Cybersecurity and Quantum Computing:

A Quantitative Analysis Proposing a Framework for Assessing Quantum Cybersecurity Maturity

Dissertation

Submitted

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy in Quantum Computing

by

Andrew S. Vance

Capitol Technology University

Laurel, Maryland

April 2025

Abstract

Emerging technology is a key driver of the transformative changes anticipated in the 21st century, particularly within the Fourth Industrial Revolution and the expanding domain of cyber warfare. This dissertation examines the cybersecurity challenges and opportunities introduced by quantum computing, a rapidly advancing field with the potential to disrupt existing cryptographic systems. As quantum computers approach operational maturity, their ability to break classical encryption algorithms presents a significant threat to global cybersecurity. This research addresses the critical need for a structured framework to evaluate cybersecurity readiness with respect to quantum threats. Through quantitative policy analysis and a comprehensive literature review, the study explores current advancements in quantum technologies and their implications for national and organizational security. Building on these findings, this dissertation develops and proposes a novel framework to assess preparedness and guide strategic defense initiatives. The framework enables organizations and governments to identify cybersecurity vulnerabilities and adopt proactive, scalable quantum-resistant strategies. Its efficacy is demonstrated through detailed case studies of the United States, China, and Estonia, representing varying levels of technological investment and regulatory enforcement. These cases highlight disparities in quantum readiness and validate the framework's adaptability across geopolitical contexts. This research contributes a practical and scalable solution to strengthen quantum cybersecurity maturity, emphasizing the role of policy enforcement, encryption adoption, and investment alignment. This research offers a transformative tool for securing digital infrastructure in the quantum era.

Keywords: quantum computing, cybersecurity, maturity framework, post-quantum encryption, cyber risk.

Acknowledgments

My dissertation would not have been possible without the support of many people. Many sincere thanks to the faculty of Capitol Technology University, particularly Dr. Vera Dolan, whose insight and knowledge guided me through my research. Her enthusiasm for my thesis was encouraging, challenging, and corroborating of my ideas. Finally, I must thank my family for their unconditional support throughout my studies. To my kids, for being a source of inspiration and motivation to make the world safer for them, thinking of them as I wrote this thesis. And to my amazing wife for always being there for me and giving me unconditional, unequivocal, and loving support, without which I would likely have indefinitely terminated my studies a long time ago.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The Fourth Industrial Revolution (FIR), characterized by the convergence of physical, digital, and biological systems, fundamentally reshapes industries, economies, and societies (World Economic Forum, 2024). Technological advancements, such as artificial intelligence, robotics, the Internet of Things (IoT), and quantum computing, are transforming traditional practices and creating new opportunities. These practices and opportunities include the enhancement of productivity through automation and artificial intelligence, the creation of new business models powered by data and analytics, and the potential for unprecedented innovation in healthcare, manufacturing, and other industries (Moret-Bonillo, 2014). The integration of IoT and advanced robotics, for example, can lead to more innovative manufacturing processes, reducing costs and increasing efficiency. Additionally, advancements in biotechnology offer the potential for personalized medicine, where treatments are tailored to individual genetic profiles, vastly improving patient prognosis. This modern industrial revolution enables the rise of new opportunities, such as digital and emerging technologies, creating jobs, and compelling exponential growth.

