awareness levels must also be raised so that NZ organisations can comfortably adopt quantum technology and protect against any adverse impacts of quantum computing. A greater understanding of these issues is needed at board levels in NZ organisations to ensure cybersecurity teams receive the support they require to implement positive change and lift cybersecurity maturity levels. Additionally, NZ organisations should invest more time, money, and attention to implementing fundamental security controls sustainably. NZ cyber professionals require support to introduce reliable controls such as complete systems and cryptographic inventories that would allow them

greater visibility and control over networks, thereby enabling protection against current and future threats that quantum computing may pose.

This study found that NZ organisations lack trust in the public agencies tasked with addressing cybersecurity. These agencies are seen as under-resourced and lack the skills and mandate to help NZ organisations prevent, protect, and respond sufficiently to cyber threats. Therefore, developing greater national capacity and capability for public cybercrime response, investigation, and law enforcement will also be essential to ensure the consequences of malicious or negligent activity in cyberspace are managed, and trust in this crucial national function is strengthened.

Many NZ cybersecurity professionals consider quantum computing esoteric, confusing, highly theoretical, and unapproachable. Demystifying this area will be crucial to ensure NZ develops a skilled and aware professional community that can harness quantum computing benefits and protect against quantum computing threats. The study uncovered several areas where the language and framing used to describe cyber threats, quantum technology, and cybersecurity may negatively impact NZ organisations' ability and drive to prepare proactively for cyber threats. Firstly, it was clear that negatively framing the potentially severe impacts that quantum computing cyber threats may pose to NZ drove a lack of accountability for these threats. Secondly, the phrase "it's not if, but when" used to highlight the ubiquitous nature of cyber-attacks was seen in this study as enhancing a feeling of apathy and helplessness towards cyber threat preparation. The findings suggested that rather than encouraging more preparation for cyber threats, using this phrase may result in the opposite response from NZ organisations and prevent proactive preparation. Finally, the findings suggest that the growing cybersecurity and quantum technology rhetoric centred around combative and inflammatory terms such as battle, supremacy, race, and adversaries should be explored further to determine the result this is having on the way nations and societies think about and address cybersecurity and emerging quantum technology.

This research uncovered surprisingly high levels of helplessness, apathy, and resignation from NZ cybersecurity professionals, leading to low expectations and standards when implementing cybersecurity controls. This finding is critical to advance the understanding of the landscape, as the high level of acceptance of cyber-attacks as a "normal" part of operating in a digital landscape may contribute to a culture where NZ organisations aim to "just do enough" rather than implementing quality solutions. Without addressing these issues, NZ will continue to struggle in a cyber environment of low maturity, high successful attack rates, and professional burnout, ensuring neither current nor quantum computing threats are sufficiently addressed.

The future availability of quantum infrastructure will be crucial to ensure NZ can defend against quantum computing threats. NZ will not be the first in the world to build a quantum computer as the nation has not invested heavily in this technology; however, this study shows that starting to develop quantum-supporting infrastructure, such as QKD networking, could be vital to building trust in these technologies and encouraging their adoption and use in NZ organisations. The development of quantum-supporting infrastructure in NZ will require establishing a stable quantum industry presence to provide quantum systems, networks, and expertise to assist organisations in transitioning to these solutions. NZ should consider following the lead of other nations globally who are prioritising the establishment of quantum industries to ensure the benefits of these technologies can be harnessed for protection.

Based on the qualitative analysis of interview and document data, it can be concluded that the NZ Government must play an active role in global efforts to mitigate the ethical and cybersecurity impacts of quantum computing technologies and ensure that values important to New Zealanders, such as democracy, equality, freedom, and openness are reflected in any multinational approach to these technologies. However, many nations emphasise the use of quantum technologies to achieve national sovereignty, and the study findings suggest the NZ Government may struggle to be heard on the global stage and maintain accessibility to advanced quantum technology in a global environment that emphasises national digital sovereignty over international partnerships.

Due to its limited domestic investment in this area, NZ will need to rely on international relationships to access and use quantum technology. Maintaining research and development in quantum technology will be necessary for NZ to ensure accessibility to the quantum supply chain of materials and innovative solutions, as traditional allies will only collaborate and share advancements in quantum technology if both parties can benefit the relationship equally. Therefore, NZ must continue to invest and grow quantum and cybersecurity capabilities to have something valuable to add to the global landscape.

This study concludes that strongly advocating for international cooperation and collaboration in this space over growing protectionist rhetoric will be critical to maintaining a global quantum ecosystem where no nations, including NZ, are left behind. The need for the NZ Government to develop a strong, values-centric national strategy and vision for cybersecurity and quantum technology is evident. The NZ Government must aggressively, collaboratively, and transparently decide on their approach to domestic quantum technology development and use, become a role model, and promote this agreed stance globally.

Finally, this study uncovered a range of global, national, industrial, and organisational factors influencing NZ's preparedness to face cyber threats in a quantum computing-enabled world. At a global level, the NZ Government should aim to positively impact the geopolitical environment, global quantum governance, international standards and development frameworks, and the language used to describe this emerging technology. Nationally, NZ requires robust cyber and emerging technology governance, clear strategy, quantum cybersecurity awareness programmes, sufficient quantum-supporting infrastructure, a supportive regulatory environment, a stable economy, ongoing technology research and innovation, sufficient national cyber defence, and strong diplomatic capacity. The cybersecurity and technology industry must contribute to readiness with suitable products, technical guidance, quantum cybersecurity skills and awareness, and open markets and alliances. Finally, NZ organisations require strong awareness, skills, technology agility and maturity, cyber governance, proactive cybersecurity functions, cyber-focused cultures, third-party relationships, and a manageable cyber threat landscape.

Each of these readiness areas requires equal focus, highlighting the extremely interconnected nature of the cybersecurity landscape. All parties must contribute to keeping NZ safe from the cyber threats that emerging technologies will pose and building strong, trusted relationships between these areas, which is seen in this study as critical for enabling success.

7.2 Research Limitations

Research to satisfy a doctoral qualification is conducted over several years. This timeframe presents challenges in producing relevant findings when investigating a technology topic evolving increasingly fast.

To ensure a static dataset for rigorous analysis, it was necessary to stop collecting and considering literature for the document analysis in 2022. This means any new contributions to the literature, including national strategies or scientific findings published after 2022, are not included in the scope of this document analysis portion of the study.

Additionally, it was only possible to include publicly available documentation in this study of preparedness. Therefore, due to the confidential nature of cybersecurity and national security, there is a possibility that further preparatory or development activity is underway in the quantum computing cybersecurity space in NZ that is not represented or considered by this study.

7.3 Contributions

This study has shed light on the under-researched NZ cyber threat environment and the conditions in which NZ organisations operate that limit their ability or drive to prepare for quantum computing-enabled cyber threats. It has closed a gap in existing knowledge by identifying that greater awareness of quantum computing-enabled threats is required to ensure NZ organisations can adequately prepare for these and by confirming that no NZ organisations are preparing to face them.

This study contributes an in-depth analysis of the cybersecurity landscape in NZ, identifying areas that are preventing the execution of successful cyber threat preparation and quality cybersecurity maturity initiatives. It described how existing methods of cyber threat intelligence and knowledge transfer are insufficient to combat the volume and nature of emerging cyber threats and uncovered a cybersecurity culture of low trust, low quality, and acceptance of mediocrity that was previously unexplored. The study confirms that areas such as cyber governance and quantum technology capacity require improvement to successfully address the emerging threat landscape, thereby adding valuable knowledge to the existing knowledge on cybersecurity in NZ. Using a qualitative interview method successfully granted new insights into how framing cyber threats and the cybersecurity landscape potentially impact preparedness actions. These insights challenge the accepted language norms in cybersecurity and are important to understanding how cybersecurity professionals might change the way cyber threats are communicated to achieve a more effective preparation response from NZ organisations.

This research satisfied its aim to create actionable knowledge by contributing practical, contextually relevant guidance for NZ organisations that will aid in preparing for quantum computing-enabled threats. This guidance is intended to drive greater awareness and agency and prompt NZ organisations to start preparatory action for quantum computing-enabled threats, thereby enhancing NZ's cybersecurity posture.

Finally, in developing the QCCP model, this research has further advanced NZ's quantum cybersecurity preparedness concept, which was otherwise unexplored by literature. The QCCP model describes the key global, national, industrial and organisational readiness factors influencing quantum cybersecurity preparedness in NZ and provides context and direction for cybersecurity preparedness strategies.

7.4 Future Research

There are several potential further research areas that, if undertaken, could further advance overall knowledge around the preparation for quantum computing-enabled threats in the NZ landscape.

7.4.1 Technical Preparation

This study identified the necessity for NZ organisations to transfer to quantum-resistant algorithms imminently; however, it is still unclear how challenging this process will be. The number of devices or systems in NZ organisations that cannot be upgraded or use quantum-resistant cryptography is unknown. Therefore, the volume of potential business interruption or the cost of this process cannot be estimated. As a next step, undertaking a case study that pilots the initial activities required for a business to undertake this transition could provide valuable insights into the potential challenges that all NZ organisations will eventually face in transition.

Additionally, this study focused only on the awareness and preparation of large NZ organisations. Small and medium-sized organisations typically have fewer resources to support cybersecurity despite potentially holding sensitive information at risk from quantum computing threats. Further research to build on this study and explore readiness strategies for small to medium-sized organisations in NZ may be warranted.

7.4.2 Language Use

The findings of this research suggest that the language and dialogue used to communicate cyber threats and quantum technology must be considered very carefully as it may influence both the attitudes and the preparatory cyber security actions of NZ organisations. Developing and testing the outcomes of various framing of these issues could further the insights uncovered by this study and promote greater cybersecurity preparedness and smother adoption of quantum technologies.

7.4.3 Risk Management

This study described how challenging cyber risk assessment is for NZ organisations. The inability to quantitatively assess cyber risk presents difficulties for cybersecurity professionals when attempting to justify funding for cybersecurity measures. Therefore, further research that develops specific systems and frameworks to better aid organisations and nations in evaluating and quantifying cyber risk is needed.

7.4.4 Investigating the Transfer of Knowledge

It was clear from this study that current methods to inform and educate NZ organisations on critical cybersecurity issues are not very effective. Therefore, research is recommended to determine alternative methods for communicating cyber threat information and information about emerging cyber risks and preparatory guidance. This study recommended several ideas to improve intelligence transfer; however, better systems to communicate contextually relevant cyber threat intelligence must be developed. Additionally, investigating how awareness programmes could more effectively translate and communicate research outcomes to the cybersecurity industry in NZ is warranted.

7.5 Conclusion

NZ organisations cannot and will not proactively sufficiently prepare for the threats posed by emerging technology, such as quantum computing, until the current cyber risk environment becomes manageable. This study demonstrates that driving down cyber risk before the full impact of quantum computing threats is felt is possible but will require aggressive intervention through regulation, governance, and increased national capacity.

This study's findings call for participants in the NZ cybersecurity and emerging technology landscape to lift the bar and expect more of ourselves and our peers across all areas of technology strategy, innovation, development, and security implementation. NZ needs a greater national technology and cybersecurity vision to strive for, one that embraces quality and strongly supports the ethical values of New Zealanders. A granular strategy that provides clear guidance and ensures all New Zealanders understand and are protected from the emerging issues that quantum computing will pose should be a priority. This strategy should drive an open and accountable cybersecurity and quantum technology culture that rewards excellence and penalises those who do not comply with accepted norms. Notably, leading with vulnerability and adopting a mindset that embraces openness, sharing, and trust may be one of the most valuable steps NZ could take to protect against cyber threats that target both technical and human vulnerabilities.

Finally, the NZ Government should stand up for a less divisive global technology environment that is not driven by fear. Supporting greater international collaboration and driving more anticipatory ethical technology research will ensure that the values important to New Zealanders are embedded into new quantum technology development and promote an equitable, open, and safe online environment for the next generation.

References

AbuGhanem, M., & Eleuch, H. (2024). NISQ Computers: A Path to Quantum Supremacy. *IEEE Access, 12*, 102941-102961. https://doi.org/10.1109/ACCESS.2024.3432330

Achini, K., & Ekundayo, S. (2022). *The challenges of cybersecurity for SMEs in Australia and New Zealand*. Proceedings of the 13th Annual CITRENZ Conference Unifying Educational Delivery and Collaborating Towards Technical Excellence. Christchurch, New Zealand.

Adams, E. (2013, November 26). Researchers predict “cryptopolypse”. *Security Innovation Blog*. https://blog.securityinnovation.com/blog/2013/11/researchers-predict-cryptopolypse.html

Agarwal, V., Agarwal, M., Pareek, P., Chaurasia, V., & Pandey, S. K. (2019). Ultrafast optical message encryption–decryption system using semiconductor optical amplifier based XOR logic gate. *Optical and Quantum Electronics*, *51*(7). https://doi.org/10.1007/s11082-019-1930-9

Agence Nationale de la Sécurité des Systèmes D’information. (2020). *Technical position paper: QKD v2.1 Should quantum key distribution be used for secure communications?* https://cyber.gouv.fr/sites/default/files/2020/05/anssi-technical_position_papers-qkd.pdf

Agence Nationale de la Sécurité des Systèmes D’information. (2022). *ANSSI views on the post-quantum cryptography transition*. https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf

Agence Nationale de la Sécurité des Systèmes D’information. (2023). *Annual review 2022*. https://cyber.gouv.fr/actualites/anssi-annual-review-2022/

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Akerlof, G. A., & Dickens, W. T. (1982). The economic consequences of cognitive dissonance. *American Economic Review, 72*(3), 307–319.

Akinsanya, O. O., Papadaki, M., & Sun, L. (2020). Towards a maturity model for health-care cloud security (M²HCS). *Information & Computer Security, 28*(3), 321–345. https://doi.org/10.1108/ICS-05-2019-0060

Aleiner, I., Bardin, J., Hamilton, M., Kieferová, M., Kitaev, A., Korotkov, A., . . . Zhu, N. (2023). Suppressing quantum errors by scaling a surface code logical qubit. Nature, 614(7949), 676. https://doi.org/10.1038/s41586-022-05434-1

Alexander, S. (2022). A uniquely Australian approach: A thematic analysis of the normative foundations of Australia’s approach to the regulation of the internet. *Adelaide Law Review*, *43*(1), 345–375.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences, 10*(10), 3660. https://doi.org/10.3390/app10103660

Alkhulaifi, A., & El-Alfy, E. (2020). Exploring lattice-based post-quantum signature for JWT authentication: Review and case study. *2020 IEEE 91st Vehicular Technology Conference*. https://doi.org/10.1109/VTC2020-Spring48590.2020.9129505

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. In D. C. Wyld & D. Nagamalai (Eds.), *Computer science & information technology, 7*, 51–62. https://doi.org/10.5121/csit.2017.70305

Alvesson, M., & Sköldberg, K. (2017). *Reflexive methodology: New vistas for qualitative research* (3rd ed.). SAGE.

Ameri, A., Ye, E., Cappellaro, P., Krovi, H., & Loureiro, N. F. (2023). Quantum Algorithm for the Linear Vlasov Equation with Collisions. Proceedings of 2023 *IEEE International Conference on Quantum Computing and Engineering* (QCE), 56-65. https://doi.org/10.1109/QCE57702.2023.10185

Andersen, C. K., Remm, A., Lazar, S., Krinner, S., Heinsoo, J., Besse, J.-C., Gabureac, M., Wallraff, A., & Eichler, C. (2019). Entanglement stabilization using ancilla-based parity detection and real-time feedback in superconducting circuits. *NPJ Quantum Information*, 5(1). https://doi.org/10.1038/s41534-019-0185-4

Apgar, C. (2021). Mitigating risk: The importance of an incident response plan. *Briefings on HIPAA, 21*(4), 5–6.

Ardley, B. (2006). Situated learning and marketing: Moving beyond the rational technical thought cage. *Marketing Intelligence & Planning*, *24*(3), 202–217. https://doi.org/10.1108/02634500610665682

Aripin, A. I., Abimanyu, A., Prabowo, F. S., Priandika, B., Sulivan, B., & Zahra, A. (2020). Mobile cloud computing readiness assessment framework in upstream oil and gas using RAMI 4.0. *2020 International Conference on Information Management and Technology*, 130–135. https://doi.org/10.1109/ICIMTech50083.2020.9211193

Arrow, J., Marsh, S., & Meyer, J. (2023). *A Holistic Approach to Quantum Ethics Education*. 2023 IEEE International Conference on Quantum Computing and Engineering. https://doi.org/10.1109/QCE57702.2023.20332

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Arya, S., Ansar, S. A., & Aggarwal, S. (2023). *Quantum Odyssey: Traversing the NISQ Era's Quantum Terrain*. 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), 686-694. https://doi.org/10.1109/ICTACS59847.2023.10390350

Asghar, R. (2019, May 8). Cyberattack, cybersecurity and protecting New Zealand. *DEMM Engineering & Manufacturing Magazine*. https://demm.co.nz/article/cyberattack-cybersecurity-and-protecting-new-zealand

Atkinson, D. (2020). Quantum computing: The promises and potential perils. *Computer & Internet Lawyer, 37*(1), 4–15.

Aura Information Security. (2021). *Cyber security market research report, 2021*. https://www.kordia.co.nz/aura-cyber-security-market-research-2021

Australian Institute of Company Directors. (2023). *King and Wood Mallesons: International comparison of cybersecurity obligations*. https://www.aicd.com.au/risk-management/framework/cyber-security/king-and-wood-mallesons-international-comparison-of-cybersecurity-obligations.html

Australian Institute of Company Directors. (2024). It's not if but when a cyber security attack will happen. https://www.aicd.com.au/board-of-directors/performance/succession-plan/its-not-if-but-when-a-cyber-security-attack-will-happen.html

Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). *Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography*. 15th International Conference on Network of the Future (NoF), 195-203. https://doi.org/10.1109/NoF62948.2024.10741441

Avesani, M., Calderaro, L., Schiavon, M., Stanco, A., Agnesi, C., Santamato, A., Zahidy, M., Scriminich, A., Foletto, G., Contestabile, G., Chiesa, M., Rotta, D., Artiglia, M., Montanaro, A., Romagnoli, M., Vallone, G. & Villoresi, P. (2021). Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Information 7*, 93. https://doi.org/10.1038/s41534-021-00421-2

Axon, L., Creese, S., Saunders, J., & Dixon, W. (2020, June 23). Why we need to solve our quantum security challenges. *World Economic Forum*. https://weforum.org/agenda/2020/06/quantum-computers-security-challenges/

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal: A Global Perspective, 28*(6), 164–177. https://doi.org/10.1080/19393555.2019.1689318

Baker, G. (2021). Time to get serious about cybersecurity. *NZ Business + Management, 35*(3), 28–29.

Ballance, C. J., Harty, T. P., Linke, N. M., Sepiol, M. A., & Lucas, D. M. (2016). High-fidelity quantum logic gates using trapped-ion hyperfine qubits. *Physical Review Letters*, *117*(6). https://doi.org/10.1103/PhysRevLett.117.060504

Bao, Z., Xu, S., Song, Z., Wang, K., Xiang, L., Zhu, Z., . . . Li, T. (2024). Creating and controlling global Greenberger-Horne-Zeilinger entanglement on quantum processors. *Nature Communications, 15*(1), 1-7. https://doi.org/10.1038/s41467-024-53140-5

Barker, W., Polk, W., & Souppayya, M. (2020). *Getting ready for post-quantum cryptography: Exploring challenges associated with adoption and use of post-quantum cryptographic algorithms*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.04282021

Barreto, P. S. L. M., Gueron, S., Güneysu, T., Misoczki, R., Persichetti, E., Sendrier, N., & Tillich, J. P. (2017). CAKE: Code-based algorithm for key encapsulation. In M. O'Neill (Ed.), *Cryptography and coding* (pp. 207–226). Springer Verlag. https://doi.org/10.1007/978-3-319-71045-7_11

Bavdekar, R., Jayant Chopde, E., Agrawal, A., Bhatia, A., & Tiwari, K. (2023). *Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations*. 2023 International Conference on Information Networking (ICOIN), 146-151. https://doi.org/10.1109/ICOIN56518.2023.10048976

Bazerman, M. H. (1984). The relevance of Kahneman and Tversky's concept of framing to organizational behaviour. *Journal of Management, 10*(3), 333–343. https://doi.org/10.1177/014920638401000307

Beattie, A. (2018, May 13). Data protectionism: The growing menace to global business. *Financial Times*. https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb

Bell, E., Bryman, A., & Harley, B. (2022). *Social research methods* (6th ed.). Oxford University Press.