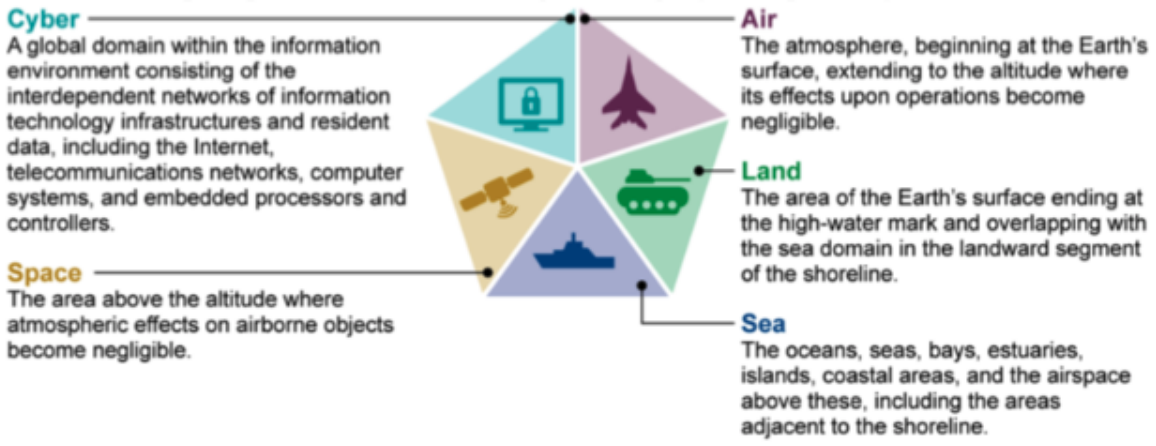
Quantum computing is the most nascent technology within FIR. It represents a significant departure from classical computing, leveraging the principles of quantum mechanics to process information in fundamentally new ways. Unlike classical computers, which use bits as the basic unit of information (represented as *0–1*), and can only exist in singular states, quantum computers utilize quantum-bits or qubits, which can exist in multiple states simultaneously due to the properties of superposition and entanglement. Superposition and entanglement allow quantum computers to perform highly complex calculations at exponentially faster rates compared to classical computers. The potential applications of quantum computing are myriad,

ranging from cryptography, which could enhance or break traditional encryption methods, accelerate testing in materials science, solve optimization problems, and expand drug discoveries (National Security Agency, 2022). As this technology advances, it poses both opportunities and significant challenges, particularly relating to cybersecurity, where current protocols may become obsolete in the face of quantum capabilities (Vance et al., 2022).

While industries and societies envision these opportunities, correlated literary analysis reveals that industry and society must ensure that the benefits and threats of these technologies are widely shared and that policies are in place to mitigate associated risks, particularly those related to cybersecurity. When technologies become more interconnected and data-driven, the attack surface for malicious actors expands, making it increasingly difficult to protect critical infrastructures, personal data, and national security (Vance, 2022). Correspondingly, the advent of the FIR has given rise to a new domain of warfare: cyber, as shown in Figure 1.

Figure 1

Department of Defense Domains of War



Note. This illustration was produced by the Government Accountability Office (GAO) for J. Kirschbaum, Director, Defense Capabilities and Management before the subcommittee on Cyber, Innovative Technologies, and Information Systems.

Unlike traditional warfare, which is waged on physical battlefields, cyber warfare operates in the digital domain, where state and non-state actors engage in activities such as espionage, sabotage, and influence operations exploiting cybersecurity vulnerabilities. The integration of advanced technologies, principally quantum computing, into this domain, is predicted to amplify the scale and impact of cyber conflicts (Congressional Research Service, 2024a). The ability of quantum computers to break the encryption algorithms that secure global communications would destabilize the digital infrastructure on which modern societies depend (National Security Agency, 2022). Current efforts to secure quantum computing primarily focus on addressing the potential risks of quantum algorithms capable of compromising classical cryptographic systems. This has accelerated research into post-quantum cryptography to develop algorithms resistant to quantum decryption to help governments and organizations mitigate the "quantum threat" (Grobman, 2020; Herman & Friedson, 2018). Quantum key distribution (QKD) has been implemented to create secure communication channels, leveraging the unique properties of quantum mechanics to detect eavesdropping attempts (Gruska, 2013). This would ensure intrusion attempts cause detectable disturbances, allowing systems to maintain security during transmission.

While these technologies and approaches provide promising solutions, research suggests that developing and deploying quantum-resistant algorithms must be further accelerated to safeguard the digital infrastructure before quantum computing becomes commercially available (Mavroeidis et al., 2018). As quantum computing evolves, a collaborative approach between cryptographers, policymakers, and industry leaders will be essential to address the risks while leveraging the opportunities (Grobman, 2020; Vance, 2024).