Bem, D. (1972). Self-perception theory. *Advances in Experimental Social Psychology, 6,* 1–62. https://doi.org/10.1016/S0065-2601(08)60024-6

Ben-David, R., & Toi Staff. (2022, February 16). Defense Ministry, innovation authority to fund Israel's first quantum computer. *The Times of Israel*. https://www.timesofisrael.com/defense-ministry-innovation-authority-to-fund-israels-first-quantum-computer/

Better Business Bureau. (2017). *State of cybersecurity among small businesses in North America*. https://www.bbb.org/stateofcybersecurity

Bettie, J. (2014). *Women without class: Girls, race, and identity*. University of California Press.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Visions and voices on emerging challenges in digital business strategy: Introduction. *MIS Quarterly, 37*(2), 633–634.

Blau, J. (2017). A quantum leap for Europe's research program. *Research-Technology Management*, *60*(5). https://www.thefreelibrary.com/A+quantum+leap+for+Europe%27s+research+program-a0509015098

Boenink, M., & Kudina, O. (2020). "Values in Responsible Research and Innovation: From Entities to Practices." *Journal of Responsible Innovation 7* (3). 450–470. https://doi.org/10.1080/23299460.2020.1806451

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., & Stehle, D. (2018). CRYSTALS – Kyber: A CCA-secure module-lattice-based KEM. *2018 IEEE European Symposium on Security and Privacy*. https://doi.org/10.1109/EuroSP.2018.00032

Bos, J., Stebila, D., Costello, C., Naehrig, M., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., & Raghunathan, A. (2016). Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* https://doi.org/10.1145/2976749.2978425

Bova, F., Goldfarb, A. & Melko, R.G. (2021). Commercial applications of quantum computing. *EPJ Quantum Technol. 8*(2). https://doi.org/10.1140/epjqt/s40507-021-00091-1

Braithwaite, M. (2016, July 7). Experimenting with post-quantum cryptography. *Google Security Blog*. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

Brandl, M. F., van Mourik, M. W., Postler, L., Nolf, A., Lakhmanskiy, K., Paiva, R. R., Möller, S., Daniilidis, N., Häffner, H., Kaushal, V., Ruster, T., Warschburger, C., Kaufmann, H., Poschinger, U. G., Schmidt-Kaler, F., Schindler, P., Monz, T., & Blatt, R. (2016). Cryogenic setup for trapped ion quantum computing. *Review of Scientific Instruments, 87*(11). https://doi.org/10.1063/1.4966970

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. SAGE.

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE.

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). *Thematic analysis*. In P. Liamputtong (Eds.), *Handbook of research methods in health social sciences* (pp. 843–860). Springer. https://doi.org/10.1007/978-981-10-5251-4_103

Bravyi, S. B., & Kitaev, A. Y. (1998). Quantum codes on a lattice with boundary. *arXiv.* https://doi.org/10.48550/arXiv.quant-ph/9811052

Brinkmann, S. (2017). Humanism after posthumanism: Or qualitative psychology after the "posts". *Qualitative Research in Psychology*, *14*(2), 109–130. https://doi.org/10.1080/14780887.2017.1282568

Brinkmann, S., & Kvale, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd. ed.). SAGE.

Broadbent, A., & Schaffner, C. (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes & Cryptography*, *78*(1), 351–382. https://doi.org/10.1007/s10623-015-0157-4

Brooks, M. (2023a, May 25). IBM wants to build a 100,000-qubit quantum computer. *MIT Technology Review*. https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/

Brooks, M. (2023b, January 6). What's next for quantum computing. *MIT Technology Review*. https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/

Budinski, L. (2021). Quantum algorithm for the advection–diffusion equation simulated with the lattice Boltzmann method. *Quantum Information Processing, 20*(2), 1-17. https://doi.org/10.1007/s11128-021-02996-3

Burton, J. (2013). Cyber security: The strategic challenge and New Zealand's response. *New Zealand International Review, 38*(3). https://nz.vlex.com/vid/cyber-security-the-strategic-635661189

Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International Affairs*, *97*(6), 1727–1747. https://doi.org/10.1093/ia/iiab172

Butin, D. (2018). Hash-based signatures: State of play. *IEEE Security & Privacy, Security & Privacy, 15*(4), 37–43. https://doi.org/10.1109/MSP.2017.3151334

Byrd, G., & Ding, Y. (2023). Quantum Computing: Progress and Innovation. *Computer, 56*(1), 20-29. https://doi.org/10.1109/MC.2022.3217021

Byrne, D. (2022). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity*, *56*(3), 1391–1412. https://doi.org/10.1007/s11135-021-01182-y

Cabinet Office, Government of Japan. (n.d.). *Moonshot Research and Development Program*. https://www8.cao.go.jp/cstp/english/moonshot/top.html

Cacciapuoti, S., Caleffi, M., Van Meter, R., & Hanzo, L. (2020). When entanglement meets classical communications: Quantum teleportation for the quantum internet. *IEEE Transactions on Communications, 68*(6), 3808–3833. https://doi.org/10.1109/TCOMM.2020.2978071

Caleffi, M., Chandra, D., Cuomo, D., Hassanpour, S., & Cacciapuoti, A. S. (2020). The rise of the quantum internet. *Computer*, *53* (6), 67–72. https://doi.org/10.1109/MC.2020.2984871

Campagna, M., & Crockett, C. (2020). *Internet-draft: Hybrid post-quantum key encapsulation methods (PQ KEM) for transport layer security 1.2 (TLS).* Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-campagna-tls-bike-sike-hybrid/03/

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2021). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. *IEEE Transactions on Engineering Management, 68*(1), 223–234. https://doi.org/10.1109/TEM.2019.2909909

Carita, S., & Kabetta, H. (2023). *Implementation of A New Quasi-Cyclic Goppa Code in McEliece Cryptography. I*EEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 412-417. https://doi.org/10.1109/ICITISEE58992.2023.10404912

Cassell, C., Cunliffe, A., & Grandy, G. (2018). *The SAGE handbook of qualitative business and management research methods: History and traditions*. SAGE. https://doi.org/10.4135/9781526430212

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811–831. https://doi.org/10.46743/2160-3715/2016.2337

Cavaliere, F., Mattsson, J., & Smeets, B. (2020). The security implications of quantum cryptography and quantum computing. *Network Security*, *2020*(9), 9–15. https://doi.org/10.1016/S1353-4858(20)30105-7

Cegielski, C. G., Reithel, B. J., & Rebman, C. M. (2005). Emerging information technologies: Developing a timely IT strategy. *Communications of the ACM, 48*(8), 113–117. https://doi.org/10.1145/1076211.1076214

Center for Internet Security. (2021). *CIS controls version 8*. https://learn.cisecurity.org/control-download

Center for Quantum Computation & Communication Technology. (2024). *Our mission*. https://www.cqc2t.org/about-us/

Center for Security and Emerging Technology. (2021). *Translation: Outline of the People's Republic of China 14th five-year plan for national economic and social development and long-range objectives for 2035*. https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

Centre for Excellence for Quantum Computation and Communication Technology. (2024). *Our mission*. https://www.cqc2t.org/about-us/

CERTNZ. (2022). *2022 report summary*. https://www.cert.govt.nz/about/quarterly-report/2022-report-summary/

CERTNZ. (2024). *Public communications for cyber security incidents. A framework for organisations*. https://www.cert.govt.nz/assets/Uploads/documents/public-communications-for-cyber-security-incidents-a-framework-organisations.pdf

Chang, C., Lin, Y., Chiu, K., & Huang, T. (2020). The second quantum revolution with quantum computers. *AAPPS Bulletin*, *30* (1), 9–22. https://doi.org/10.22661/AAPPSBL.2020.30.1.09

Chang, H. L. (2010). A roadmap to adopting emerging technology in e-business: An empirical study. *Information Systems & e-Business Management, 8*(2), 103–130. https://doi.org/10.1007/s10257-009-0111-y

Chang, J., Edward, P., Gonzales, D., Kochhar, A., Litterer, S., O'Connor, K., Schmid, J., Scholl, K., Silberglitt, R., Eusebi, C., & Harold, S. (2022). *An assessment of the U.S. and Chinese industrial bases in quantum technology*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA869-1.html

Chapman, T. A., & Reithel, B. J. (2020). Perceptions of cybersecurity readiness among workgroup IT managers. *Journal of Computer Information Systems*, *61*(5), 438–449. https://doi.org/10.1080/08874417.2019.1703224

Charlet, K., & King, H. (2020). The future of cybersecurity policy. *IEEE Security & Privacy,18*(1), 8–10. https://doi.org/10.1109/MSEC.2019.2953368

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). SAGE.

Chatterjee, A., Phalak, K., & Ghosh, S. (2023). *Quantum Error Correction For Dummies*. 2023 IEEE International Conference on Quantum Computing and Engineering (QCE), 1, 70-81. https://doi.org/10.1109/QCE57702.2023.00017

Chen, A. (2020). Introduction: Zeros and ones, off and on. In A. Chen. A (Ed.), *Shouting zeros and ones: Digital technology, ethics, and policy in New Zealand* (pp. iii–iv). Bridget Williams Books.

Chen, Y., Neill, C., Roushan, P., Leung, N., Fang, M., Barends, R., Kelly, J., Campbell, B., Chen, Z., Chiaro, B., Dunsworth, A., Jeffrey, E., Megrant, A., Mutus, J. Y., O'Malley, P. J. J., Quintana, C. M., Sank, D., Vainsencher, A., Wenner, J., … Martinis, J. M. (2014). Qubit architecture with high coherence and fast tunable coupling. *Physical Review Letters*, *113*(22), https://doi.org/10.1103/PhysRevLett.113.220502

Cherif, M., Chaari, W., & Driss, O. (2023). *A Quantum Machine Learning Approach Using an Optimized Application of Grover's Algorithm*. IEEE Afro-Mediterranean Conference on Artificial Intelligence. https://doi.org/10.1109/AMCAI59331.2023.10431508

Ching, K. H., Teoh, A. P., & Amran, A. (2020). A conceptual model of technology factors to InsurTech adoption by value chain activities. *IEEE Conference on e-Learning, e-Management and e-Services*, 88–92. https://doi.org/10.1109/IC3e50159.2020.9288465

Chi Vo, L., Mounoud, E., & Rose, J. (2012). Dealing with the opposition of rigor and relevance from Dewey's pragmatist perspective. *Management*, *15*(4), 367–390. https://doi.org/10.3917/mana.154.0368

Chong, F. T., Franklin, D., & Martonosi, M. (2017). Programming languages and compiler design for realistic quantum hardware. *Nature*, *549*(7671), 180–187. https://doi.org/10.1038/nature23459

Clark, H., & Brash, D. (2024, February 13). NZ must not abandon our independent foreign policy. *The New Zealand Herald*. https://www.nzherald.co.nz/nz/helen-clark-and-don-brash-aukus-nz-must-not-abandon-our-independent-foreign-policy/LLYEOE4WH5AY5DTV3D323OXRUU/

Cloud Security Alliance. (2018). *The state of post-quantum cryptography*. https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/State_of_PQC_web.pdf

Cloud Security Alliance. (2019). *Quantum-safe security awareness survey*. https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/quantum-safe_security_awareness_survey.pdf

Coenen, C., Grinbaum, A., Grunwald, A., Milburn, C., & Vermaas, P. (2022). Quantum technologies and society: Towards a different spin. *NanoEthics, 16*(1), 1–6. https://doi.org/10.1007/s11569-021-00409-4

Collins English Dictionary. (n.d.). Mediocre. In *Collins English Dictionary*. Retrieved April 1, 2024, from https://www.collinsdictionary.com/us/dictionary/english/mediocre

Commonwealth of Australia. (2023a). *2023–2030 Australian cyber security strategy*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Commonwealth of Australia. (2023b). *Budget 2023–24: Growing the economy: Modernising our economy and maximising our strengths*. https://budget.gov.au/content/03-economy.htm

Commonwealth Scientific and Industrial Research Organisation. (2020). *Growing Australia's quantum technology industry*. https://www.csiro.au/-/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf

Cong, I., Choi, S., & Lukin, M. D. (2019). *Quantum convolutional neural networks*. *Nature Physics*, *15*(12), 1273–1278. https://doi.org/10.1038/s41567-019-0648-8

Congiunti, L., Lo Piccolo, F., Russo, A., & Serio, M. (Eds.). (2023). *Ethics in research: Principles and practical considerations*. Springer.

Conover, E. (2020). Quantum computing's error problem. *Science News, 197*(11), 18–23.

Corbin, J. M., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). SAGE.

Corcoles, A. D., Kandala, A., Javadi-Abhari, A., McClure, D. T., Cross, A. W., Temme, K., Nation, P. D., Steffen, M., & Gambetta, J. M. (2020). Challenges and opportunities of near-term quantum computing systems. *Proceedings of the IEEE, 108*(8), 1338–1352. https://doi.org/10.1109/JPROC.2019.2954005

Creswell, J. W. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). SAGE.

Cross, A., Javadi-Abhari, A., Alexander, T., de Beaudrap, N. Bishop.L. ,… Johnson,B. (2022). OpenQASM 3: *A broader and deeper quantum assembly language*. arXiv:2104.14722v1.

Curtis, P., Mehravari, N., & Stevens, J. (2015). *Cybersecurity capability maturity model for information technology services (c2m2 for IT services) version 1.0*. Carnegie-Mellon University. https://apps.dtic.mil/sti/pdfs/AD1026943.pdf

Cybersecurity Disclosure Act of 2021, S. 808, 117th Cong. (2021). https://www.congress.gov/115/bills/s536/BILLS-115s536is.pdf

Daft, R. L., & Lewin, A. Y. (2008). Rigor and relevance in organization studies: Idea migration and academic journal evolution. *Organization Science*, *19*(1), 177–183. https://doi.org/10.1287/orsc.1070.0346

Das, S., Krause, S., Giering, K., Pousa, R. J., Bassoli, R., & Fitzek, F. H. (2024). Leveraging quantum uncertainty: Quantum randomness through the lens of classical communication networks. *Computer Networks, 254*. https://doi.org/10.1016/j.comnet.2024.110781

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

De Abiega-L'Eglisse, F., Delgado-Vargas, K. A., Valencia-Rodriguez, F. Q., Gonzalez-Quiroga, V. G., Gallegos-Garcia, G., & Nakano-Miyatake, M. (2020). Performance of new hope and CRYSTALS-dilithium postquantum schemes in the transport layer security protocol, *IEEE Access, 8*, 213968–213980. https://doi.org/10.1109/access.2020.3040324

De Veras, T. M. L., de Araujo, I. C. S., Park, D. K., & da Silva, A. J. (2021). Circuit-based quantum random access memory for classical data with continuous amplitudes. *Institute of Electrical and Electronics Engineers. Transactions on Computers, 70*(12), 2125-2135. https://doi.org/10.1109/TC.2020.3037932

Debenedictis, E. P. (2020). Beyond quantum supremacy*, Computer, 53*(2), 91–94. https://doi.org/10.1109/mc.2019.2958446

Defense Advanced Research Projects Agency. (2020, May 11). DARPA *kicks off program to advance quantum computing*. https://www.darpa.mil/news-events/2020-05-11a

Defense Advanced Research Projects Agency (DARPA). (2023, December 6). *DARPA-funded research leads to quantum computing breakthrough*. https://www.darpa.mil/news-events/2023-12-06

Delilbasic, A., Le Saux, B., Riedel, M., Michielsen, K., & Cavallaro, G. (2024). *Reverse Quantum Annealing for Hybrid Quantum-Classical Satellite Mission Planning.* IEEE International Geoscience and Remote Sensing Symposium, Geoscience and Remote Sensing Symposium, 432-436. https://doi.org/10.1109/IGARSS53475.2024.10640974

Department for Science, Innovation and Technology. (2023a). *National quantum strategy*. https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national_quantum_strategy.pdf

Department for Science, Innovation and Technology. (2023b). *Plan to forge a better Britain through science and technology unveiled*. https://www.gov.uk/government/publications/uk-science-and-technology-framework

Department of Home Affairs. (2020). *Australia's cyber security strategy 2020*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Department of Home Affairs. (2023). *2023–2030 Australian cyber security strategy discussion paper*. https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

Department of Industry, Science and Resources. (2022). *Australia's quantum advantage National Quantum Strategy: Consultation paper*. https://storage.googleapis.com/converlens-au-industry/industry/p/prj221726a232884dc6016a1/public_assets/Consultation%20Paper%20-%20National%20Quantum%20Strategy%20-%20FINAL.pdf

Department of Industry, Science and Resources. (2023). *National quantum strategy: Building a thriving future with Australia's quantum advantage*. https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf

Department of Science and Technology. (2024). *National quantum mission* (NQM). https://dst.gov.in/national-quantum-mission-nqm

Department of the Prime Minister and Cabinet. (2019). *New Zealand's cyber security strategy 2019*. https://www.dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

Department of the Prime Minister and Cabinet. (2023). *Let's talk about our national security: National security long term insights briefing*. https://www.dpmc.govt.nz/sites/default/files/2023-05/National%20Security%20Long-term%20Insights%20Briefing.pdf

Der Derian, J., & Wendt, A. (2020). 'Quantizing international relations': The case for quantum approaches to international theory and security practice. *Security Dialogue*, *51*(5), 399–413. https://doi.org/10.1177/0967010620901905

Devoret, M. H., & Schoelkopf, R. J. (2013). Superconducting circuits for quantum information: An outlook. *Science*, *339*(6124), 1169–1174. https://doi.org/10.1126/science.1231930

Dewey, J. (1929). Nature, mind and the subject. *Experience and nature.* W W Norton & Co; 208-247. https://doi.org/10.1037/13377-006

Dewey, J. (1931). *Philosophy and civilization*. Balch & Company.

Dewey, J. (2000a). Experience and philosophic method. In J. Stuhr (Ed.). *Pragmatism and classical American philosophy: Essential readings and interpretive essays* (2nd ed., pp. 460–470). Oxford University Press. (Original work published 1925)

Dewey, J. (2000b). The postulate of immediate empiricism. In J. Stuhr (Ed.), *Pragmatism and classical American philosophy: Essential readings and interpretive essays* (2nd ed., pp. 455–460). Oxford University Press. (Original work published 1925)

de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology*, *19*(4), 271–276. https://doi.org/10.1007/s10676-017-9439-z

Dexter, G. (2023, December 21). Luxon 'exploring' non-nuclear part of AUKUS pact. *Radio New Zealand*. https://www.rnz.co.nz/news/political/505227/luxon-exploring-non-nuclear-part-of-aukus-pact

Dhara, S. K., & Sen, D. (2018). Low light image enhancement using Grover's algorithm on superposed luminance levels. *2018 25th IEEE International Conference on Image Processing.* https://doi.org/10.1109/ICIP.2018.8451651

Di Matteo, O. (2024). *On the need for effective tools for debugging quantum programs*. IEEE/ACM 5th International Workshop on Quantum Software Engineering (Q-SE), 17-20. https://doi-org/10.1145/3643667.3648226

DigiCert. (2019). *Quantum's promise and peril: 2019 DigiCert post quantum crypto survey*. https://www.digicert.com/content/dam/digicert/pdfs/2019-digicert-post-quantum-crypto-survey-report-en.pdf

Dizon, M. A. C., & McHugh, P. J. (2022). Encryption laws and regulations in one of the five eyes: The case of New Zealand. *Information & Communications Technology Law*, *31*(2), 220–239. https://doi.org/10.1080/13600834.2021.1988321

Djordjevic, I. B. (2020). Secure, global quantum communications networks. *2020 22nd International Conference on Transparent Optical Networks.* https://doi.org/10.1109/ICTON51198.2020.9203116

Dodd-Walls Centre. (2022). *Annual report*. https://www.doddwalls.ac.nz/about#annual-reports.