Statement of the Problem

The problem addressed in this study is that emerging technologies, specifically quantum computing, impose challenges on existing cybersecurity frameworks, hence the vital need to develop strategies to safeguard against quantum threats (Vance, 2024). Quantum computing introduces significant vulnerabilities in the field of cybersecurity due to its capability to undermine existing cryptographic methods, posing a critical threat to global communication and data security (Baker, 2019; Bridgewater, 2017; National Security Agency, 2022). Widely used public-key cryptosystems, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), which are essential to security, are particularly vulnerable to quantum attacks. The ability of quantum computers to break these cryptographic systems jeopardizes the confidence of communications, financial transactions, and sensitive national security information (National Security Agency, 2022). This impending threat has prompted nation-states and industries to develop quantum-resistant cryptographic algorithms and strengthen existing cybersecurity frameworks (Congressional Research Service, 2024b).

However, despite growing awareness of these risks, current cybersecurity frameworks and maturity models, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, have not evolved at the pace of quantum advancements. Originally designed to address classical computing threats, these models lack the specificity and adaptability required to respond to the distinct challenges posed by quantum algorithms like Shor's and Grover's. As a result, efforts to mitigate quantum risks have been fragmented, insufficient, and often lack coordination or comprehensive scope (Walden & Kashefi, 2019). The inadequacy of existing cybersecurity models leaves organizations and

critical systems vulnerable to quantum-based attacks. Without accounting for quantum-specific risks, organizations will be ill-prepared to defend against potential breaches, exposing them to catastrophic consequences (Soroko, 2020). This gap underscores the urgent need for a quantum-adapted model that addresses the unique challenges posed by quantum computing, ensuring robust cybersecurity preparedness at organizational and national levels.

Purpose of the Study

The purpose of this quantitative study was to design a comprehensive framework to assess and enhance cybersecurity maturity in the context of quantum computing. The resultant quantum cybersecurity maturity framework (Figure 2) was developed to serve as a critical tool for organizations and governments to evaluate their preparedness for quantum threats, identify vulnerabilities, and implement strategic improvements to strengthen cybersecurity defenses. This dissertation builds on prior research conducted in the field of quantum cybersecurity, where initial studies explored the implications of quantum technologies on existing cybersecurity frameworks. These peer-reviewed studies, conducted during my previous doctoral publication route before transitioning to a traditional dissertation program, identified critical deficiencies in existing frameworks and highlighted emerging trends in cybersecurity maturity models. Building on these foundational insights, this dissertation synthesizes the findings into a novel quantum cybersecurity maturity framework (QCMF). This framework represents a significant advancement, offering a structured and scalable approach to assessing and improving quantum cybersecurity readiness. By addressing the unique challenges posed by quantum computing, the study aimed to fill a critical gap in cybersecurity preparedness by proposing a novel methodology that integrates quantum-specific risks into a cybersecurity maturity model that leverages lessons from existing models.

This study's framework was designed to be adaptable across multiple sectors, including government, finance, healthcare, and infrastructure. Its goal is to ensure broad applicability and usability for diverse stakeholders. This framework was tested using ‘case studies’ from three countries: the United States, China, and Estonia. While this study references case studies, it is not a qualitative case study approach. Instead, the selected case study countries strictly serve as a structured framework for organizing and analyzing empirical, quantitative data on cybersecurity maturity. These nations were selected based on their varying levels of investment in quantum technologies and cybersecurity preparedness. These case studies demonstrated the framework’s adaptability to diverse geopolitical contexts and its potential to guide global efforts in mitigating quantum cybersecurity risks. This study contributes to quantum cybersecurity by introducing a practical framework for developing quantum-resilient strategies. Ultimately, this study sought to address these gaps by proposing a framework that integrated quantum-specific considerations into cybersecurity maturity models, ensuring readiness in the quantum era.