DORA (Digital Operational Resilience Act), Regulation (EU) 2022/2554 of the European Parliament and of the Council. (2022). http://data.europa.eu/eli/reg/2022/2554/oj

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS directive compliant cybersecurity maturity assessment framework. *IEEE 44th Annual Computers, Software, and Applications Conference*, 1641–1646. https://doi.org/10.1109/COMPSAC48688.2020.00-20

Dupont, B. (2013). Cybersecurity futures: How can we regulate emergent risks? *Technology Innovation Management Review, 3*(7), 6–11. https://doi.org/10.22215/timreview700

Economist Intelligence Unit. (2008). *The 2008 e-readiness rankings, a white paper from the Economist Intelligence Unit*. https://graphics.eiu.com/upload/ibm_ereadiness_2008.pdf

The Education Hub. (2022a). *Long literacy report*. https://cdn.theeducationhub.org.nz/wp-content/uploads/2022/03/Ed-Hub_Long-literacy-report_v2.pdf

The Education Hub. (2022b). *What's happening with literacy in Aotearoa New Zealand?* https://cdn.theeducationhub.org.nz/wp-content/uploads/2022/03/Ed-Hub_Long-literacy-report_v2.pdf

Education Review Office. (2013). *Science in the New Zealand curriculum years 5 to 8*. https://ero.govt.nz/sites/default/files/2021-05/Science-in-the-New-Zealand-Curriculum-Years-5-to-8.pdf

Eilts, D. (2020). *An empirical assessment of cybersecurity readiness and resilience in small businesses* [Doctoral thesis, Nova Southeastern University]. https://nsuworks.nova.edu/gscis_etd/1106

Ekerå, M. (2020). On post-processing in the quantum algorithm for computing short discrete logarithms. *Designs, Codes & Cryptography*, *88*(11), 2313–2335. https://doi.org/10.1007/s10623-020-00783-2

Elhoushi, M., El-Kharashi, M. W., & Elrefaei, H. (2011). Modeling a quantum processor using the QRAM model. *Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*. https://doi.org/10.1109/PACRIM.2011.6032928

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005). Current status of the DARPA quantum network. *arXiv.* https://doi.org/10.48550/arXiv.quant-ph/0503058

The Embassy of the People's Republic of China in New Zealand. (2024, February 24). *Remarks by the Spokesperson of the Chinese Embassy in New Zealand on the Joint Statement on ANZMIN 2024* [Press release]. http://nz.china-embassy.gov.cn/eng/zyxw/202402/t20240202_11238593.htm

Epstein, S. (2019). Algorithmic no-cloning theorem, *IEEE Transactions on Information Theory*, *65*(9), 5925–5930. https://doi.org/10.1109/TIT.2019.2910562

Esmaeilifar, L., Mirza, B., & Mohammadzadeh, H. (2020). Relativistic quantum information of anyons. *International Journal of Theoretical Physics, 59*(10), 3289–3298. https://doi.org/10.1007/s10773-020-04586-y

European Commission. (2023). *European declaration on quantum technologies*. https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies

European Parliament. (2022a). *Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: The European Way for the Digital Decade*. https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf

European Parliament. (2022b). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030* (PE/50/2022/REV/1). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32022D2481

European Quantum Flagship. (2020). *Strategic research agenda*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65402

European Telecommunications Standards Institute. (2023). *Quantum key distribution (QKD); Common criteria protection profile - Pair of prepare and measure quantum key distribution modules*. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

Falkenmire, B. (2023). Held to RANSOM. *Acuity, 10*(6), 56–59.

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Fathian, M., Akhavan, P., & Hoorali, M. (2008). E-readiness assessment of non-profit ICT SMEs in a developing country: The case of Iran. *Technovation, 28*(9), 578–590. https://doi.org/10.1016/j.technovation.2008.02.002

Federal Ministry of the Interior, Building, and Community. (2021). *Cyber security strategy for Germany 2021*. https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=AE37C355F11195E09FFA474F486DD655.live892?__blob=publicationFile&v=4

Federal Office for Information Security. (2021). Quantum-safe cryptography – Fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6

Feilzer, M. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research, 4*(1), 6–16. https://doi.org/10.1177/1558689809349691

Ferranti, M. (2021). *The Netherlands made a huge bet on quantum computing — Will it pay off?* CIO. https://www.cio.com/article/191607/the-netherlands-made-a-huge-bet-on-quantum-computing-will-it-pay-off.html

Financial Markets Authority. (2019). *Cyber-resilience in FMA-regulated financial services*. https://www.fma.govt.nz/assets/Guidance/Cyber-resilience-in-FMA-regulated-financial-services.pdf

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: An introduction to theory and research*. Addison-Wesley.

Fisher, E., & Rip, A. (2013). *Responsible Innovation: Multi-Level Dynamics and Soft Intervention Practices*, In Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society, edited by R. Owen, J. R. Bessant, and M. Heintz. 9, 165–185. Chichester, UK: John Wiley & Sons Ltd. https://doi.org/10.1002/9781118551424.ch9

Fitch Solutions. (2023). *Country risk index*. https://www.fitchsolutions.com/sites/default/files/2023-04/BMI_Country_Risk_Index_Overview.pdf

Fitzgibbon, G., & Ottaviani, C. (2024). Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography. *Cryptography (2410-387X), 8*(2), 21-37. https://doi.org/10.3390/cryptography8020021

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research...second article in an occasional series. *Australian & New Zealand Journal of Psychiatry*, *36*(6), 717–732. https://doi.org/10.1046/j.1440-1614.2002.01100.x

Friese, S. (2014). *Qualitative data analysis with ATLAS.ti* (2nd ed.). SAGE.

Gangwar, A., Upadhyay, A., & Azad, A. S. (2022). Optimised smart AI surveillance in quantum computing age. *2022 IEEE 7th International conference for Convergence in Technology.* https://doi.org/10.1109/I2CT54291.2022.9824610

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis, 40*(1), 183–199. https://doi.org/10.1111/risa.12891

Garae, J., Ko, R. K. L., Kho, J., Suwadi, S., Will, M. A., & Apperley, M. (2017). Visualizing the New Zealand cyber security challenge for attack behaviors. *2017 IEEE Trustcom/BigDataSE/ICESS,* 1123–1130. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.362

Genus, A., & Stirling, A. (2018). Collingridge and the dilemma of control: Towards responsible and accountable innovation. *Research Policy*, *47*(1), 61–69. https://doi.org/10.1016/j.respol.2017.09.012

GESDA. (2022). *Impact story: Quantum computing*. https://gesda.global/wp-content/uploads/2022/09/GESDA-Quantum-Computing-Impact-Story-Apr2022-1.pdf

Gibney, E. (2019, October 23). Hello quantum world! Google publishes landmark quantum supremacy claim. *Nature News*. https://www.nature.com/articles/d41586-019-03213-z

Gilkison, A., Giddings, L., & Smythe, L. (2016). Real life narratives enhance learning about the 'art and science' of midwifery practice. *Advances in Health Sciences Education*, *21*(1), 19–32. https://doi.org/10.1007/s10459-015-9607-z

Gillespie, A., & Patman, R. (2023, April 19). Approach with caution: Why NZ should be wary of buying into the AUKUS security pact. *The Conversation*. https://theconversation.com/approach-with-caution-why-nz-should-be-wary-of-buying-into-the-aukus-security-pact-203915

Gillies-Walker, L., Ramzan, N., Rankin, J., Nimbley, E., & Gillespie-Smith, K. (2023). "You feel like you kind of walk between the two worlds": A participatory study exploring how technology can support emotion regulation for autistic people. *Journal of Autism & Developmental Disorders*, *53*(1), 216–228. https://doi.org/10.1007/s10803-021-05392-z

Giovannetti, V., Lloyd, S., & Maccone, L. (2008). Quantum random access memory. *Physical Review Letters*, *100*(16), 160501. https://doi.org/10.1103/PhysRevLett.100.160501

Giron, A. A., Custódio, R., & Rodríguez-Henríquez, F. (2023). Post-quantum hybrid key exchange: A systematic mapping study. *Journal of Cryptographic Engineering, 13*(1), 71-88. https://doi.org/10.1007/s13389-022-00288-9

Gluckman, P., & Bardsley, A. (2021). *Uncertain but inevitable: The expert-policy-political nexus and high-impact risks*. Informed Futures. https://informedfutures.org/high-impact-risks/

Gluckman, P., & Bardsley, A. (2023). *Risk listening: Rethinking how we understand and manage risk*. Informed Futures. https://informedfutures.org/wp-content/uploads/pdf/Risk-listening-rethinking-how-we-understand-and-manage-risk.pdf

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems, 21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54

Government Communications Security Bureau. (2020). *National cyber security centre cyber threat report for 2019/20*. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2020.pdf

Government Communications Security Bureau. (2022a). *MSP supplier panel update – November 2022*.

Government Communications Security Bureau. (2022b). *The New Zealand information security manual v3.6*. https://www.nzism.gcsb.govt.nz/ism-document/pdf

Government of Canada. (2022). *Canada's national quantum strategy*. https://ised-isde.canada.ca/site/national-quantum-strategy/en

Government of France. (2023). *France national quantum strategy annual report March 2023*. https://www.gouvernement.fr/upload/media/organization/0001/01/sites_default_files_contenu_piece-jointe_2023_04_france2030_quantique_rapport_activite_2022_vdef2.pdf

Government of Ireland. (2019). *National cyber security strategy 2019–2024*. *https://assets.gov.ie/76728/567c89b8-47f6-4e13-8782-409cff8b5b94.pdf*

Grant, B., & Giddings, L. (2002). Making sense of methodologies: A paradigm framework for the novice researcher. *Contemporary Nurse*, *13*, 10–28. https://doi.org/10.5172/conu.13.1.10

Gregory, A., & Chiang, C. (2018). Simulation of quantum walks via Hamiltonian reduction. *2018 IEEE Nanotechnology Symposium.* https://doi.org/10.1109/NANOTECH.2018.8653568

Greinert, F., Müller, R., Goorney, S., Sherson, J., & Ubben, M. S. (2023). Towards a quantum ready workforce: The updated European Competence Framework for Quantum Technologies. *Frontiers in Quantum Science & Technology*, 1–8. https://doi.org/10.3389/frqst.2023.1225733

Grinbaum, A. (2017). Narratives of quantum theory in the age of quantum technologies. *Ethics and Information Technology*, *19*(4), 295–306. https://doi.org/10.1007/s10676-017-9424-6

Grobman, S. (2020). Quantum computing's cyber-threat to national security. *PRISM, 9* (1), 52–67. https://www.jstor.org/stable/26940159

Grody, A. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*, *13*(2), 155–162.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. https://doi.org/10.1145/237814.237866

Grumbling, E., & Horowitz, M. (Eds.). (2019). *Quantum computing progress and prospects*. The National Academies Press. https://doi.org/10.17226/25196

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 105–117). SAGE.

Guccione, G., Darras, T., Jeanni, H., Cavaillès, A., Laurat, J., Verma, V., & Nam, S. (2020). Connecting heterogeneous quantum networks by hybrid entanglement swapping. *Science Advances, 6*(22). https://doi.org/10.1126/sciadv.aba4508

Gulati, R. (2007). Tent poles, tribalism, and boundary spanning: The rigor-relevance debate in management research. *Academy of Management Journal*, *50*(4), 775–782. https://doi.org/10.5465/amj.2007.26279170

Hadi, M., & José Closs, S. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38*(3), 641–646. https://doi.org/10.1007/s11096-015-0237-6

Hagens, V., Dobrow, M. J., & Chafe, R. (2009). Interviewee transcript review: Assessing the impact on qualitative research. *BMC Medical Research Methodology*, *9*(1), 47. https://doi.org/10.1186/1471-2288-9-47

Hampton, A. (2019, April 5). *Improving the cyber security resilience of New Zealand businesses* [Speech]. Government Communications Security Bureau. https://www.gcsb.govt.nz/news/improving-the-cyber-security-resilience-of-new-zealand-businesses/

Hampton, A. (2023, March 27). *Statement to intelligence and security committee by Andrew Hampton Director-General GCSB* [Speech]. Government Communications Security Bureau. https://www.gcsb.govt.nz/news/statement-to-intelligence-and-security-committee-by-andrew-hampton-director-general-gcsb/

Han, S., Ding, H., Zhang, C., Zhou, X., Zhang, C., & Wang, Q. (2020). Practical decoy-state quantum random number generator with weak coherent sources. *Quantum Information Processing, 19*(11), 396–404. https://doi.org/10.1007/s11128-020-02902-3

Hanna, P. (2012). Using internet technologies (such as Skype) as a research medium: A research note. *Qualitative Research*, *12*(2), 239–242. https://doi.org/10.1177/1468794111426607

Hashim, K. F., Hashim, N. L., Ismail, S., Miniaoui, S., & Atalla, S. (2020). Citizen readiness to adopt the new emerging technologies in Dubai smart government services. *2020 6th International Conference on Science in Information Technology*. https://doi.org/10.1109/ICSITech49800.2020.9392071

Odin Hashemi, S. H., & Hodtani, G. A. (2019). A modified McEliece public-key cryptosystem based on irregular codes of QC-LDPC and QC-MDPC. 2019 27th Iranian Conference on Electrical Engineering, 1373–1376. https://doi.org/10.1109/IranianCEE.2019.8786376

Havlíček, V., Córcoles, A., Temme, K., Kandala, A., Chow, J., Gambetta, J., & Harrow, A. (2019). Supervised learning with quantum-enhanced feature spaces. *Nature, 567*(7747), 209–212. https://doi.org/10.1038/s41586-019-0980-2

Herrmann, N., Arya, D., Doherty, M. W., Mingare, A., Pillay, J. C., Preis, F., & Prestel, S. (2023). *Quantum utility – definition and assessment of a practical quantum advantage*. IEEE International Conference on Quantum Software (QSW), 162-174. https://doi.org/10.1109/QSW59989.2023.00028

Hesse-Biber, S. (2015). Mixed methods research: The "thing-ness" problem. *Qualitative Health Research, 25*(6), 775–788. https://doi.org/10.1177/1049732315580558

HM Government. (2022). *National cyber strategy 2022 – Pioneering a cyber future with the whole of the UK*. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Hoefler, T., Häner, T., & Troyer, M. (2023). *Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage.* Communications of the ACM, 66(5), 82-87. https://doi.org/10.1145/3571725

Holm, K., & Goduscheit, R. C. (2020). Assessing the technology readiness level of current blockchain use cases. *2020 IEEE Technology & Engineering Management Conference*. https://doi.org/10.1109/TEMSCON47658.2020.9140147

Holmes, A., Jokar, M. R., Pasandi, G., Ding, Y., Pedram, M., & Chong, F. T. (2020). NISQ+: Boosting quantum computing power by approximating quantum error correction. *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture*. https://doi.org/10.1109/ISCA45697.2020.00053

Holt, A. (2010). Using the telephone for narrative interviewing: A research note. *Qualitative Research*, *10*(1), 113–121. https://doi.org/10.1177/1468794109348686

Hosseini, R., Tajik, S., Koohi Lai, Z., Jamali, T., Haven, E., & Jafari, R. (2023). Quantum Bohmian-inspired potential to model non–Gaussian time series and its application in financial markets. *Entropy, 25*(7), 1061–1069. https://doi.org/10.3390/e25071061

HPCWire. (2024, February 5). UK Government announces £45m investment in quantum tech. *Off the Wire*. https://www.hpcwire.com/off-the-wire/uk-government-announces-45m-investment-in-quantum-tech/

Huang, Y., & Martonosi, M. (2019). Statistical assertions for validating patterns and finding bugs in quantum programs. *2019 ACM/IEEE 46th Annual International Symposium on Computer Architecture*. https://doi.org/10.1145/3307650.3322213

Hulsing, A., Butin, D., Darmstadt, T., Gazdag, S., Rijineveld, J., & Mohaisen, A. (2018). *Internet-draft: XMSS: Extended hash-based signatures*. Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc8391/

Hung, S., Hietala, K., Zhu, S., Hicks, M., Wu, X., & Ying, M. (2019). Quantitative robustness analysis of quantum programs. *Proceedings of the ACM on Programming Languages*. https://doi.org/10.1145/3290344

IEEE Standards Association. (2022). *Standard for post-quantum network security.* https://standards.ieee.org/ieee/1943/10957/

Ikeda, K., Nakamura, Y., & Humble, T. (2019). Application of quantum annealing to nurse scheduling problem. *Scientific Reports*, *9*(1), 1–10. https://doi.org/10.1038/s41598-019-49172-3

Iles, I. A., Egnoto, M. J., Fisher Liu, B., Ackerman, G., Roberts, H., & Smith, D. (2017). Understanding the adoption process of national security technology: An integration of diffusion of innovations and volitional behavior theories. *Risk Analysis, 37*(11), 2246–2259. https://doi.org/10.1111/risa.12771

Ilyas, M., Cui, S., & Perkowski, M. (2022). Ternary logic design in topological quantum computing. *Journal of Physics A: Mathematical & Theoretical, 55*(30), 1-54. https://doi.org/10.1088/1751-8121/ac7b55

Indian Institute of Science. (n.d.). Initiative on quantum technology (IQT@IISc). https://ceqt.iisc.ac.in/

Infocomm Media Development Authority. (2023, June 6). *Singapore launches Southeast Asia's first quantum-safe network infrastructure to help businesses tap on quantum-safe technologies.* https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/sg-launches-southeast-asias-first-quantum-safe-network-infrastructure

Inglesant, P., Artswood, M., & Jirotka, M. (2018). *Thinking ahead to a world with quantum computers*. University of Oxford. https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2016-11/RRI%20Landscape%20Report%20November%202016.pdf

Inglesant, P., Ten Holter, C., Jirotka, M., & Williams, R. (2021). Asleep at the wheel? Responsible Innovation in quantum computing. *Technology Analysis & Strategic Management, 33*(11), 1364-1376. https://doi.org/10.1080/09537325.2021.1988557

Institute of Materials Research and Engineering. (2023). *National Quantum Fabless Foundry (NQFF)*. https://www.a-star.edu.sg/imre/research-departments/national-quantum-fabless-foundry

International Organization for Standardization. (2018). *ISO/IEC 27000:2018(en)*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Internet Engineering Task Force. (2021). *Standardization roadmap on quantum key distribution networks.* https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2021-07-26-itu-t-sg-13-opsawg-ls-on-work-progress-on-quantum-key-distribution-qkd-network-in-sg13-as-of-july-2021-attachment-1.pdf

ISACA. (2021). *CMMI cybermaturity platform*. https://www.isaca.org/enterprise/cmmi-cybermaturity-platform

Ismail, Y., & Petruccione, F. (2018). The race towards quantum security. *2018 IST-Africa Week Conference*. https://ieeexplore.ieee.org/abstract/document/8417339

ISO/IEC. (2018). *ISO/IEC 27000:2018(en).* https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ITU-T. (2020). *Security considerations for quantum key distribution networks*. https://www.itu.int/hub/publication/t-tut-qkd-2020-1/

Jakob, P. (2023, April 13). Chinese quantum companies and national strategy 2023. *The Quantum Insider*. https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/

Jarzabkowski, P., Mohrman, S. A., & Scherer, A. G. (2010). Organization studies as applied science: The generation and use of academic knowledge about organizations introduction to the special issue. *Organization Studies*, *31*(9–10), 1189–1207. https://doi.org/10.1177/0170840610374394

Javadi-Abhari, A., Patil, S., Kudrow, D., Heckey, J., Lvov, A., Chong, F. T., & Martonosi, M. (2014). ScaffCC: A framework for compilation and analysis of quantum computing programs. *Proceedings of the 11th ACM Conference on Computing Frontiers.* https://doi.org/10.1145/2597917.2597939

Jennewein, T. (2018). Towards quantum communications with satellites. *2018 IEEE Photonics Society Summer Topical Meeting Series*. https://doi.org/10.1109/PHOSST.2018.8456781

Jing, J., Ma, Y., Wang, Q., Long, Z., & Dong, S. (2020). Realization of cyons and anyons by atoms. *International Journal of Theoretical Physics, 59*(9), 2830–2838. https://doi.org/10.1007/s10773-020-04543-9

Ji-Seop, K., & Kim, S. (2024, February 15). S. Korea to launch quantum cloud services, UAM test flights. *The Chosun Daily*. https://www.chosun.com/english/national-en/2024/02/15/R65DC6VLG5AGRHYCGBAEFRZAWI/

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 138–146. https://doi.org/10.5688/ajpe7120

Johnson, W. G. (2019). Governance tools for the second quantum revolution. *Jurimetrics, 59*(4), 487–522.