The QCMF proposed in this study is designed to address critical gaps in existing cybersecurity maturity models while ensuring alignment with quantum-specific challenges. Traditional cybersecurity frameworks rely on outdated encryption methods and lack quantum-specific metrics. The QCMF integrates quantum computing research to address this gap. By addressing vulnerabilities posed by quantum-enabled algorithms, such as Shor’s and Grover’s, the QCMF provides actionable strategies for enhancing organizational resilience. Its structure emphasizes scalability and adaptability, ensuring relevance across diverse sectors, including government, finance, healthcare, and critical infrastructure, while fostering a phased progression from awareness to proactive quantum security. This framework is positioned as a dynamic solution for organizations and nation-states to prepare effectively for the disruptive potential of

quantum technologies. As depicted in Figure 2, the framework emphasizes a structured, adaptable approach to evaluating and enhancing cybersecurity readiness at the organizational and national levels. The framework integrates foundational theories, contemporary research, and practical applications, aligning with its three evaluative dimensions: process evaluation, impact evaluation, and cost-benefit analysis. The upper part of the diagram focuses on the QCMF's overarching goals, including identifying vulnerabilities associated with quantum threats and building on the strengths of existing cybersecurity maturity models. This reflects the framework's alignment with adaptive policy principles (Purdon et al., 2001) and its emphasis on bridging the gap between classical cybersecurity paradigms and the evolving quantum landscape. For instance, integrating advancements in quantum cryptographic research ensures that the framework remains current and robust. Below the overarching goals, the framework's sectoral applicability is highlighted.

By tailoring recommendations to specific sectors, such as government, finance, healthcare, and critical infrastructure, the QCMF demonstrates its versatility and scalability. This sectoral alignment is critical for ensuring that the framework addresses the diverse challenges and resources of organizations across multiple industries, a gap often overlooked in prior models (Baseri et al., 2024). The advancement of resilient cybersecurity practices further underscores the framework's adaptive and anticipatory design. As shown in Figure 2, these practices include strengthening defenses against quantum threats, incorporating contemporary national security policies, and ensuring preparedness for quantum computing risks. This aligns directly with the evaluative dimensions of the QCMF, such as impact evaluation, which assesses the effectiveness of quantum-resistant measures in mitigating risks. The progression through the five maturity levels, from Initial Awareness to Adaptive Quantum Security, provides a structured pathway for

organizations to enhance their readiness incrementally. These maturity levels align with the process evaluation dimension of the QCMF, enabling organizations to systematically integrate quantum-resistant measures while addressing resource constraints and sector-specific challenges. For example, organizations at the *Initial Awareness* stage may focus on risk assessments and baseline quantum knowledge, while those at the *Adaptive Quantum Security* stage implement proactive monitoring and iterative policy updates. Figure 2 visually encapsulates the QCMF's design by integrating broad strategic goals, sectoral applications, and actionable steps, ensuring a clear progression from theory to practice. By incorporating the strengths of existing models and addressing identified gaps, the framework provides a comprehensive, scalable solution tailored to the quantum era.

Figure 2

Framework for Evaluating Quantum Cybersecurity Maturity

Note. The framework components all coordinate to determine the level of organizational or nation-state preparedness, from Level 1 through Level 5.

Introduction to Conceptual Framework

The conceptual framework guiding this study draws on the policy evaluation methodology outlined by Purdon et al. (2001), which emphasized assessing organizational readiness through process, impact, and cost-benefit analyses. This methodology provided a foundation for understanding how existing cybersecurity measures fall short in addressing the unique challenges of quantum computing, particularly those posed by Shor's and Grover's quantum algorithms. It also builds on insights from prior research, including my peer-reviewed publications, which identified critical gaps in existing cybersecurity maturity models and highlighted the need for quantum-specific solutions. It also integrates seminal works such as Shannon's (1948) information theory and Diffie and Hellman's (1976) contributions to public-key cryptography, which underscore the vulnerabilities of classical systems in the face of quantum-enabled threats.

By highlighting critical gaps in current cybersecurity maturity models, such as their inability to incorporate quantum-specific metrics, reliance on outdated cryptographic standards, and limited scalability, the conceptual framework guided the development of the QCMF. The QCMF builds on existing models by incorporating adaptive principles and offering a structured pathway through its five progressive maturity levels, from *Initial Awareness* to *Adaptive Quantum Security*. These levels ensure scalability and applicability across sectors, including government, finance, healthcare, and critical infrastructure, while addressing the need for sector-specific adaptability. This integration of theoretical foundations and practical considerations informed the study's research questions and objectives, ensuring the development of a robust and adaptive methodology. The resulting framework aims to enhance cybersecurity readiness in the

rapidly evolving landscape of quantum technologies by providing actionable strategies that balance innovation with familiarity, fostering broader acceptance among practitioners.

Introduction to Research Methodology and Design

This study used a quantitative research approach with structured cross-national comparisons and simulations to validate the proposed framework and assess cybersecurity maturity in the quantum era. Quantitative research is often described as a systematic and empirical approach to investigating phenomena through numerical data and statistical methods (Creswell & Creswell, 2018). This approach prioritizes breadth over depth and relies on numeric data collected through computational simulations and structured evaluations. Creswell and Creswell (2018) emphasize that quantitative research seeks to measure variables and analyze structured data through methodologies that yield replicable and generalizable results.

Rather than testing hypotheses, this study is guided by structured research questions that assess variations in cybersecurity maturity across different national contexts. The research questions drive the study's quantitative analysis, cybersecurity maturity scoring, and statistical modeling. The study uses structured numerical data, cybersecurity readiness indicators, and statistical evaluation methods to systematically compare national cybersecurity frameworks and their preparedness for quantum threats.

Quantitative research is particularly well-suited for exploring the emerging field of quantum cybersecurity, as it allows for precise measurement and statistical analysis of how organizations and governments quantify and mitigate quantum threats. This study conducts a structured cross-national cybersecurity maturity assessment, systematically evaluating variations in cybersecurity policies and preparedness using empirical data and statistical comparisons.

Although this study references comparative analysis concepts from Yin (2014) and Ragin (1987), it does not employ a qualitative case study approach. Instead, the selected nations serve as structured units of analysis within a quantitative cybersecurity maturity evaluation. Yin's (2014) work provides foundational insights into structured comparisons, which are adapted here using statistical modeling rather than thematic or narrative case study methods. Similarly, Ragin's (1987) comparative methodology informs the structured selection of nations for cybersecurity assessment; however, this study applies numerical scoring models and statistical comparisons rather than qualitative comparative analysis (QCA). By using structured cybersecurity maturity scoring, policy data, and simulation-based evaluation, this research maintains a strictly quantitative approach while benefiting from structured comparative frameworks used in broader social science research.

The study leverages structured national cybersecurity assessments to explore variations in cybersecurity preparedness for quantum threats across different nations. Rather than qualitative case study research, this study uses statistical modeling, numerical policy assessment, and cybersecurity maturity scoring. Research was collected through an extensive review of policy documentation, quantitative policy analysis, and structured statistical modeling. The research design integrated three key phases: data collection, structured cybersecurity maturity analysis, and statistical synthesis. Using a comparative analysis of cybersecurity maturity models, the study identified gaps and proposed a structured cybersecurity maturity framework. Validation of the quantitative research through simulation models demonstrated the practical utility of the framework. This design ensured the study comprehensively addressed the unique risks posed by quantum technologies and provided actionable, data-driven insights for improving cybersecurity readiness.

Research Questions

The research questions in this dissertation were designed to guide the exploration of how organizations and nation-states can assess and improve cybersecurity maturity in preparation for quantum computing threats. Aligned with the study's quantitative methodology and the proposed QCMF, these questions were devised to address critical gaps in existing maturity models. Each question reflects a facet of the overarching problem, focusing on the development of actionable strategies to enhance preparedness and resilience against quantum-enabled risks. Through this structured inquiry, the study sought to contribute significantly to both the academic and practical understanding of quantum cybersecurity readiness. These research questions guided the exploration of framework development, identification of deficiencies in current practices, and evaluation of the framework's real-world applicability across diverse geopolitical and technological contexts.