Jordan, S. P., & Liu, Y. (2019). Quantum cryptanalysis: Shor, Grover, and beyond. IEEE Security & Privacy, 16(5), 14–21. https://doi.org/10.1109/MSP.2018.3761719

Jordan, S. (n.d.). Quantum algorithm zoo. Retrieved December 13, 2024, from https://quantumalgorithmzoo.org/

Joshi, M., Mishra, M., & Karthikeyan, S. (2024). Leveraging Grover's Algorithm for Quantum Searchable Encryption in Cloud Infrastructure and its application in AES Resource Estimation. *International Journal of Theoretical Physics, 63*(8), . https://doi.org/10.1007/s10773-024-05751-3

Kademeteme, E., & Twinomurinzi, H. (2019). The ineffectiveness of technology adoption models in the 4IR era: A case of SMEs in South Africa. *Open Innovations*, 252–261. https://doi.org/10.1109/OI.2019.8908220

Kamanghad, A., Khorasgani, G. H., Kazemi, M. A., & Shadnoosh, N. (2019). Assessing the company's e-readiness for implementing mobile-CRM system: Case a nationwide distribution company. *Journal of Information Systems and Telecommunication, 7*(1), 65–73. https://doi.org/10.7508/jist.2019.01.006

Kandala, A., Temme, K., Córcoles, A. D., Mezzacapo, A., Chow, J. M., & Gambetta, J. M. (2019). Error mitigation extends the computational reach of a noisy quantum processor. *Nature*, 567(7749), 491–495. https://doi.org/10.1038/s41586-019-1040-7

Karabulut, E., & Aysu, A. (2021). FALCON down: Breaking FALCON post-quantum signature scheme through side-channel attacks. 2021 58th ACM/IEEE Design Automation Conference, 691–696. https://doi.org/10.1109/DAC18074.2021.9586131

Kaur, M. (2023). *Overview of quantum initiatives worldwide 2023*. Retrieved May 10, 2023, from https://qureca.com/overview-of-quantum-initiatives-worldwide-2023

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social Sciences, 8*(9), 255. https://doi.org/10.3390/socsci8090255

Kavanagh, C. (2021). *Digital technologies and civil conflicts: Insights for peacemakers*. European Union Institute for Security Studies. http://www.jstor.org/stable/resrep30222

Keall, C. (2023, November 26). 10 pressing issues for new Technology Minister Judith Collins. *The New Zealand Herald*. https://www.nzherald.co.nz/business/10-pressing-issues-for-new-technology-minister-judith-collins/C7OY3VC5FRDC3PZ5BTURMU3U24/

Kelemen, M., & Rumens, N. (2013). *American pragmatism and organization: Issues and controversies*. Gower.

Kelly, J., Barends, R., Fowler, A. G., Megrant, A., Jeffrey, E., White, T. C., Sank, D., Mutus, J. Y., Campbell, B., Chen, Y., Chen, Z., Chiaro, B., Dunsworth, A., Hoi, I. C., Neill, C., O'Malley, P. J. J., Quintana, C., Roushan, P., Vainsencher, A., … Martinis, J. M. (2015). State preservation by repetitive error detection in a superconducting quantum circuit. *Nature, 519*, 66–69. https://doi.org/10.1038/nature14270

Kelly, M. L., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2). https://doi.org/10.1177/2059799120937242

Kiljan, S., Simoens, K., & De Cock, D. (2017). A survey of authentication and communications security in online banking. *ACM Computing Surveys, 49*(4), 1–35. https://doi.org/10.1145/3002170

Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly, 33*(3), 567–582. https://doi.org/10.2307/20650309

Kim, D., Choi, H., & Seo, S. C. (2024a). *Parallel Implementation of SPHINCS plus With GPUs*. IEEE Transactions On Circuits And Systems I-Regular Papers. https://doi.org/10.1109/TCSI.2024.3370802

Kim, M., Kang, M., Kim, J., Hong, Y., & Lee, G. (2024b). Flexible and Wearable Encryption Primitive Based on Optical Physically Unclonable Functions. *IEEE Journal of Selected Topics in Quantum Electronics, Selected Topics in Quantum Electronics. 30*(3), 1-8. https://doi.org/10.1109/JSTQE.2023.3345178

Kjaergaard, M., Schwartz, M. E., Braumüller, J., Krantz, P., Wang, J. I. J., Gustavsson, S., & Oliver, W. D. (2020). Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics, 11*, 369–395. https://doi.org/10.1146/annurev-conmatphys-031119-050605

Kolberg, J., Drozdowski, P., Gomez-Barrero, M., Rathgeb, C., & Busch, C. (2020). Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption. *2020 International Conference of the Biometrics Special Interest Group.* https://ieeexplore.ieee.org/document/9548305

Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I. G., . . . Laflamme, R. (2024a). Towards Responsible Quantum Technology: Safeguarding, Engaging and Advancing Quantum R&D. *UC Law Science and Technology Journal, 15*(1), 63-94.

Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I. G., . . . Laflamme, R. (2024b). Ten principles for responsible quantum innovation. *Quantum Science And Technology, 9*(3), 035013-35025. https://doi.org/10.1088/2058-9565/ad3776

Krinner, S., Lacroix, N., Remm, A. et al. Realizing repeated quantum error correction in a distance-three surface code. (2022). *Nature, 605*, 669–674. https://doi-org /10.1038/s41586-022-04566-8

Kuang, R., & Perepechaenko, M. (2022). *Digital Signature Performance of a New Quantum Safe Multivariate Polynomial Public Key Algorithm*. 7th International Conference on Computer and Communication Systems (ICCCS), 419-424. https://doi.org/10.1109/ICCCS55155.2022.9846785

Kukutai, T., Cormack, D., & & Cormack, D. (2020). Not one byte more: From data colonialism to data sovereignty In A. Chen (Ed.), *Shouting zeros and ones: Digital technology, ethics and policy in New Zealand* (pp. 28–34). Bridget Williams Books.

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security & Privacy, 5*(2), 1-10. https://doi.org/10.1002/spy2.200

Kurnia, S., Alzougool, B., Ali, M., & Alhashmi, S. M. (2009). Adoption of electronic commerce technologies by SMEs in Malaysia. *42nd Hawaii International Conference on System Sciences,* 1–10. https://doi.org/10.1109/HICSS.2009.49

Kurohi, R. (2022, May 31). S'pore boosts investments in quantum computing with 2 new programmes. *The Straits Times*. https://www.straitstimes.com/tech/tech-news/spore-boosts-investments-in-quantum-computing-with-2-new-programmes-heng-swee-keat

Lami, L. (2020). Completing the grand tour of asymptotic quantum coherence manipulation. *IEEE Transactions on Information Theory, 66*(4), 2165–2183. https://doi.org/10.1109/TIT.2019.2945798

Lamport, L. (1979). *Constructing digital signatures from one-way function*. Microsoft. https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/

Lan, C., Li, H., & Wang, C. (2020). Cryptanalysis of "certificateless remote data integrity checking using lattices in cloud storage". *2020 10th International Conference on Information Science and Technology*. https://doi.org/10.1109/ICIST49303.2020.920210

Lange, T. (2018). *Results of PQCRYPTO (ICT-645622) post-quantum cryptography for long-term security*. Commission of the European Communities. http://hyperelliptic.org/tanja/vortraege/tpm-ws.pdf

Lanteigne, M. (2021, September 19). AUKUS without us: New Zealand's responses to a new Indo-Pacific alliance. *The Diplomat*. https://thediplomat.com/2021/09/aukus-without-us-new-zealands-responses-to-a-new-indo-pacific-alliance/

Learner, S. (2023, May 3). Quantum computing could break the internet. This is how. *The Financial Times*. https://ig.ft.com/quantum-computing/

Lee, A. S., & Liebenau, J. (1997). Information systems and qualitative research. In A. S. Lee, J. Liebenau, & J. I. DeGross (Eds.), *Information systems and qualitative research* (pp. 1–8). Springer. https://doi.org/10.1007/978-0-387-35309-8_1

Lee, K., & Joshi, K. (2017). Examining the use of status quo bias perspective in IS research: Need for re-conceptualizing and incorporating biases. *Information Systems Journal, 27*(6), 733–752. https://doi.org/10.1111/isj.12118

Lee, J., Kim, H., Si, S., & Lee, S. (2024). Techno-nationalism to collaborative technology sovereignty. *Science And Public Policy*. https://doi.org/10.1093/scipol/scae046

Lees, M. J., Crawford, M., & Jansen, C. (2018). Towards industrial cybersecurity resilience of multinational corporations. *IFAC–PapersOnLine, 51*(30), 756–761. https://doi.org/10.1016/j.ifacol.2018.11.201

Le Van, L. (2019). An improved identity-based multivariate signature scheme based on rainbow. *Cryptography, 3*(1), 8. https://doi.org/10.3390/cryptography3010008

Li, F., Chen, T., Li, M., & Lin, C. (2024). Efficient and Verifiable General Quantum Secret Sharing Based on Special Entangled State. *IEEE Internet of Things Journal, 11*(8), 14127-14135. https://doi.org/10.1109/JIOT.2023.3339715

Liang, M., & Yang, L. (2020). Block encryption of quantum messages. *Quantum Information Processing, 19*(4), 111–135. https://doi.org/10.1007/s11128-020-2612-z

Lichtman, M. (2013). *Qualitative research in education: A user's guide* (3rd ed.). SAGE. https://doi.org/10.4324/9781003281917

Liman, A., & Weber, K. (2023). Quantum computing: Bridging the national security-digital sovereignty divide. *European Journal of Risk Regulation*, *14*(3), 476–483. https://doi.org/10.1017/err.2023.44

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, *30*, 73–84. https://doi.org/10.1002/ev.1427

Lindsay, J. (2020). Surviving the quantum cryptocalypse. *Strategic Studies Quarterly, 14*(2), 49–73.

Lorino, P. (2018). *Pragmatism and organization studies*. Oxford University Press. https://doi.org/10.1093/oso/9780198753216.001.0001

Ma, Z., & Zhang, S. (2020). Risk-based multi-attribute decision-making for normal cloud model considering pre-evaluation information. *IEEE Access, 8*, 153891–153904. https://doi.org/10.1109/ACCESS.2020.3018153

Mabad, T., Ali, O., Ally, M., Wamba, S. F., & Chan, K. C. (2021). Making investment decisions on RFID technology: An evaluation of key adoption factors in construction firms. *IEEE Access, 9*, 36937–36954. https://doi.org/10.1109/ACCESS.2021.3063301

Mahmoud, M. (2023). *The Involvement of Quantum Computing in the Realm of Cybersecurity*. International Conference on Computational Science and Computational Intelligence (CSCI), 881-886. https://doi.org/10.1109/CSCI62032.2023.00147

Mailloux, L. O., Lewis, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-quantum cryptography: What advancements in quantum computing mean for IT professionals. *IT Professional*, *18*(5), 42–47. https://doi.org/10.1109/MITP.2016.77

Manning, R. A. (2020). *Emerging technologies: New challenges to global stability*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/06/Emerging-Technologies-New-Challenges-To-Global-Stability-May-2020.pdf

Marshall, C., & Rossman, G. (2006). *Designing qualitative research* (4th ed.). SAGE.

Mathews, M., V, P., & Ajith, V. (2024). Quantum Cryptanalysis of Affine Cipher. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 14*(3), 507-519. https://doi.org/10.1109/JETCAS.2024.3428436

McArdle, S., Endo, S., Aspuru-Guzik, A., Benjamin, S. C., & Yuan, X. (2020). Quantum computational chemistry. *Reviews of Modern Physics*, *92*(1). https://doi.org/10.1103/revmodphys.92.015003

McGrew, D., Curcio, M., & Fluhrer, S. (2019). *Internet-draft: Hash-based signatures*. Internet Engineering Task Force. https://datatracker.ietf.org/doc/rfc8554/

McGrew, D., Kampanakis, P., Fluhrer, S., Gazdag, S., Butin, D., & Buchmann, J. (2016). State management for hash-based signatures. *Security Standardisation Research: Third International Conference*. https://doi.org/10.1007/978-3-319-49100-4_11

McKinsey & Company. (2023). Quantum *technology monitor*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., & Voznak, M. (2021). Quantum key distribution: A networking perspective. *ACM Computing Surveys, 53*(5), 96–136. https://doi.org/10.1145/3402192

Menand, L. (2001). *The metaphysical club: A story of ideas in America*. HarperCollins.

Merkle, R. C. (1989). A certified digital signature. *Advances in Cryptology — CRYPTO' 89 Proceedings.* https://doi.org/10.1007/0-387-34805-0_21

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Metz, C. (2020, February 10). White House earmarks new money for A.I. and quantum computing. *New York Times*. https://www.nytimes.com/2020/02/10/technology/white-house-earmarks-new-money-for-ai-and-quantum-computing.html

Michael, J., Kuhn, R., & Voas, J. (2020). Cyberthreats in 2025. *Computer, 53*(6), 16–27. https://doi.org/10.1109/MC.2020.2983529

Mills, J., & Birks, M. (2014). *Qualitative methodology: A practical guide*. SAGE. https://doi.org/10.4135/9781473920163

Min, S., So, K. K. F., & Jeong, M. (2019). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. *Journal of Travel & Tourism Marketing, 36*(7), 770–783. https://doi.org/10.1080/10548408.2018.1507866

Ministry of Business, Innovation & Employment. (n.d.). Focus area: Enhancing the skills and talent pipeline. Retrieved January 10, 2024, from https://www.mbie.govt.nz/business-and-employment/economic-development/industry-policy/industry-transformation-plans/digital-technologies/digital-technologies-industry-transformation-plan/focus-area-enhancing-the-skills-and-talent-pipeline/

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review*, *4*(10), 33–39. https://doi.org/10.22215/timreview837

Molla, A., & Licker, P. (2005). Perceived e-readiness factors in e-commerce adoption: An empirical investigation in a developing country. *International Journal of Electronic Commerce, 10*(1), 83–110. https://doi.org/10.1080/10864415.2005.11043963

Mone, G. (2020). The quantum threat: Cryptographers are developing algorithms to ensure security in a world of quantum computing. *Communications of the ACM, 63*(7), 12–14. https://doi.org/10.1145/3398388

Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process*. NIST. https://doi.org/10.6028/NIST.IR.8309

Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics 38*(8).

Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative Inquiry*, *20*(8), 1045–1053. https://doi.org/10.1177/1077800413513733

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Moses, S., Baldwin, C., Allman, M., Ancona, R., Ascarrunz, L., Barnes, C., . . . Vogt, E. (2023). A Race-Track Trapped-Ion Quantum Processor. *Physical Review X, 13*(4), . https://doi.org/10.1103/PhysRevX.13.041052

Munro, W. J., & Nemoto, K. (2020). Routing on quantum repeater networks. *2020 Conference on Lasers and Electro-Optics*. https://doi.org/10.1364/cleo_qels.2020.fth3d.4

Murison, A. (2021). Cybercrime: A growing business during Covid-19: While the world was in lockdown, cybercriminals were hard at work, finding more efficient ways to extract money from hacking into computer systems -- and Asia Pacific is firmly in their sights. *Journal of the Australian & New Zealand Institute of Insurance & Finance, 44*(3), 36–40.

National Cyber Security Centre. (n.d.). *Thinking ahead: Being prepared*. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Resilience-Assessment.pdf

National Cyber Security Centre. (2019). *Cybersecurity governance*. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Intro-Nov-2019.pdf

National Cyber Security Centre. (2020). *Cyber threat report 2019/20*. https://www.gcsb.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Threat-Report-2020.pdf

National Cyber Security Centre. (2022). *Cyber threat report 2021/2022*. https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-NCSC-Cyber-Threat-Report.pdf

National Cyber Security Centre. (2023). *Cyber threat report 2022/2023*. https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2022.2023-Cyber-Threat-Report.pdf

National Institute of Standards and Technology. (2018a). *Framework for improving critical infrastructure cybersecurity version 1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2018b). *NIST special publication 800-series general information*. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

National Institute of Standards and Technology. (2020). *Post-quantum cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography

National Institute of Standards and Technology. (2021). *Getting ready for post-quantum cryptography.* https://doi.org/NIST/CSWP/NIST.CSWP.04282021

National Institute of Standards and Technology. (2023). *Cryptography in the quantum age*. https://nist.gov/physics/introduction-new-quantum-revolution/cryptography-quantum-age

National Institute of Standards and Technology. (2024a). August 13, 2024. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. Retrieved https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

National Institute of Standards and Technology. (2024b). August 13, 2024. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024c). August 13, 2024. *Module-Lattice-Based Digital Signature Standard*. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024d). August 13, 2024. *Stateless Hash-Based Digital Signature Standard.* https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2024e). *NIST IR 8547: Interim public draft*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

National Quantum-Safe Network Singapore. (n.d.). *About NQSN*. https://www.nqsn.sg/

National Science & Technology Council. (2018). *National strategic overview for quantum information science*. https://www.quantum.gov/wpcontent/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf

National Science & Technology Council. (2023). *National quantum initiative supplement to the President's FY 2023 budget*. https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf

National Security Agency. (2020, October 29). *NSA's laboratory for physical sciences announces first-ever qubit collaboratory*. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2397829/nsas-laboratory-for-physical-sciences-announces-first-ever-qubit-collaboratory/

Nature Research. (2024). *Exploring many paths to realize quantum computers*. https://www.nature.com/articles/d42473-023-00442-9

Nayak, C. (2023, June 21). Microsoft achieves first milestone towards a quantum supercomputer. *Microsoft Azure Quantum Blog*. https://cloudblogs.microsoft.com/quantum/2023/06/21/microsoft-achieves-first-milestone-towards-a-quantum-supercomputer/

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys, 51*(6), 1–41. https://doi.org/10.1145/3292548

New Zealand Digital Skills Forum. (2021). *Digital skills for a digital nation*. https://nztech.org.nz/wp-content/uploads/sites/8/2019/02/Digital-Skills-for-a-digital-nation-online.pdf

New Zealand Government. (2011). New Zealand's Cyber Security Strategy June 2011. https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-june-2011_0.pdf

New Zealand Government. (2019). *New Zealand's cyber security strategy 2019*. https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019

New Zealand Government. (2021). *Espionage and foreign interference threats: Security advice for members of the New Zealand Parliament and locally elected representatives*. https://protectivesecurity.govt.nz/assets/Campaigns/PSR-ElectedOfficials-spreads.pdf

New Zealand Government. (2022a). *2022/23 action plan for the digital strategy for Aotearoa*. https://www.digital.govt.nz/dmsdocument/238~202223-action-plan-for-the-digital-strategy-for-aotearoa/html

New Zealand Government. (2022b). *Te rautaki matihiko mō Aotearoa: The digital strategy for Aotearoa*. https://www.digital.govt.nz/assets/Digital-government/Strategy/Digital-Strategy-for-Aotearoa-English-PDF.pdf

New Zealand Government. (2023a). *Budget 2024 update*. https://budget.govt.nz/

New Zealand Government. (2023b, July 26). *Government strengthens cyber security* [Press release]. https://www.beehive.govt.nz/release/government-strengthens-cyber-security

New Zealand Institute of Physics. (2021, August 20). *Statement from the New Zealand Institute of Physics on release of Phase 2 NCEA Level 1 Physics and Earth & Space Science material*. https://nzip.org.nz/wp-content/uploads/2021/08/NZIPPositionOnPhase2NCEALevel1PhysicsAndEarthSpaceScience20Aug21.pdf

New Zealand Technology Industry Association Incorporated. (2022, June 15). Diversity critical for NZ tech sector's future. *NZTECH*. https://nztech.org.nz/2022/06/15/diversity-critical-for-nz-tech-sectors-future/

Nghihalwa, E., & Shava, F. B. (2018). An assessment of cloud computing readiness in the Namibian Government's information technology departments. *2018 19th IEEE Mediterranean Electrotechnical Conference*, 92–97. https://doi.org/10.1109/MELCON.2018.8379074

Ngoc, L., & Hoang, D. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience, 18*(4). https://doi.org/10.12694/scpe.v18i4.1329

Nikolopoulos, G., & Fischlin, M. (2020). Information-theoretically secure data origin authentication with quantum and classical resources. *Cryptography, 4*(4), 31. https://doi.org/10.3390/cryptography4040031

Nivelkar, M., & Bhirud, S. (2021). Supervised machine learning strategies for investigation of weird pattern formulation from large volume data using quantum computing. *Advanced Computing and Intelligent Technologies*, 569-576. https://doi.org/10.1007/978-981-16-2164-2_45

Nominet-Cyber. (2019). *CISO-report*. https://media.nominet.uk/wp-content/uploads/2019/02/12130924/Nominet-Cyber_CISO-report_FINAL-130219.pdf

North Atlantic Treaty Organization. (2023). *Emerging and disruptive technologies*. https://www.nato.int/cps/en/natohq/topics_184303.htm

Ntanos, A., Lyras, N., Stathis, A., Giannoulis, G., Panagopoulos, A., & Avramopoulos, H. (2024). Satellite-to-Ground QKD in Urban Environment: A Comparative Analysis of Small-Sized Optical Ground Stations. *IEEE Aerospace and Electronic Systems Magazine, 39*(6), 16-29. https://doi.org/10.1109/MAES.2024.3383817

Official Journal of the European Union. (2022). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030* (PE/50/2022/REV/1). http://data.europa.eu/eli/dec/2022/2481/oj

Ogburn, W. F. (1957). Cultural lag as theory. *Sociology and Social Research*, *41*, 167–174. https://doi.org/10.1108/03068299710179026

Ogunyemi, A. A., & Johnston, K. A. (2012). Towards an organisational readiness framework for emerging technologies: An investigation of antecedents for South African organisations' readiness for server virtualisation. *Electronic Journal of Information Systems in Developing Countries, 53*(1), 1–30. https://doi.org/10.1002/j.1681-4835.2012.tb00378.x

Oishi, S. M. (2003). A few words about qualitative interviewing. In S. M. Oishi (Ed.), *How to conduct in-person interviews for surveys* (pp. 171–180). SAGE. https://doi.org/10.4135/9781412984416

Organisation for Economic Co-operation and Development. (2023). *Building a skilled cyber security workforce in five countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*. https://doi.org/10.1787/4e2269c3-en

Oshikawa, N. (2019, November 23). Japan plots 20-year race to quantum computers, chasing US and China. *NIKKEIAsia.* https://asia.nikkei.com/Business/Technology/Japan-plots-20-year-race-to-quantum-computers-chasing-US-and-China

Palacios-Berraquero, C., Mueck, L., & Persaud, D. M. (2019). Instead of 'supremacy' use 'quantum advantage'. *Nature*, *576*(7786), 213–214. https://doi.org/10.1038/d41586-019-03781-0

Palmer, D., Dick, B., & Freiburger, N. (2009). Rigor and relevance in organization studies. *Journal of Management Inquiry*, *18*(4), 265–272. https://doi.org/10.1177/1056492609343491

Pan, J., Chen, Y., Yin, J., Ren, J., Cao, Y., Li, Z., ... & Wang, J. (2020). Integrated quantum communication network over 4,600 km. *Nature, 589*(7841), 214–219. https://doi.org/10.1038/s41586-020-03093-8

Papylev, D. S., Babichev, A. V., Nadtochiy, A. M., Dragunova, A. S., Kryzhanovskaya, N. V., Karachinsky, L. Y., . . . Egorov, A. Y. (2024). *Self-Assembled InGaAs Quantum Dots with Reduced Inhomogeneous Broadening.* 2024 International Conference on Electrical Engineering and Photonics, 270-273. https://doi.org/10.1109/EExPolytech62224.2024.10755942

Park, D. K., Petruccione, F., & Rhee, J.-K. K. (2019). Circuit-based quantum random access memory for classical data. *Scientific Reports*, *9*(1). https://doi.org/10.1038/s41598-019-40439-3

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th. ed.). SAGE.

Paykin, J., Rand, R., & Zdancewic, S. (2017). QWIRE: A core language for quantum circuits. *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages.* https://doi.org/10.1145/3009837.3009894

Pednault, E., Gunnels, J. A., Nannicini, G., Horesh, L., & Wisnieff, R. (2019). Leveraging secondary storage to simulate deep 54-qubit sycamore circuits. *arXiv*. https://doi.org/10.48550/arXiv.1910.09534

Peredaryenko, M. S., & Krauss, S. E. (2013). Calibrating the human instrument: Understanding the interviewing experience of novice qualitative researchers. *Qualitative Report*, *18*(43), 1–17. https://doi.org/10.46743/2160-3715/2013.1449

Pew Research Center. (2021, June 16). Experts doubt ethical AI design will be broadly adopted as the norm in the next decade. https://www.pewresearch.org/internet/2021/06/16/ethical-ai-design-about-this-canvassing-of-experts/

Polites, G. L., & Karahanna, E. (2013). The embeddedness of information systems habits in organisational and individual level routines: Development and disruption. *MIS Quarterly, 37*(1), 221–246. https://www.jstor.org/stable/43825944

Pontolillo, G., & Mousavi, M. R. (2024). *Delta Debugging for Property-Based Regression Testing of Quantum Programs*. IEEE/ACM 5th International Workshop on Quantum Software Engineering (Q-SE), 1-8. https://doi-org/10.1145/3643667.3648219

Possati, L.M. (2023). Ethics of Quantum Computing: an Outline. Philos. *Technol. 36* (48). https://doi.org/10.1007/s13347-023-00651-6

Potomac Institute for Policy Studies. (2015). *Cyber readiness index 2.0. A plan for cyber readiness: A baseline and an index*. https://www.potomacinstitute.org/images/CRIndex2.0.pdf

The Pūtaiora Writing Group. (2010). *Te ara tika: Guidelines for Māori research ethics: A framework for researchers and ethics committee members*. Health Research Council. http://www.hrc.govt.nz/assets/pdfs/publications/Te%20Ara%20Tika%20R21Jul10.pdf

PWC. (2023). *Startup investment*. https://www.pwc.co.nz/insights-and-publications/2023-publications/startup-investment-magazine-spring-2023.html

QBN. (2023, April 27). EUR 3 billion action plan for quantum technologies by German government. *QBN News*. https://qbn.world/eur-3-billion-action-plan-for-quantum-technologies-by-german-government/

Qi, M., & Chen, J. (2022). Provably secure post-quantum authenticated key exchange from supersingular isogenies. *Journal of Supercomputing, 78*(10), 12815. https://doi.org/10.1007/s11227-022-04378-7

Qiang, X., Zhou, X., Wang, J., Wilkes, C. M., Loke, T., O'Gara, S., Kling, L., Marshall, G. D., Santagati, R., Ralph, T. C., Wang, J. B., O'Brien, J. L., Thompson, M. G., & Matthews, J. C. F. (2018). Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. *Nature Photonics, 12*(9), 534. https://doi.org/10.1038/s41566-018-0236-y

Qin, H., Tang, W., & Tso, R. (2020). Hierarchical quantum secret sharing based on special high-dimensional entangled state. *IEEE Journal of Selected Topics in Quantum Electronics, 26*(3), 1–6. https://doi.org/10.1109/JSTQE.2020.2975600

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Quantum Delta Nederland. (2019). *National agenda for quantum technology*. https://qutech.nl/wp-content/uploads/2019/09/NAQT-2019-EN.pdf

The Quantum Economic Development Consortium. (2021). *A guide to a quantum-safe organisation*. https://quantumconsortium.org/guide-to-a-quantum-safe-organization/

Quantum Engineering Programme Singapore. (2022, May 31). *Singapore's quantum ecosystem gets a boost from three national platforms*. https://qepsg.org/singapores-quantum-ecosystem-gets-a-boost-from-three-national-platforms/

Quantum Technologies Strategic Advisory Board. (2015). *National strategy for quantum technologies: A new era for the UK*. *https://www.ukri.org/wp-content/uploads/2021/12/IUK-071221-NationalQuantumTechnologyStrategy.pdf*

QuTech. (2024, January 25). *Fujitsu and Delft University of Technology establish new quantum lab*. https://qutech.nl/2024/01/25/fujitsu-and-delft-university-of-technology-establish-new-quantum-lab/

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight, 20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020

Randles, S., Loconto, A., & Steen, M. (2024). Demonstrating the deep institutionalisation of de facto responsible research and innovation (rri) in participatory market contexts: Examples from Bolivia and the Netherlands. *Journal of Responsible Innovation, 11*(1), https://doi.org/10.1080/23299460.2024.2316365

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE Access, 12*, 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520

Riedel, M., Calarco, T., Binosi, D., & Thew, R. (2017). The European quantum technologies flagship programme. *Quantum Science and Technology, 2*(3). https://doi.org/10.1088/2058-9565/aa6aca

Rigetti, C. (2017). Introducing Forest 1.0. *Medium.* https://medium.com/rigetti/introducing-forest-f2c806537c6d

Rim, H. J. (2023). The US-China Strategic Competition and Emerging Technologies in the Indo-Pacific Region: Strategies for Building, Dominating, and Managing Networks. *Asian Perspective, 47*(1), 1-25. https://doi.org/10.1353/apr.2023.0000

Roberson, T., Leach, J., & Raman, S. (2021). Talking about public good for the second quantum revolution: Analysing quantum technology narratives in the context of national strategies. *Quantum Science and Technology*, *6*(2). https://doi.org/10.1088/2058-9565/abc5ab

Roberson, T. (2023). Talking About Responsible Quantum: “Awareness Is the Absolute Minimum that … We Need to Do”. *NanoEthics, 17*(1). https://doi.org/10.1007/s11569-023-00437-2

Roberts, R. E. (2020). Qualitative interview questions: Guidance for novice researchers. *The Qualitative Report*, *25*(9), 3185–3203. https://doi.org/10.46743/2160-3715/2020.4640

Robinson, C. (2023, December 6). NZ’s healthcare system needs a major technology upgrade. *The New Zealand Herald*. https://www.nzherald.co.nz/business/cecilia-robinson-a-call-for-transformative-change-in-healthcare/G7TCEM5SJZDFLNVGT35NYBK5YA/

Rogers, E. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Rolfe, G. (2006). Validity, trustworthiness and rigour: Quality and the idea of qualitative research. *Journal of Advanced Nursing*, *53*(3), 304–310. https://doi.org/10.1111/j.1365-2648.2006.03727.x

Roman, R., Arjona, R., & Baturone, I. (2024). A quantum-safe authentication scheme for IoT devices using homomorphic encryption and weak physical unclonable functions with no helper data. *Internet Of Things, 28*, 101389-101401. https://doi.org/10.1016/j.iot.2024.101389

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). SAGE.

Russian Quantum Center. (2024). *What we do*. https://www.rqc.ru/about

Sahu, S. K., Mazumdar, K., Gong, L., & Dong, Y. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics*, 1-13. https://doi.org/10.3389/fphy.2024.1456491

Saks, M., & Allsop, J. (Eds.). (2013). *Researching health: Qualitative, quantitative and mixed methods* (2nd ed.). SAGE.

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). SAGE.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty, 1*(1), 7–59. https://doi.org/10.1007/BF00055564

Sanjab, A., Saad, W., & Basar, T. (2017). Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. *2017 IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC.2017.7996862

Savin-Baden, M. (2013). *Qualitative research: The essential guide to theory and practice*. Routledge.

Schoelkopf, R. (2016). Quantum computing with superconducting circuits. *2016 IEEE International Interconnect Technology Conference / Advanced Metallization Conference*, 43–44. https://doi.org/10.1109/IITC-AMC.2016.7507674

Schroeder, A., & Pauleen, D. (2007). KM governance: Investigating the case of a knowledge intensive research organisation. *Journal of Enterprise Information Management*, *20*(4), 414–431. https://doi.org/10.1108/17410390710772696

Scott, J. (1990). *A matter of record: Documentary sources in social research*. Polity Press.

Securities and Exchange Commission. (2023, July 26). *SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies* [Press release]. https://www.sec.gov/news/press-release/2023-139

Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (4th ed.). Teachers College Press.

Senthoor, K., & Sarvepalli, P. (2024). Communication Efficient Quantum Secret Sharing via Extended CSS Codes. *IEEE Journal on Selected Areas in Communications, 42*(7), 1818-1829. https://doi.org/10.1109/JSAC.2024.3380082

Serrano, M. A., Cruz-Lemus, J. A., Perez-Castillo, R., & Piattini, M. (2023). Quantum Software Components and Platforms: Overview and Quality Assessment. *ACM Computing Surveys, 55*(8), 1-30. https://doi.org/10.1145/3548679

Seshadreesan, K. P., Krovi, H., & Guha, S. (2019). A continuous-variable quantum repeater based on quantum scissors. *2019 Conference on Lasers and Electro-Optics*. https://doi.org/10.1364/CLEO_QELS.2019.FTh4A.5

Sewell, K. M., Mishna, F., Sanders, J. E., Bogo, M., Milne, B., & Greenblatt, A. (2023). Supervision of information communication technologies in social work practice: A mixed methods study. *The British Journal of Social Work*, *53*(1), 490–512. https://doi.org/10.1093/bjsw/bcac113

Shafi, S., & Mallinson, D. J. (2023). The potential of smart home technology for improving healthcare: A scoping review and reflexive thematic analysis. *Housing and Society*, *50*(1), 90–112. https://doi.org/10.1080/08882746.2021.1989857

Shah, A., Pereira, P., & Tuma, P. (2021). Quality improvement at times of crisis. *BMJ*, *373*, n928. https://doi.org/10.1136/bmj.n928

Shi, R. (2020). Useful equations about bell states and their applications to quantum secret sharing. *IEEE Communications Letters, 24*(2), 386–390. https://doi.org/10.1109/LCOMM.2019.2954134

Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, *52*(4), R2493–R2496. https://doi.org/10.1103/PhysRevA.52.R2493

Shrivastava, P., Soni, K. K., & Rasool, A. (2019). Evolution of quantum computing based on Grover's search algorithm. *2019 10th International Conference on Computing, Communication and Networking Technologies*. https://doi.org/10.1109/ICCCNT45670.2019.8944676

Simpson, B., & den Hond, F. (2022). The contemporary resonances of classical pragmatism for studying organization and organizing. *Organization Studies*, *43*(1), 127–146. https://doi.org/10.1177/0170840621991689

Smyslov, V. (2024). Use of hybrid post-quantum key exchange in internet protocols. *Journal of Computer Virology and Hacking Techniques*, Preprints, 1-8. https://doi.org/10.1007/s11416-024-00515-3

Sophos. (2023). *The state of ransomware 2023*. https://www.sophos.com/en-us/whitepaper/state-of-ransomware

Sparkes, M. (2022). Code designed to protect against quantum hackers is 'useless'. *New Scientist, 253*(3377), 15. https://doi.org/10.1016/s0262-4079(22)00417-1

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/Commentary on a past article: "Verification Strategies for Establishing Reliability and Validity in Qualitative Research". *International Journal of Qualitative Methods*, *17*(1). https://doi.org/10.1177/1609406918788237

Steffen, M., DiVincenzo, D. P., Chow, J. M., Theis, T. N., & Ketchen, M. B. (2011). Quantum computing: An IBM perspective. *IBM Journal of Research and Development*, *55*(5), 13:1–13:11. https://doi.org/10.1147/jrd.2011.2165678

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management, 26*(1), 2–12. https://doi.org/10.1080/10580530802384639

Sun, S., Zhang, R., & Ma, H. (2020). Efficient parallelism of post-quantum signature scheme SPHINCS. *IEEE Transactions on Parallel and Distributed Systems, 31*(11), 2542–2555. https://doi.org/10.1109/TPDS.2020.2995562

Swayne, M. (2023, February 28). Top quantum spenders based on GDP — List offers surprising changes in leadership status. *The Quantum Insider*. https://thequantuminsider.com/2023/02/28/top-quantum-spenders-based-on-gdp-list-offers-surprising-changes-in-leadership-status/

Swayne, M. (2024a, February 19). South Korea sets stage for technological revolution with quantum computing initiatives. *The Quantum Insider*. https://thequantuminsider.com/2024/02/19/south-korea-sets-stage-for-technological-revolution-with-quantum-computing-initiatives/

Swayne, M. (2024b, March 7). France 2030: Progress update three years after the launch of the National quantum technologies strategy and the launch of the PROQCIMA program. *The Quantum Insider*. https://thequantuminsider.com/2024/03/07/france-2030-progress-update-three-years-after-the-launch-of-the-national-quantum-technologies-strategy-and-the-launch-of-the-proqcima-program/

Szepieniec, A., & Preneel, B. (2020). Block-anti-circulant unbalanced oil and vinegar. In K. Paterson& D. Stebila (Eds.), *Selected areas in cryptography – SAC 2019* (pp. 574–588). https://doi.org/10.1007/978-3-030-38471-5_23

Tabassum, T., & Akter, F. (2023). *QRAM: Quantum Technology for Random Access Memory*. 26th International Conference on Computer and Information Technology (ICCIT), 1-4. https://doi.org/10.1109/ICCIT60459.2023.10441238

Tashakkori, A., & Teddlie, C. (Eds.). (2003). *Handbook of mixed methods in social & behavioral research*. SAGE.

TASS. (2023, February 22). Russia creates 20-qubit quantum computer – Rosatom. *TASS: Russian News Agency*. https://tass.com/science/1749867

Teddlie, C., & Tashakkori, A. (2003). Major issues and controversies in the use of mixed methods in the social and behavioural sciences. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioural research* (pp. 3–49). SAGE.

Tellez, C., Pereira, D., & Borges, F. (2019). Trade-off between performance and security for coding and ring learning with errors-based Diffie-Hellman cryptosystems. *2019 II Workshop on Metrology for Industry 4.0 and IoT*. https://doi.org/10.1109/METROI4.2019.8792913

Ten Holter, C., Inglesant, P., Srivastava, R., & Jirotka, M. (2022). Bridging the quantum divides: A chance to repair classic(al) mistakes? *Quantum Science And Technology, 7*(4), 044006-44010. https://doi.org/10.1088/2058-9565/ac8db6

Ten Holter, C., Inglesant, P., & Jirotka, M. (2023). Reading the road: Challenges and opportunities on the path to responsible innovation in quantum computing. *Technology Analysis & Strategic Management, 35*(7), 844-856. https://doi.org/10.1080/09537325.2021.1988070

Thapliyal, H., & Humble, T. (Eds.). (2023). *Quantum computing: Circuits, systems, automation and applications*. Springer.