RQ_1

How can a quantum cybersecurity maturity framework be developed, incorporating specific criteria and metrics to evaluate and enhance preparedness for quantum-enabled cybersecurity threats?

RQ_2

What are the critical deficiencies in existing cybersecurity maturity models, and how do these limitations impact the ability of organizations and nation-states to address quantum-related threats?

RQ_3

How do variations in national cybersecurity policies impact quantum cybersecurity maturity and readiness across different maturity levels?

Significance of the Study

This study is significant for its potential to reshape how organizations and governments prepare for the quantum era. By proposing a tailored framework that addresses the specific challenges posed by quantum computing, the research provides actionable solutions to enhance cybersecurity maturity. Practically, the framework equips practitioners with tools to identify vulnerabilities, implement quantum-resistant measures, and safeguard critical infrastructure against emerging threats. The framework also provides a structured methodology for assessing and mitigating quantum-specific risks, offering a scalable approach that can be adapted to diverse organizational and national contexts. Theoretically, the study contributes to academic discourse by extending existing cybersecurity maturity models to address quantum-specific risks.

It integrates principles of adaptive policy-making and quantitative evaluation, filling critical gaps in the literature where current frameworks fail to account for the unique vulnerabilities introduced by quantum technologies. By bridging these theoretical and practical domains, the research not only advances the field of quantum cybersecurity but also establishes a foundation for future interdisciplinary studies and global policy innovation.

Globally, this study advocates for collaborative policy making and international cooperation and alignment to ensure that all nations have access to effective quantum-resistant policies and strategies (Vance et al., 2020). The findings underscored the urgent need to advance quantum-resilient cryptographic standards, strengthen international agreements, and secure global digital infrastructures against the imminent quantum threat. By addressing these critical challenges, the study not only deepens academic discourse but also provides actionable recommendations to inform global policy and organizational strategies, ensuring preparedness for emerging quantum cybersecurity risks.

Definition of Key Terms

This section provides definitions for key terms used throughout the study to ensure clarity and facilitate a deeper understanding of the concepts discussed. Terms are cited and defined in accordance with current industry standards and recent research, supporting a consistent interpretation of critical concepts across the study's analysis and findings.

Binary Digit (Bit)

A Binary Digit (Bit) is the fundamental unit of classical computing represented as either a 0 or a 1. The concept of a bit is rooted in binary logic, which operates on two discrete states, corresponding to "off" (0) and "on" (1) in computing systems (Rieffel & Polak, 2019).

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a cryptographic technique that uses the mathematical properties of elliptic curves to secure communications. ECC provides the same level of security as Rivest-Shamir-Adleman, but with shorter key lengths, making it more efficient (NIST, 2024).

Entanglement

Entanglement is a quantum phenomenon where two or more particles become interdependent, connoting that the state of one particle directly affects the other, regardless of the distance between them. Entanglement is crucial in quantum communication and computing (NIST, 2024).

Grover's Algorithm

Grover's Algorithm is a quantum algorithm that achieves quadratic speedup in searching unsorted databases compared to classical algorithms, demonstrating the potential computational power of quantum systems (Rieffel & Polak, 2019).

Harvesting Attacks

Harvesting attacks, a quantum-specific threat, involve adversaries collecting and storing encrypted data with the intent to decrypt it later using quantum computers once they achieve sufficient computational power (Grobman, 2020).

Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) is a cryptographic algorithm that is secure against attacks by quantum computers. The National Institute of Standards and Technology (NIST) is leading efforts to standardize these algorithms to protect against future quantum-enabled breaches (NIST, 2024).