Tines. (2023). *Voice of the SOC 2023*. https://www.tines.com/reports/voice-of-the-soc-2023

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust,* 223–228. https://doi.org/10.1109/PST.2016.7906931

Trager, R. F. (2022). The security governance challenge of emerging technologies. *Orbis, 66*(4), 536–550. https://doi.org/10.1016/j.orbis.2022.08.008

Truong, N., Haw, J., Assad, S., Lam, P., & Kavehei, O. (2019). Machine learning cryptanalysis of a quantum random number generator. *IEEE Transactions on Information Forensics and Security, 14*(2), 403–414. https://doi.org/10.1109/TIFS.2018.2850770

Tsuchimoto, Y., Nakamura, I., Shirai, S. (2024). Superconducting surface trap chips for microwave-driven trapped ions. *EPJ Quantum Technol. 11*, 56. https://doi.org/10.1140/epjqt/s40507-024-00269-3

Turner, D. (2022). *Understanding NIST's orocess on post-quantum cryptography (PQC) standardization.* https://www.cryptomathic.com

Tusun, M., Wu, Y., Liu, W., Rong, X., & Du, J. (2019). Experimental implementation of a continuous-time quantum random walk on a solid-state quantum information processor. *Chinese Physics B, 28*(11), 110302–110305. https://doi.org/10.1088/1674-1056/ab44ae

Tverskoi, D., Babu, S., & Gavrilets, S. (2022). The spread of technological innovations: Effects of psychology, culture and policy interventions. *Royal Society Open Science*, *9*(6), 211833. https://doi.org/10.1098/rsos.211833

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453–458. https://doi.org/10.1126/science.7455683

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*(4), 297–323. https://doi.org/10.1007/BF00122574

Uğurlu, A. D., Thyrrestrup, H., Uppu, R., Ouellet-Plamondon, C., Schott, R., Wieck, A. D., Ludwig, A., Lodahl, P., & Midolo, L. (2020). Suspended spot-size converters for scalable single-photon devices. *Advanced Quantum Technologies*, *3*(2). https://doi.org/10.1002/qute.201900076

Uppu, R., Pedersen, F. T., Wang, Y., Olesen, C. T., Papon, C., Zhou, X., Midolo, L., Scholz, S., Wieck, A. D., Ludwig, A., & Lodahl, P. (2020). Scalable integrated single-photon source. *Science Advances*, *6*(50), 1–6. https://doi.org/10.1126/sciadv.abc8268

US Department of Defense. (2016). *DOD directive 3020.40: Mission assurance (MA)*. https://fas.org/irp/doddir/dod/d3020_40.pdf

US Department of Defense. (2023). AUKUS: The trilateral security partnership between Australia, U.K. and U.S. https://www.defense.gov/Spotlights/AUKUS/

US Government Publishing Office. (2022). *H.R.7535 – Quantum Computing Cybersecurity Preparedness Act*. https://www.congress.gov/bill/117th-congress/house-bill/7535/text

Uzoka, F. M. E. (2008). Organisational influences on e-commerce adoption in a developing country context using UTAUT. *International Journal of Business Information Systems*, *3*(3), 300–316. https://doi.org/10.1504/IJBIS.2008.017287

Valdez, F., & Melin, P. (2023). A review on quantum computing and deep learning algorithms and their applications. *Soft Computing*, *27*(18), 13217–13236. https://doi.org/10.1007/s00500-022-07037-4

van der Heijden, J., Kobayashi, T., House, M. G., Salfi, J., Barraud, S., Laviéville, R., Simmons, M. Y., & Rogge, S. (2018). Readout and control of the spin-orbit states of two coupled acceptor atoms in a silicon transistor. *Science Advances, 4*(12). https://doi.org/10.1126/sciadv.aat9199

Vannatta, S. (2011). The pragmatism reader: From Peirce through the present. In R. B. Talisse & S. F. Aiken (Eds.), Princeton University Press , 2011. In (Vol. 7, pp. 85-91).

Van Steenbergen, M., Bos, R., Brinkkemper, S., Van De Weerd, I., & Bekkers, W. (2010). The design of focus area maturity models. In R. Winter, J. L. Zhao, & S. Aier (Eds.) *Global perspectives on design science research* (pp. 317–332). Springer. https://doi.org/10.1007/978-3-642-13335-0_22

Vasiloiu, I. (2023). Cyber diplomacy: *A new frontier for global cooperation in the digital age*. *Informatica Economică*, *27*(1), 41–50. https://doi.org/10.24818/issn14531305/27.1.2023.04

Venegas-Gomez, A. (2020). The quantum ecosystem and its future workforce: A journey through the funding, the hype, the opportunities, and the risks related to the emerging field of quantum technologies. *PhotonicsViews*, *17*(6), 34–38. https://doi.org /10.1002/phvs.202000044

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478. https://doi.org/10.2307/30036540

Verizon. (2021). *2021 data breach investigations report (DBIR)*. https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics And Information Technology*, *19*(4), 241–246. https://doi.org/10.1007/s10676-017-9429-1

Vigliar, C., Paesani, S., Adcock, J., Morley-Short, S., Thompson, M., Rarity, J., . . . Wang, J. Error-protected qubits in a silicon photonic chip. *Nature Physics, 17*(10), 1137. https://doi.org/10.1038/s41567-021-01333-w

Viksna, J., Kozlovics, S., & Rencis, E. (2023). POSTER: *Integrating quantum key distribution into hybrid quantum-classical networks*. In J. Zhou, L. Batina, Z. Li, J. Lin, E. Losiouk, S. Majumdar, D. Mashima, W. Meng, M. A. Rahman, J. Shao, M. Shimaoka, E. Soremekun, C. Su, J. S. Teh, A. Udovenko, C. Wang, & Y. Zhauniarovich (Eds.), Applied cryptography and network security workshops: ACNS 2023 satellite workshops. 13907, pp. 695–699. Springer. https://doi.org/10.1007/978-3-031-41181-6_42

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. *Communications of the ACM, 62*(4), 120–129. https://doi.org/10.1145/3241037

Walsh, K., & Love-Grayer, L. (2023). *Global cybercrime: Federal agency efforts to address international partners' capacity to combat crime* (GAO-23-104768). U.S. Government Accountability Office. https://www.gao.gov/products/gao-23-104768

Wang, S., Chen, W., Yin, Z.-Q., Li, H.-W., He, D.-Y., Li, Y.-H., Zhou, Z., Song, X.-T., Li, F.-Y., Wang, D., Chen, H., Han, Y.-G., Huang, J.-Z., Guo, J.-F., Hao, P.-L., Li, M., Zhang, C.-M., Liu, D., Liang, W.-Y., … Han, Z.-F. (2014). Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express, 22*(18), 21739. https://doi.org/10.1364/OE.22.021739

Wang, S., Chen, W., Yin, Z.-Q., Zhang, Y., Zhang, T., Li, H.-W., Xu, F.-X., Zhou, Z., Yang, Y., Huang, D.-J., Zhang, L.-J., Li, F.-Y., Liu, D., Wang, Y.-G., Guo, G.-C., & Han, Z.-F. (2010). Field test of wavelength-saving quantum key distribution network. *Optics Letters*, *35*(14), 2454–2456.

Wang, X., Qiu, H., & Xie, F. (2017). A survey on the industrial readiness for internet of things. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, 591–596. https://doi.org/10.1109/UEMCON.2017.8249015

Wang, X.-L., Chen, L.-K., Li, W., Huang, H. L., Liu, C., Chen, C., Luo, Y. H., Su, Z. E., Wu, D., Li, Z. D., Lu, H., Hu, Y., Jiang, X., Peng, C. Z., Li, L., Liu, N. L., Chen, Y.-A., Lu, C.-Y., & Pan, J.-W. (2016). Experimental ten-photon entanglement. *Physical Review Letters*, *117*(21), https://doi.org/10.1103/PhysRevLett.117.210502

Ward, A., & Bambos, N. (2020). *Quantum annealing assisted deep learning for lung cancer detection*. Stanford University. http://vision.stanford.edu/teaching/cs231n/reports/2017/pdfs/534.pdf

Weber, M. (2015). Bureaucracy. In T. Waters & D. Waters (Eds.), *Rationalism and modern society: New translations on politics, bureaucracy, and social stratification* (pp. 37–58). Palgrave MacMillan.

Wen, X., Zhao, X., Gong, L., & Zhou, N. (2019). A semi-quantum authentication protocol for message and identity. *Laser Physics Letters, 16*(7), 75206–75215. https://doi.org/10.1088/1612-202X/ab232c

Wendin, G. (2017). Quantum information processing with superconducting circuits: A review. *Reports on Progress in Physics*, *80*(10), 106001. https://doi.org/10.1088/1361-6633/aa7e1a

Wengraf, T. (2001). *Qualitative research interviewing*. SAGE.

The White House. (2023). *National cybersecurity strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Wibowo, T. S., Endroyono, E., & Pratomo, I. (2020). Analysis of Malang City readiness in realising smart tourism with new integrated e-readiness model. *International Conference on Smart Technology and Applications*. https://doi.org/10.1109/ICoSTA48221.2020.1570616406

Wicks, A. C., & Freeman, R. E. (1998). Organization studies and the new pragmatism: Positivism, anti-positivism, and the search for ethics. *Organization Science*, *9*(2), 123–140. https://doi.org/10.1287/orsc.9.2.123

Wiesner, K. (2017). The careless use of language in quantum information. *arXiv*. https://doi.org/10.48550/arXiv.1705.06768

Wiggans, A. (2023, March 22). Making the grade: Why NZ kids are falling behind at school. *The New Zealand Herald*. https://www.nzherald.co.nz/nz/making-the-grade-new-zealands-struggling-school-education-system-how-we-can-do-better/VDDQDPYUYBFMRL2RMWFUB7DS54/

Wiggans, A. (2023, April 20). Changes to the roll-out of the curriculum refresh and new NCEA assessment have gained mixed responses. *The New Zealand Herald*. https://www.nzherald.co.nz/nz/changes-to-the-roll-out-of-the-curriculum-refresh-and-new-ncea-assessment-have-gained-mixed-responses/3KJ6KG5MUVCYNPE4MDMINJNGQM/

Wilson, J. R. (2020, August 26). The future of artificial intelligence and quantum computing. *Military & Aerospace Electronics*. https://www.militaryaerospace.com/computers/article/14182330/future-of-artificial-intelligence-and-quantum-computing

Wolff, J. (2021). How is technology changing the world, and how should the world change technology? *Global Perspectives*, *2*(1). https://doi.org/10.1525/gp.2021.27353

World Economic Forum. (2022a). *State of quantum computing: Building a quantum economy*. https://www.weforum.org/publications/state-of-quantum-computing-building-a-quantum-economy/

World Economic Forum. (2022b). *Transitioning to a quantum-secure economy*. https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/

World Economic Forum. (2023, June 30). *The European Union's Artificial Intelligence Act, explained*. https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/

World Economic Forum. (2024a). *Global cybersecurity outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

World Economic Forum (WEF). (2024b). *Quantum economy blueprint 2024*. https://www3.weforum.org/docs/WEF_Quantum_Economy_Blueprint_2024.pdf

Wu, H., Yin, Z., Tong, X., Ding, P., Xie, J., Wang, L., Liu, P., Song, H., Chen, X., Xu, L., Xu, S., & Zhang, Y. (2020). An experimental demonstration of long-haul public-channel key distribution using matched superlattice physical unclonable function pairs. *Science Bulletin, 65*(11), 879. https://doi.org/10.1016/j.scib.2020.02.029

Xia, F., Liu, J., Nie, H., Fu, Y., Wan, L., & Kong, X. (2020). Random walks: A review of algorithms and applications. *IEEE Transactions on Emerging Topics in Computational Intelligence, 4*(2), 95–107. https://doi.org/10.1109/TETCI.2019.2952908

Ying, M., Ying, S., & Wu, X. (2017). Invariants of quantum programs: Characterisations and generation. *ACM SIGPLAN Notices, 52*(1), 818–832. https://doi.org/10.1145/3093333.3009840

Yoneda, J., Takeda, K., Noiri, A., Nakajima, T., Li, S., Kamioka, J., Kodera, T., & Tarucha, S. (2020). Quantum non-demolition readout of an electron spin in silicon. *Nature Communications, 11*(1), 1–7. https://doi.org/10.1038/s41467-020-14818-8

Younus, A. M., Tarazi, R., Younis, H., & Abumandil, M. (2022). The role of behavioural intentions in implementation of bitcoin digital currency factors in terms of usage and acceptance in New Zealand: Cyber security and social influence. *ECS Transactions*, *107*(1), 10847. https://doi.org/10.1149/10701.10847ecst

Zhang, Y., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., Huang, Y., Xu, C., Zhang, X., Wang, Z., Li, M., Zhang, X., Zheng, Z., Chu, B., Gao, X., Meng, N., Cai, W., Wang, Z., Wang, G., … Guo, H. (2019). Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology, 4*(3), 035006. https://doi.org/10.1088/2058-9565/ab19d1

Zhang, Y., Luan, Z., Zhang, X., Shu, J., & Wang, P. (2019). PbS quantum dots based on physically unclonable function for ultra high-density key generation. *Journal of Electronic Materials, 48*(12), 7603–7607. https://doi.org/10.1007/s11664-019-07660-2

Zhang, Y., Shang, T., Liu, J., & Wu, W. (2020). Quantum homomorphic encryption based on quantum obfuscation. *2020 International Wireless Communications and Mobile Computing*. https://doi.org/10.1109/IWCMC48107.2020.9148407

Zhao, Y. (2019). The integration of QKD and security services. *Proceedings of the ITU QIT4N Workshop Shanghai*. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Yong

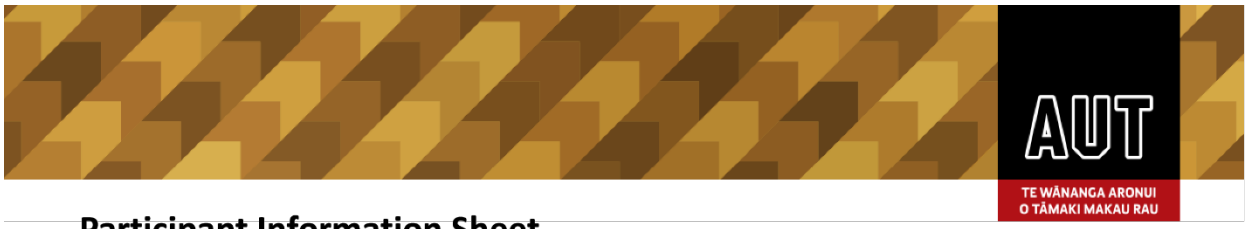
Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., Qin, J., Wu, D., Ding, X., Hu, Y., Hu, P., Yang, X.-Y., Zhang, W.-J., Li, H., Li, Y., Jiang, X., Gan, L., Yang, G., You, L., … Pan, J.-W. (2020). Quantum computational advantage using photons. *Science, 370*(6523), 1460–1463. https://doi.org/10.1126/science.abe8770

Zhu, S., & Han, Y. (2020). Analysis of McEliece public cryptography using Deep AutoEncoder. *2020 39th Chinese Control Conference*. https://doi.org/10.23919/CCC50068.2020.9188592

Zundel, M., & Kokkalis, P. (2010). Theorizing as engaged practice. *Organization Studies*, *31*(9/10), 1209–1227. https://doi.org/10.1177/0170840610374405

Appendices

Appendix A: Participant Information Sheet Round 1 and Round 2



Participant Information Sheet

Date Information Sheet Produced:

10 June 2022

Project Title

Cyberthreats in a quantum computing enabled world – A study of New Zealand's role and readiness.

An Invitation

My name is Nicole Girvan and I am currently researching New Zealand's readiness to face the potential cybersecurity threats that a quantum computing enabled world may pose. This research is in support of a Doctor of Philosophy.

I would like to invite you to take part in this research by way of a semi-structured interview, which would take around 50 minutes, at a time and place convenient to you. You have been purposefully selected as a potential participant on the basis of your role and level of experience and expertise in the ICT sector.

Participation is of course voluntary and, should you agree to participate, you may withdraw your consent at any time.

What is the purpose of this research?

The escalating nature of cyberattacks demonstrates that increasing New Zealand's cyber resilience is critical to maintaining a stable and thriving business ecosystem. Unfortunately, the cybersecurity mechanisms fundamental for New Zealand's safety and security, such as the use of cryptography to secure data communication, are increasingly threatened by emerging technology such as quantum computing.

The cryptographic algorithms that currently enable Public Key Infrastructure and secure communications globally rely upon the assumption that certain mathematical problems are intractable. A widely used example is the "discrete-log problem on elliptic curves". Unfortunately, quantum computing introduces such an enormous paradigm shift in the underlying technology that new threats and attacks will become possible, and perhaps even trivial, to execute. Functioning quantum computing at scale will have a devastating impact on several of the main cryptographic algorithms in use today. For example, Peter Shor's quantum computing based integer factorisation algorithm can break all PKI systems that use RSA, Elliptic-curve and Diffie–Hellman cryptography by providing an exponentially faster way to solve problems such as the discrete-log.

This research will identify the level of awareness and preparedness of New Zealand organisations to face the emerging cybersecurity threats posed by a quantum computing enabled world. It will additionally investigate New Zealand's role in global conversations relating to these emerging threats.

This research aims to produce actionable knowledge on emerging threat preparedness for practical use in the New Zealand business landscape. Insights and recommendations regarding specific policy and practices that New Zealand could adopt to combat these threats will also be described.

The research will form completion of a Doctor of Philosophy and it is also anticipated that the findings of this research may be used for academic publications and presentations.

How was I identified and why am I being invited to participate in this research?

You have been purposefully selected as someone who can comment specifically on the issues surrounding preparedness to face emerging cybersecurity threats in the New Zealand business landscape. I have selected a range of participants from medium to large New Zealand organisations in order to understand a variety of different perspectives.

How do I agree to participate in this research?

Your participation in this research is voluntary (it is your choice) and whether or not you choose to participate will neither advantage nor disadvantage you. You are able to withdraw from the study at any time. If you choose to withdraw from the study, then you will be offered the choice between having any data that is identifiable as belonging to you removed or allowing it to continue to be used. However, once the findings have been produced, removal of your data may not be possible.

Attached with this email is a consent form. This form asks that you confirm your understanding of the research process, that consent maybe withdrawn at any time, and whether you would like a copy of the final research report. Confirming consent via this form is a requirement of the AUT Ethics Committee and makes it transparent that you agree to participate and fully understand the process.

What will happen in this research?

A total of around 40 participants will be interviewed using a semi-structured interview format for this research. Each interview is expected to take around 50 minutes. In your interview, a standard set of questions will be asked of you and you will be invited to respond openly and contribute your insights, experiences and perspectives in this area.

What are the discomforts and risks?

The research process has been designed in such a way that free and frank discussion is encouraged and you are not put in a position of feeling uncomfortable or at risk. Potential issues that may arise, however, include potential commercial sensitivity if answering a question from the perspective of any organisation you work for.

How will these discomforts and risks be alleviated?

Your interview will be recorded and transcribed. You will have the opportunity to validate the interview transcript and the transcript will only be used in the research with your explicit approval. This will additionally enable the identification and removal of any comments which appear to be commercially sensitive.

What are the benefits?

This research is being undertaken in fulfilment of a Doctor of Philosophy qualification at AUT. It is furthermore anticipated that this research will provide valuable knowledge on the understudied area of New Zealand's preparedness for emerging cybersecurity threats in a quantum enabled world, ultimately enabling better preparation and mitigation of these threats.

How will my privacy be protected?

Your identity and the identity of your business will remain confidential in all research output. Your responses will be de-identified. In some cases, actual quotes from interviews may be used but only with the explicit approval of the person who made them.

What are the costs of participating in this research?

The cost to you is expected to total approximately 1-2 hours of your time, encompassing the interview itself and the familiarisation with this information sheet. An additional 30 minutes may also be required for the review of the interview transcription.

What opportunity do I have to consider this invitation?

This information sheet is attached to your email invitation to participate. The interview day/time will be set at least two weeks away from your receipt of this information and at a time convenient to you. You may withdraw your consent at any time.

Will I receive feedback on the results of this research?

You will receive a 1-2 page summary of the final research report if you have indicated you wish to do so in the consent form.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Professor Marilyn Waring, Marilyn.waring@aut.ac.nz, 09 021 9999 ext. 8306.

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTEC, *ethics@aut.ac.nz* , (+649) 921 9999 ext 6038.

Whom do I contact for further information about this research?

Please keep this Information Sheet and a copy of the Consent Form for your future reference.

Researcher Contact Details:

You may contact the researcher via email at Nicole.girvan@aut.ac.nz or via telephone on 0272773549.

Project Supervisor Contact Details:

The project supervisor. Professor Marilyn Waring, may be contacted via email at Marilyn.waring@aut.ac.nz,or via telephone at 09 021 9999 ext. 8306.

Approved by the Auckland University of Technology Ethics Committee on Approved by the Auckland University of Technology Ethics Committee on 13 June 2022. AUTEC Reference number 22/136.

Participant Information Sheet

Date Information Sheet Produced:

01 March 2022

Project Title

Cyberthreats in a quantum computing enabled world – A study of New Zealand's role and readiness.

An Invitation

My name is Nicole Girvan and I am currently researching New Zealand's readiness to face the potential cybersecurity threats that a quantum computing enabled world may pose. This research is in support of a Doctor of Philosophy.

I would like to invite you to take part in this research by way of a semi-structured interview, which would take around 50 minutes, at a time and place convenient to you. You have been purposefully selected as a potential participant on the basis of your role and level of experience and expertise relevant to this research.

Participation is of course voluntary and, should you agree to participate, you may withdraw your consent at any time.

What is the purpose of this research?

The escalating nature of cyberattacks demonstrates that increasing New Zealand's cyber resilience is critical to maintaining a stable and thriving business ecosystem. Unfortunately, the cybersecurity mechanisms fundamental for New Zealand's safety and security, such as the use of cryptography to secure data communication, are increasingly threatened by emerging technology such as quantum computing.

The cryptographic algorithms that currently enable Public Key Infrastructure and secure communications globally rely upon the assumption that certain mathematical problems are intractable. A widely used example is the "discrete-log problem on elliptic curves". Unfortunately, quantum computing introduces such an enormous paradigm shift in the underlying technology that new threats and attacks will become possible, and perhaps even trivial, to execute. Functioning quantum computing at scale will have a devastating impact on several of the main cryptographic algorithms in use today. For example, Peter Shor's quantum computing based integer factorisation algorithm can break all PKI systems that use RSA, Elliptic-curve and Diffie–Hellman cryptography by providing an exponentially faster way to solve problems such as the discrete-log.

Quantum technology is very specialised and building and maintaining a quantum infrastructure requires a stable government, reliable power grid, roading infrastructure, and a highly educated population. The number of entities capable of building this technology is limited to those with the significant wealth required to invest in necessary components such as shielded facilities, supercooling technology, rare materials, and intellectual capital. A valid concern is that poorer nations will not have the ability to build quantum-safe cryptography into all facets of their economy leaving them vulnerable on the global stage.

Other ethical concerns also exist when discussing quantum computing, including questions such as how free speech or any level of privacy is maintained in a world whereby governments or large private institutions with quantum computing can decrypt all communications. These complex ethical and moral issues suggest the transition to a world with quantum computing is not straightforward, and governments may need to take a leading role in guiding the introduction of this technology. However, at this stage, no legal or policy-based frameworks have emerged to support the governing of quantum technologies.

This research will identify the level of awareness and preparedness of New Zealand organisations to face the emerging cybersecurity threats posed by a quantum computing enabled world. It will additionally investigate New Zealand's role in global conversations relating to these emerging threats. This research aims to produce actionable knowledge on emerging threat preparedness for practical use in the New Zealand business landscape. Insights and recommendations regarding specific policy and practices that New Zealand could adopt to combat these threats will also be described.

The research will form completion of a Doctor of Philosophy and it is also anticipated that the findings of this research may be used for academic publications and presentations.

How was I identified and why am I being invited to participate in this research?

You have been selected purposefully as someone who can comment specifically on the role New Zealand is playing or might play in global conversations around preparedness to face the emerging cybersecurity threats and the power imbalances that quantum-enabled computing may pose. I have selected a range of participants from the academic, political and business arenas in order to understand a variety of different perspectives. In many cases, the participants are known to the me; however, in others, participants have been recommended by other experts and contact is being made via those third parties.

How do I agree to participate in this research?

Attached with this email is a consent form. This form asks that you confirm your understanding of the research process, that consent maybe withdrawn at any time, and whether you would like a copy of the final research report. Confirming consent via this form is a requirement of the AUT Ethics Committee and makes it transparent that you agree to participate and fully understand the process.

What will happen in this research?

A total of around 40 participants will be interviewed using a semi structured interview format for this research. Each interview is expected to take around 50 minutes. In your interview a standard set of questions will be asked of you and you will be invited to respond openly and contribute your insights , experiences and perspectives in this area.

What are the discomforts and risks?

The research process has been designed in such a way that free and frank discussion is encouraged and you are not put in a position of feeling uncomfortable or at risk. Potential issues that may arise, however, include potential commercial sensitivity if answering a question from the perspective of any organisation you work for.

How will these discomforts and risks be alleviated?

Your interview will be recorded and transcribed. You will have the opportunity to validate the interview transcript and the transcript will only be used in the research with your explicit approval. This will additionally enable identification and removal of any comments which appear to be commercially sensitive.

What are the benefits?

This research is being undertaken in fulfilment of a Doctor of Philosophy qualification at AUT. It is furthermore anticipated that this research will provide valuable knowledge on the understudied area of New Zealand's preparedness for emerging cybersecurity threats in a quantum enabled world, ultimately enabling better preparation and mitigation of these threats.

How will my privacy be protected?

You will be anonymous in all research output. Your responses will be de-identified. In some cases, actual quotes from interviews may be used but only with the explicit approval of the person who made them.

What are the costs of participating in this research?

The cost to you is expected to total approximately one hour of your time, encompassing the interview itself and the familiarisation with this information sheet. An additional 30 minutes may also be required for review of the interview transcription.

What opportunity do I have to consider this invitation?

This information sheet is attached to your invitation to participate. The interview day/time will be set at least two weeks away from your receipt of this information and at a time convenient to you. You may withdraw your consent at any time.

Will I receive feedback on the results of this research?

You will receive a copy of the final research report if you have indicated you wish to do so in the consent form.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Professor Marilyn Waring, Marilyn.waring@aut.ac.nz, 09 021 9999 ext. 8306.

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTEC, *ethics@aut.ac.nz* , (+649) 921 9999 ext 6038.

Whom do I contact for further information about this research?

Please keep this Information Sheet and a copy of the Consent Form for your future reference.

Researcher Contact Details:

You may contact the researcher via email at Nicole.girvan@aut.ac.nz or via telephone on 0272773549.

Project Supervisor Contact Details:

The project supervisor. Professor Marilyn Waring, may be contacted via email at Marilyn.waring@aut.ac.nz,or via telephone at 09 021 9999 ext. 8306.

Approved by the Auckland University of Technology Ethics Committee on Approved by the Auckland University of Technology Ethics Committee on 13 June 2022. AUTEC Reference number 22/136.

Appendix B: Consent Form

Consent Form

Project title: *Cyberthreats in a quantum computing enabled world – A study of New Zealand's role and readiness*

Project Supervisor: *Professor Marilyn Waring*

Researcher: *Nicole Girvan*

- ○ I have read and understood the information provided about this research project in the Information Sheet dated 10 June 2022.
- ○ I have had an opportunity to ask questions and to have them answered.
- ○ I understand that notes will be taken during the interviews and that they will also be audio-taped and transcribed.
- ○ I understand that taking part in this study is voluntary (my choice) and that I may withdraw from the study at any time without being disadvantaged in any way.
- ○ I understand that if I withdraw from the study then I will be offered the choice between having any data that is identifiable as belonging to me removed or allowing it to continue to be used. However, once the findings have been produced, removal of my data may not be possible.
- ○ I agree to take part in this research.
- ○ I wish to receive a summary of the research findings (please tick one): Yes○ No○

Participant's signature: .....

Participant's name: .....

Participant's Contact Details (if appropriate):

.....

.....

.....

.....

Date:

Approved by the Auckland University of Technology Ethics Committee on 13 June 2022. AUTEC Reference number 22/136.

Note: The Participant should retain a copy of this form.

Appendix C: Interview Guide Round 1 and Round 2

Interview Guide (Round One)

Introduction:

Date of Interview:

Location of Interview:

Name of Interviewee:

Overview and purpose of this research

The cryptographic algorithms that currently enable Public Key Infrastructure and secure communications globally rely upon the assumption that certain mathematical problems are intractable. A widely used example is the "discrete-log problem on elliptic curves". Unfortunately, quantum computing introduces such an enormous paradigm shift in the underlying technology that new threats and attacks will become possible, and perhaps even trivial, to execute. Functioning quantum computing at scale will have a devastating impact on several of the main cryptographic algorithms in use today. For example, Peter Shor's quantum computing based integer factorisation algorithm can break all PKI systems that use RSA, Elliptic-curve and Diffie–Hellman cryptography by providing an exponentially faster way to solve problems such as the discrete-log.

The purpose of this research is to identify the level of awareness and preparedness of New Zealand organisations to face the emerging cybersecurity threats posed by a quantum computing enabled world. It will additionally investigate New Zealand's role in global conversations relating to these emerging threats.

This research aims to produce actionable knowledge on emerging threat preparedness for practical use in the New Zealand business landscape. Insights and recommendations regarding specific policy and practices that New Zealand could adopt to combat these threats will also be described.

The research will form completion of a Doctor of Philosophy and it is also anticipated that the findings of this research may be used for academic publications and presentations.

Information about interview procedure, informed consent and confidentiality

During this interview, you will be asked to respond to several open-ended questions. You may choose not to answer any or all of the questions. Your participation in this research is voluntary (it is your choice) and whether or not you choose to participate will neither advantage nor disadvantage you. You are able to withdraw from the study at any time. If you choose to withdraw from the study, then you will be offered the choice between having any data that is identifiable as belonging to you removed or allowing it to continue to be used. However, once the findings have been produced, removal of your data may not be possible.

The procedure will involve recording the interview and this recording will then be transcribed verbatim. You may elect for your identity to remain confidential in any research output. In which case, your confidentiality and the confidentiality of your institute or organisation will be maintained and neither you nor your institute or organisation will be able to be identified. The procedure will involve recording the interview and this recording will then be transcribed verbatim. You may elect to remain anonymous in any research output. In which case, your confidentiality and the confidentiality of your organisation will be maintained and neither you nor your business will be able to be identified individually.

Draft Questions

1. Can you tell me what you know about the threats quantum enabled computing may pose to existing systems and cybersecurity mechanisms used today?
2. What is your opinion on the risk these threats pose to your organisation?
    a. What (if anything) would change or influence your opinion on this?
3. Can you describe the current processes in your business for identifying and validating cyber threats and preparing to respond to these?
4. How has your organisation considered the threat that quantum enabled computing poses to cybersecurity mechanisms, if at all?
5. How do you see the IT Industry supporting your organisational readiness to address the cybersecurity threats that quantum computing may pose?
6. What influence do vendors have on your decisions around preparing for cyberthreats?
7. What role do you see the government playing in supporting your organisation to prepare for cyberthreats posed by quantum enabled technology?
8. What influence do your third-party relationships (such as other businesses, partners, industry bodies) have on your preparedness decisions?
9. What factors do you believe have influenced your organisations decisions to plan or not plan for the cyberthreats posed by quantum enabled computing?
    a. What would accelerate your readiness to address these threats?
    b. What would prevent your organisation from preparing to address these threats?
10. Do you feel sufficiently prepared to face emerging threats such as those posed by quantum enabled computing?
    a. If so – what makes you feel confident in this area?
    b. If not – what do you believe needs to be addressed for you to be confident in your preparedness?

Closing

Thank you to the participant

Next steps and timeframes

Contact Information

Interview Guide (Round Two)

Introduction:

This interview protocol was designed to create consistency in the questions asked of each participant.

Date of Interview:

Location of Interview:

Name of Interviewee:

Overview and purpose of this research

The cryptographic algorithms that currently enable Public Key Infrastructure and secure communications globally rely upon the assumption that certain mathematical problems are intractable. Unfortunately, quantum computing introduces such an enormous paradigm shift in the underlying technology that new threats and attacks will become possible, and perhaps even trivial, to execute. Functioning quantum computing at scale will have a devastating impact on several of the main cryptographic algorithms in use today.

Quantum technology is also very specialised and building and maintaining a quantum infrastructure requires a stable government, reliable power grid, roading infrastructure, and a highly educated population. The number of entities capable of building this technology is limited to those with the significant wealth required to invest in necessary components such as shielded facilities, supercooling technology, rare materials, and intellectual capital. A valid concern is that poorer nations will not have the ability to build quantum-safe cryptography into all facets of their economy leaving them vulnerable on the global stage.

Other ethical concerns also exist when discussing quantum computing, including questions such as how free speech or any level of privacy is maintained in a world whereby governments or large private institutions with quantum computing can decrypt all communications. These complex ethical and moral issues suggest the transition to a world with quantum computing is not straightforward, and governments may need to take a leading role in guiding the introduction of this technology. However, at this stage, no legal or policy-based frameworks have emerged to support the governing of quantum technologies.

The purpose of this research is to investigate New Zealand's role in global conversations relating to the emerging cybersecurity threats posed by a quantum computing enabled world. It will also identify the level of awareness and preparedness of New Zealand organisations to face these threats. This research aims to produce actionable knowledge on emerging threat preparedness for practical use in the New Zealand business landscape. Insights and recommendations regarding specific policy and practices that New Zealand could adopt to combat these threats will also be described.

The research will form completion of a Doctor of Philosophy and it is also anticipated that the findings of this research may be used for academic publications and presentations.

Information about interview procedure, informed consent and confidentiality

During this interview you will be asked to respond to several open-ended questions. You may choose not to answer any or all of the questions. The procedure will involve recording the interview and this recording will then be transcribed verbatim. You may elect to remain anonymous in any research output. In which case, your confidentiality and the confidentiality of your institute or organisation will be maintained and neither you nor your institute or organs will be able to be identified individually.

Draft Questions

1. Can you tell me what you know about the threats quantum enabled computing may pose to existing systems and cybersecurity mechanisms used globally today?
2. What is your opinion on the risk these threats pose to current global power structures?
3. Can you describe any involvement that New Zealand has in global conversations or preparations for these emerging threats?
4. What role do you believe New Zealand could play in the global stage when discussing and planning for emerging technology threats such as those quantum-enabled computing pose?

Closing

Thank you to participant

Next steps and timeframes

Contact Information

Appendix D: Codebook – Interview Data

Name	Files	References
Acceptance of Cyber Incidents	8	14
Assigning accountability	12	39
Bus and Government need more collaboration on cybersecurity	7	10
Capacity for addressing cyberrisk	8	10
Commercial issues impact cybersecurity effectiveness	2	3
Compliance, regulation, standardisation drives preparation	8	24
Concern around quantum accessibility, approachability	23	53
Contingency and response plans	4	8
Current maturity level impacts risk and ability to prepare	22	63
Current technical defence strategies	4	6
Cyber is a hard, complex problem and no easy solutions	9	18
Cyber Risk Planning and Assessment	24	117
Cyberrisk visibility	7	13
Cybersecurity is important and not valued enough	8	10
Cyberthreat landscape is a high-risk environment	10	10
Ethical issue awareness	18	47
Fast pace of environment and rate of change is challenging	19	29
Feeling the Impact drives preparation	10	25
Frameworks and standards used in cyberrisk planning	13	28
Critically review existing structures such as IP law	2	3
General cybersecurity risk awareness is varied - it is growing but more is needed	21	96
Getting the basics right	9	15
Governance Structures	9	16
Government role in cyber should be limited to protecting public safety	4	6
Government should provide leadership and direction around emerging quantum threats	11	21
Helpless against cyberthreats, feel like we are victims and cannot win.	18	36

Name	Files	References
High Volume of work, overwhelm, limits preparation	16	44
Inappropriate or Insufficient legislation, regulation, mandates for emerging tech	24	76
Industry or technology specific factors	9	10
Influence of cyber at upper levels of the business	11	20
Innovation and Investment Opportunities	7	14
IT Industry Role	6	6
Lack of forum or formal opportunity to share info	6	11
Lack of national capacity or capability in emerging tech	11	19
Lack of transparent discussion and open information sharing	9	11
Legacy technology is a challenge	16	30
Legislation and standards creation is too slow	3	6
Limited Quantum enabled computing cyberthreat awareness	30	95
Need for tested quantum secure standards and solutions	18	27
Need for timely, trusted cyber intelligence and advisory	20	41
Need to all work together	11	34
Not confident we are prepared for emerging cyberthreats like quantum	11	14
Not my problem, lack of ownership	11	17
Not prepared for Quantum yet but confident in tackling emerging cyberthreats	12	13
NZ can exert global influence	5	6
NZ doesn’t have the money, resources, capacity or influence to compete internationally	12	20
NZ is a Tech consumer or taker and we do not have a unique role in QC	6	9
NZ is not doing enough, being left behind, lacking maturity.	13	30
NZ must build global alliances and collaborate through existing structures	9	14
NZ must determine its own approach to emerging tech threats includ QC	17	48
NZ needs clear and more transparent cybersecurity strategy	21	33
NZ should build quantum expertise and infrastructure	18	34
NZ should partner with other nations to develop quantum technology and industry	9	17
NZ should play an active role globally discussing emerging tech threats	19	24

Name	Files	References
NZs response influenced by global partners and geopolitics	11	18
Peers influence	15	34
People are key	8	15
Positive and interested in QC	14	19
Pressure should be put on vendors and providers to be secure	6	6
Providing incentives for cybersecurity	4	9
Public & private sector collaboration	7	8
Quantifying cyberrisk is hard - especially when threat theoretical in nature	21	56
Quantum threat not imminent enough to act	10	12
Relentlessness and novel attack landscape	12	23
Reliance on third parties or vendors impacts preparation	19	42
Risk appetite and behaviour	5	6
Risk Perception of Quantum enabled threats	32	146
Sense of inevitability, quantum and therefore quantum attacks will happen	12	25
Skills and resources and capacity and quantum industry	27	90
Solution options	3	4
Strategic thinking and planning capacity	19	55
Successful Cyber culture	1	1
Technology adaption levels	12	22
Technology Hype	5	5
Threat Intelligence sources	18	65
Trusted relationships for collaboration are vital	20	54
Understanding cyberrisk	12	18
Understanding cybersecurity is a constant journey not a destination	6	12
Value of open information sharing	16	40
Vendors influence cybersecurity preparation	27	83
We have a social responsibility in cyberspace	11	17

Appendix E: Codebook – Document Analysis

Name	Files	References
Broad & Cross functional consultation required	11	12
Build a skilled and diverse quantum tech workforce	20	110
Build and provide quantum infrastructure	17	64
Collaborate and cooperate more with international allies	16	49
Contribute and shape global thinking on ethical and secure tech use	17	55
Create bilateral, multilateral, and international partnerships	10	21
Create practical quantum use cases for industry	4	8
Create transparent national quantum strategy	18	41
Current national cyber capabilities not keeping up with environment	6	12
Demonstrate global leadership in QIS & Cyber	14	36
Develop International Standards for Quantum	12	31
Develop quantum technology solutions	11	25
Develop specific implementation plans for quantum goals	15	30
Develop specific IR plans	6	10
Develop thriving national quantum ecosystem	12	40
Develop, Test, and Implement quantum resistant cyber security cryptography and solutions	15	54
Drive awareness and provide info on quantum threats	17	34
Drive Economic growth & future proof economy	15	68
Drive industry, academia, government collaboration	16	54
Emerging quantum tech contributes to national digital sovereignty	11	23
Enable and drive early adoption	9	34
Enable innovation and quantum research commercialisation	15	74
Enhance regulatory frameworks	15	45
Ensure quantum accessibility and supply chain	15	40
Establish national quantum governance	8	13
Focus cybersecurity efforts more strategically	4	8

Name	Files	References
Focus on values in quantum technology development	15	51
Fund research on ethical use of quantum tech	3	3
Geopolitics is driving increased cyberthreats & response	14	27
Government must protect its own systems and act as role model	9	20
Grow government quantum capabilities & expertise	8	19
Hold those accountable for poor behaviour in cyberspace	3	7
Identify and secure vulnerable information and systems	4	5
National security and economic success rely on cyber security	4	10
Need to maintain national security	17	49
Now is the time to ramp up quantum efforts	11	22
Protect cyber insurance industry stability	1	1
Protect Intellectual Property	4	20
Quantum and emerging tech may lead to public harm and national security challenges	17	29
Quantum investment rqd for effective international partnerships	2	2
Quantum tech is expanding and evolving rapidly	5	6
Quantum tech provides national challenges and opportunities	13	25
Quantum tech will be transformative	2	3
Responsibility for cybersecurity must change	2	8
Support cross disciplinary and international QIS research	17	54
Technology innovation key to national prosperity	3	4

Appendix F: Document Analysis Document List

Document Title	Document Reference
ANSSI views on the Post-Quantum Cryptography transition.	ANSSI. (2022a). *ANSSI views on the Post-Quantum Cryptography transition.* https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf
Technical Position Paper: QKD v2.1 Should Quantum Key Distribution be Used for Secure Communications?	ANSSI. (2020). *Technical Position Paper: QKD v2.1 Should Quantum Key Distribution be Used for Secure Communications?* https://cyber.gouv.fr/sites/default/files/2020/05/anssi-technical_position_papers-qkd.pdf
Annual Review 2022	ANSSI. (2022b). *Annual Review 2022*. https://cyber.gouv.fr/actualites/anssi-annual-review-2022/
Growing Australia's Quantum Technology Industry	Commonwealth Scientific and Industrial Research Organisation (CSIRO). (2020). *Growing Australia's Quantum Technology Industry. https://www.csiro.au/-/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf*
New Zealand's Cyber Security Strategy 2019	Department of the Prime Minister and Cabinet (DPMC). (2019). *New Zealand's Cyber Security Strategy 2019.* https://www.dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
Australia's Cyber Security Strategy 2020.	Department of Home Affairs. (2020). *Australia's Cyber Security Strategy 2020*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
Let's talk about our national security: National Security Long Term Insights Briefing	Department of the Prime Minister and Cabinet (DPMC). (2023). *Let's talk about our national security: National Security Long Term Insights Briefing.* https://www.dpmc.govt.nz/sites/default/files/2023-05/National%20Security%20Long-term%20Insights%20Briefing.pdf
National Quantum Strategy Building a thriving future with Australia's quantum advantage.	Department of Industry, Science and Resources. (2023). *National Quantum Strategy Building a thriving future with Australia's quantum advantage.* https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf
National Quantum Strategy	Department for Science, Innovation and Technology. (2023). *National Quantum Strategy.* https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national_quantum_strategy.pdf
Australia's quantum advantage National Quantum Strategy: consultation paper	Department of Industry, Science and Resources. (2022). *Australia's quantum advantage National Quantum Strategy: consultation paper.* https://storage.googleapis.com/converlens-au-industry/industry/p/prj221726a232884dc6016a1/public_assets/Consultation%20Paper%20-%20National%20Quantum%20Strategy%20-%20FINAL.pdf
2023 - 2030 Australian Cyber Security Strategy Discussion Paper.	Department of Home Affairs. (2023). *2023 - 2030 Australian Cyber Security Strategy Discussion Paper. https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf*
Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030	European Parliament, Council of the European Union. (2022b). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030*. PE/50/2022/REV/1. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32022D2481

Document Title	Document Reference
Communication From the Commission to The European Parliament, The Council, The European Economic and Social Committee and the Committee Of The Regions 2030 Digital Compass: the European way for the Digital Decade	European Parliament, Council of the European Union. (2022a). *Communication From the Commission to The European Parliament, The Council, The European Economic and Social Committee and the Committee Of The Regions 2030 Digital Compass: the European way for the Digital Decade.* https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf
Strategic Research Agenda.	European Quantum Flagship. (2020). *Strategic Research Agenda. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65402*
Quantum-safe cryptography – fundamentals, current developments and recommendations.	Federal Office for Information Security (BSI). (2021). *Quantum-safe cryptography – fundamentals, current developments and recommendations. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6*
Cyber Security Strategy for Germany 2021	Federal Ministry of the Interior, B. a. C. (2021). *Cyber Security Strategy for Germany 2021.* https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=AE37C355F11195E09FFA474F486DD655.live892?__blob=publicationFile&v=4
Annual Report 2022	Federal Ministry of Education, Science and Research (BMBWF). (2022). *Annual Report 2022.* https://www.fwf.ac.at/fileadmin/Website/publications/Publikationen/FWF-Jahresberichte/fwf-jahresbericht-2022.pdf
MSP Supplier Panel Update 2022.	Government Communications Security Bureau. (2022a). *MSP Supplier Panel Update 2022*.
Impact Story Quantum Computing.	GESDA. (2022). *Impact Story Quantum Computing*. https://gesda.global/wp-content/uploads/2022/09/GESDA-Quantum-Computing-Impact-Story-Apr2022-1.pdf
Canada's National Quantum Strategy	Government of Canada. (2022). *Canada's National Quantum Strategy*. https://ised-isde.canada.ca/site/national-quantum-strategy/en
National Cyber Security Strategy 2019-2024	Government of Ireland. (2019). *National Cyber Security Strategy 2019-2024. https://assets.gov.ie/76728/567c89b8-47f6-4e13-8782-409cff8b5b94.pdf*
National Cyber Strategy 2022 - Pioneering a cyber future with the whole of the UK	HM Government. (2022). *National Cyber Strategy 2022 - Pioneering a cyber future with the whole of the UK.* https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
National Strategic Overview for Quantum Information Science	National Science & Technology Council. (2018). *National Strategic Overview for Quantum Information Science.* https://www.quantum.gov/wpcontent/uploads/2020/10/2018_NSTC_National_Strategic_Overview_QIS.pdf
National Quantum Initiative Supplement to the President's FY 2023 Budget.	National Science & Technology Council. (2023). *National Quantum Initiative Supplement to the President's FY 2023 Budget.* https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf
Te Rautaki Matihiko mō Aotearoa. The Digital Strategy for Aotearoa.	New Zealand Government. (2022a).*Te Rautaki Matihiko mō Aotearoa. The Digital Strategy for Aotearoa*. https://www.digital.govt.nz/assets/Digital-government/Strategy/Digital-Strategy-for-Aotearoa-English-PDF.pdf

Document Title	Document Reference
2022/23 Action Plan for the Digital Strategy for Aotearoa.	New Zealand Government (2022b). *2022/23 Action Plan for the Digital Strategy for Aotearoa.* https://www.digital.govt.nz/dmsdocument/238~202223-action-plan-for-the-digital-strategy-for-aotearoa/html
Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030.	Official Journal of the European Union. (2022). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030*. PE/50/2022/REV/1. http://data.europa.eu/eli/dec/2022/2481/oj
National strategy for quantum technologies A new era for the UK.	Quantum Technologies Strategic Advisory Board. (2015). *National strategy for quantum technologies A new era for the UK.* *https://www.ukri.org/wp-content/uploads/2021/12/IUK-071221-NationalQuantumTechnologyStrategy.pdf*
National Cybersecurity Strategy	The White House. (2023). *National Cybersecurity Strategy.* *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*
R.7535 - Quantum Computing Cybersecurity Preparedness Act.	U.S. Government Publishing Office. (2022). R.7535 - *Quantum Computing Cybersecurity Preparedness Act.* https://www.congress.gov/117/plaws/publ260/PLAW-117publ260.pdf
Transitioning to a Quantum-Secure Economy.	World Economic Forum. (2022b). *Transitioning to a Quantum-Secure Economy.* https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/

Appendix G: Ethical Approval

Auckland University of Technology Ethics Committee (AUTEC)

Auckland University of Technology
D-88, Private Bag 92006, Auckland 1142, NZ
T: +64 9 921 9999 ext. 8316
E: ethics@aut.ac.nz
www.aut.ac.nz/researchethics

22 June 2022

Marilyn Waring
Faculty of Culture and Society

Dear Marilyn

Ethics Application: 22/136 **Cyberthreats in a quantum computing enabled world – A study of New Zealand's role and readiness**

We advise you that the Auckland University of Technology Ethics Committee (AUTEC) has **approved** your ethics application at its meeting of 13 June 2022.

This approval is for three years, expiring 13 June 2025.

Standard Conditions of Approval

1. The research is to be undertaken in accordance with the Auckland University of Technology Code of Conduct for Research and as approved by AUTEC in this application.
2. A progress report is due annually on the anniversary of the approval date, using the EA2 form.
3. A final report is due at the expiration of the approval period, or, upon completion of project, using the EA3 form.
4. Any amendments to the project must be approved by AUTEC prior to being implemented. Amendments can be requested using the EA2 form.
5. Any serious or unexpected adverse events must be reported to AUTEC Secretariat as a matter of priority.
6. Any unforeseen events that might affect continued ethical acceptability of the project should also be reported to the AUTEC Secretariat as a matter of priority.
7. It is your responsibility to ensure that the spelling and grammar of documents being provided to participants or external organisations is of a high standard and that all the dates on the documents are updated.
8. AUTEC grants ethical approval only. You are responsible for obtaining management approval for access for your research from any institution or organisation at which your research is being conducted and you need to meet all ethical, legal, public health, and locality obligations or requirements for the jurisdictions in which the research is being undertaken.

Please quote the application number and title on all future correspondence related to this project.

For any enquiries please contact ethics@aut.ac.nz. The forms mentioned above are available online through http://www.aut.ac.nz/research/researchethics

(This is a computer-generated letter for which no signature is required)

The AUTEC Secretariat
Auckland University of Technology Ethics Committee

Cc: nicole.girvan@aut.ac.nz; Alastair Nisbet

Appendix H: Data Management Plan

AUCKLAND UNIVERSITY OF TECHNOLOGY ETHICS COMMITTEE (AUTEC)

Data Management Plan

DEFINITION & PURPOSE:

A data management plan describes how researchers are collecting, storing, and managing the use of data collected as part of their research. It describes how data is being stored now and in the future. It describes who has access to the data and for what purposes. It records the conditions under which the data was collected. It describes who has control over access to the data.

Project title and brief description:

Cyberthreats in a quantum computing enabled world – A study of New Zealand's role and readiness.

This research seeks to understand the preparedness of New Zealand organisations to face emerging quantum cybersecurity threats and New Zealand's role in global conversations relating to these emerging threats.

For the first round of interviews, a sample of 15-20 business leaders from a wide variety of large-scale New Zealand organisations (including organisations of national significance) is desired. I seek the views of these key business leaders in New Zealand companies around what preparedness for cybersecurity threats in a quantum would look like and what aspects of their environment are driving decision making and preparedness activities for these threats. By interviewing these stakeholders, I seek to capture their "lived" realities and understand their level of preparedness for quantum enabled cyber security threats.

For the second round of interviews a sample of 15-20 academic and political leaders will be asked their views around what New Zealand's role may be in global conversations around the cybersecurity threats emerging from quantum enabled computing and how we are or should contribute to these conversations as a nation.

Primary Researcher

Nicole Girvan

Supervisors or other researchers

Professor Marilyn Waring

Dr Alastair Nisbet

Who will have the primary responsibility for the data at the different stages of its life cycle?

The primary researcher

What is the nature of the data being collected and produced?

What type of data will be produced, used, or generated (both physical and digital)?

- ☒ Digital audio recording
- ☒ Written physical documentation
- ☒ Electronic documents and data (ms word files, pdfs, tables, qualitative analysis output such as NVIVO files)

How will data be collected and in what formats?

Data will be collected using semi structured interviews in audio and written format.

How will the data collection be documented so that others can work out what is involved? Is there a data dictionary?

The data will be coded for analysis in NVivo.

Will the data be reproducible?

If the same data collection method was used (for example the same interviews repeated) and the same methodology followed it is possible the data could be reproducible however this is not guaranteed as an interview is fluid and the participant may not disclose the same information the second time.

How much data will it be, and at what rate will it grow? How often will it change?

The data collected will be at least 80 hours of recorded transcripts and publicly available office documents such published reports in pdf or word format. After collection, the audio data will be transcribed for use in analysis.

Are there tools or software needed to create or process or visualize the data?

NVIVO software will be used

What costs, training, or resources are needed to implement this?

The primary researcher will undertake free training in NVivo.

Will pre-existing data be used and if so, from where will it be sourced?

No pre-existing data is to be used.

Where are you collecting data?

Where are you collecting data?

Either online or in person at a location of the participants choice (likely offices in Auckland, Wellington or Christchurch).

What jurisdiction requirements apply to the collection of data?

New Zealand Law (NZ Privacy Act 2020)

If you are collecting personal data from non-NZ residents are you compliant with relevant local data protection legislation?

N/A

Note: If you are collecting the personal data of European Union residents you will need to comply with the General Data Protection Regulations.

What are the data storage plans?

What are the data storage and backup strategies? What would happen if it got lost or became unusable later?

The data will primarily be held securely on a hard drive connected to the primary researcher's computer. An encrypted copy of all data will be stored separately on a separate portable hard drive to ensure if the primary copy is lost then this can be recovered. The encrypted backup copy will be updated once a week.

Will any data be stored on portable devices (e.g. audio files on a mobile phone)?

Yes, an application will be used (on iPhone) to record the interviews. This will save audio files to the device and these will then be exported via dropbox or email and saved to the primary researchers harddrive.

How will the security of any temporary storage be assured?

Using Multifactor Authentication in all storage applications. (Biometric and password protection)

Will the data be securely stored or transferred to a secure data repository?

It will be stored on the primary researcher harddrive (which is encrypted using latest encryption standards) and also to the backup external hard drive (also encrypted with up-to-date encryption standards).

What data will you keep and what data will be destroyed?

Temporary copies of any data (electronic, written) will be destroyed immediately. The primary and backup data copies will be saved for 6 years and deleted at the end of the retention period.

When and how will data be destroyed?

All data will be destroyed via wiping of the drives (electronic) and via confidential destruction bin services (written/physical)

What are the ethical requirements for your data?

How will the undertakings about consent, confidentiality, deidentification, and other ethical considerations given to participants be assured?

Consent will be formally obtained for all participants using the consent form attached to this application.

The interview information sheet and the interview protocol outline to the participant how the researcher will maintain their confidentiality and this is to be addressed before the interview formally commences.

How sensitive is your data?

There is minimal risk of sensitive data being disclosed however some information deemed commercially sensitive may be raised. This might include the current state of risk management processes within the participants business for example. This kind of information (if disclosed further) has a small risk of jeopardising the business or participants reputation.

How identifiable is your data (Will it be directly or indirectly identifiable? Will it be deidentified though potentially re-identifiable? Will it be permanently unidentifiable?) Will this alter? When?

The data may be indirectly identifiable. All attempts will be made to ensure confidentiality is maintained however as New Zealand is a small country it is possible a combination of data items may indirectly enable a reader to guess or surmise the participant or business they work for.

The primary researcher will highlight any areas of the interview transcripts that may impact confidentiality or contain sensitive data. These will be reviewed for exclusion by the participant. Any data deemed sensitive will be deleted.

What will happen to the identifiable information?

Unless express permission is gained to retain identifiable information, all data will be coded, analysed and generalised into findings.

Any data deemed identifiable or sensitive will be deleted.

Should some data be destroyed or returned? When and how? By whom?

If at any stage a participant wishes to withdraw from the study all data relating to that participant will be destroyed by the primary researcher.

What consultation has occurred around the management of your data?

With which communities or stakeholders has consultation occurred?

At this stage the data management plan has been discussed with 1 pilot interviewee.

How are any Māori data sovereignty issues being managed (please refer to https://www.temanararaunga.maori.nz)?

At this stage Māori data is not targeted for this study however should the final participant list include Māori then the principles of Rangatiratanga will be undertaken in regards to control of data, jurisdiction and self-determination.

How are the principles of whakapapa, whanaungatanga, rangatiratanga, kotahitanga, manaakitanga, and kaitiakitanga being implemented?

The researcher shall:

- Ensure free and informed consent is undertaken for any data collection and use
- Ensure data is collected with due respect and care to the individual and community
- Ensure a consultative process is undertaken throughout the research
- Ensure all data is stored securely
- Ensure the accurate collection of data and metadata

Should it be identified in the final participant list that the collection of Māori data is likely then further consultation will occur.

How is your data being organised and what documentation and metadata is being used?

What is the plan for organising, documenting, and using descriptive metadata to assure quality control and reproducibility of these data?

Standard free text descriptive metadata such as data, time, location, subject number will be recorded on the interview transcripts as per the interview guide.

What standards will be used for documentation and metadata and what version controls are in place?

Primarily version control will be used for revision of documents and data. A documented encoding system (using NVivo is yet to be produced).

How is the use of good project and data documentation formats or tools being assured and evaluated?

Review by supervision team

What folder and file naming convention will be used?

Identifying Code (text)+Date

What project and data identifiers will be assigned?

TBC

What community standards for metadata sharing or integration might be involved?

N/A

What are the plans for data sharing and access?

Have you discussed data sharing with your research collaborators or supervisor?

Yes, they are comfortable with current plans for data management

What steps will be taken to protect privacy, security, confidentiality, intellectual property or other rights?

All sources of information referred to in this research will be referenced and acknowledged appropriately using APA referencing conventions. Any supplementary documentary evidence to be used within this research will be obtained from publicly available sources such as a company or government website.

The researcher will ensure the confidentiality of the participants by reviewing transcripts for sensitive or confidential data and removing this, and coding and generalising the raw transcript data for use in analysis.

Is a data sharing agreement needed?

No

What are the access concerns associated with your data?

None

What process does someone undertake to access your data?

None

Who controls access to the data (e.g., primary researcher, student, lab, University, funder)?

Primary Researcher

What special privacy or security requirements are needed (e.g., for personal data, for high-security data)?

None

Can your data be released immediately, or should you embargo (delay access to) the data?

No embargo requirements

What embargo periods need to be upheld?

None

Have human participants been advised about the plans for sharing data in their Information Sheet?

Yes

When your research involves people, have you obtained appropriate consent for data sharing?

Yes

How will people's rights to access, correct, and remove information about themselves be managed?

Any participant may request any data held about them to be shared with them, corrected or removed. The participant will direct this request to the primary researcher who will act immediately on the request.

Does your research funder have specific data management and sharing requirements?

N/A

For how long should data be available?

6 years

If you allow others to reuse your data, how will the data be discovered and shared?

No reuse of data is allowed. Only research outputs such as the written thesis shall be shared via the AUT library.

What are the likely audiences for reused data? Who will use it now? Who will use it later?

None

When will you publish and where?

The final thesis shall be published via AUT library

What level of data access is the publisher likely to require and how will participants consent to sharing their data with publishers?

Only access to the final written document, no access is required to source data. Consent for participant data to be used in the final output is obtained up front.

What tools or software are needed to work with the data?

Standard office applications only.

What are the plans for managing any breaches of privacy or confidentiality?

What processes are in place to prevent breaches?

Encryption, Multi factor Authentication, Up to date Anti-virus Software, locked file cabinet.

Who will be responsible for notifying breaches to AUTEC and to the Privacy Commissioner when they are notifiable breaches under the Privacy Act 2020?

The Primary Researcher

What are the plans for data preservation and archiving

How will the data be archived for preservation and long-term access?

Data will not be archived or retained beyond the study (except throughout the retention period)

How long should it be retained (e.g., 6 years, 10 years, permanently) and how is this being assured?

6 years on an encrypted usb stick in the secondary supervisor's office.

What file formats are involved for electronic data? How will future accessibility be assured?

MS standard document files formats only (.doc, .docx, xls). Audio standard formats (.wav). As only standard formats are being utilised these will remain accessible throughout the retention period.

Are there existing data archives that are appropriate for your data, whether subject based, institutional, public?

No

Who will maintain the data for the long-term?

The primary researcher. The data will not be maintained beyond the initial study and retention period.

What are your main data challenges? Who can help?

What training or support do you need and what is available?

No training is required or foreseen at this stage in the process.

What University policies are relevant to your project? Have you read and understood them?

The following policies have been read and understood:

- AUT research data storage guideline
- AUT Ethics Committee guidelines and procedures

- AUT code of conduct for research

Don't forget to update your data management plan regularly:

Date for **next** review

07/06/2022