RSA Rivest-Shamir-Adleman (RSA)

Rivest-Shamir-Adleman (RSA) is a widely used public-key cryptosystem that relies on the difficulty of factoring large integers. It is vulnerable to attacks by quantum computers through Shor's algorithm, necessitating the adoption of quantum-resistant alternatives (NIST, 2024).

Shor's Algorithm

Shor's Algorithm is a quantum algorithm that efficiently factors large integers, threatening RSA encryption and other widely used cryptographic systems. It underscores the urgency of developing post-quantum cryptography (NIST, 2024).

Simulation Modeling

Simulation modeling aligns with Quantitative methodologies that emphasize understanding complex systems through scenario-based modeling and interpretative analysis rather than quantitative outputs (Zyoud et al., 2024).

Superposition

Superposition is a fundamental quantum principle where particles can exist in multiple states simultaneously until observed. This property allows quantum computers to perform multiple calculations in parallel (Rieffel & Polak, 2019).

Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis

Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis is a strategic planning tool used to assess an organization's internal strengths and weaknesses alongside external opportunities and threats. The SWOT analysis helps align resources with objectives and identify risks to mitigate. It is widely applied across industries, including cybersecurity strategy (Möller, 2023).

Quantum Computing

Quantum computing is a computing paradigm that leverages quantum mechanics, such as superposition and entanglement, to perform operations at scales unattainable by classical computers. It introduces both opportunities and challenges for modern cybersecurity (NIST, 2024).

Quantum Cybersecurity Maturity

Quantum Cybersecurity Maturity is the level of readiness a nation or organization has achieved to address quantum-related threats. This includes adopting quantum-resistant technologies, integrating policies, and ensuring workforce preparedness (NIST, 2024).

Quantum-Resistant

Quantum-Resistant refers to cryptographic technologies designed to remain secure against both classical and quantum computers. These technologies are essential to future-proof cybersecurity systems (NIST, 2024).

Quantum Bit (Qubit)

A Quantum Bit (Qubit) is a quantum information unit that can represent both 0 and 1 simultaneously due to the principle of superposition. Due to this property, qubits enable quantum computers to solve complex problems much faster than classical systems (Rieffel & Polak, 2019).

Summary

This chapter introduced the study's focus on quantum cybersecurity maturity and the challenges posed by quantum computing within the FIR. The problem addressed is that emerging technologies, specifically quantum computing, impose challenges on existing cybersecurity frameworks, necessitating the development of strategies to safeguard against quantum threats. The purpose of this study will be discussed in the next chapter, which expands on the need for a structured cybersecurity maturity framework. The study is significant because it highlights critical gaps in existing cybersecurity maturity models and their implications for quantum security. Findings contribute to both academic research and practical cybersecurity applications by addressing deficiencies in current frameworks, strengthening policy recommendations, and informing global cybersecurity strategies. The next chapter presents a review of existing literature, analyzing prior research on cybersecurity maturity models and quantum security challenges to establish the foundation for the study.

Chapter 2: Literature Review

The purpose of this study was to develop a maturity model for effectively evaluating cybersecurity in quantum computing, enabling organizations and nation-states to prepare for the threats posed by this emerging technology. The literature review intended to identify gaps in existing cybersecurity maturity models and explore how these models could evolve or be replaced to address the specific challenges posed by quantum computing. To achieve this, the review focused on three core areas: the intersection of quantum computing and cybersecurity, the strengths and limitations of existing cybersecurity maturity frameworks, and the critical gaps that necessitate a quantum-specific solution.

To ensure a comprehensive and rigorous review, a systematic approach was employed to identify and evaluate sources. This process involved analyzing over 148 scholarly articles and 327 policy documents sourced from leading academic and professional databases, including Google Scholar, IEEE Xplore, Scopus, Web of Science, ACM Digital Library, ScienceDirect, arXiv.org, and the Directory of Open Access Journals. Search queries began with singular terms such as "cybersecurity maturity models," "quantum computing risks," and "national security," and were progressively refined to include combinations of these terms alongside seminal concepts like "adaptive frameworks" and "cryptographic evolution." This systematic approach ensured the inclusion of both seminal and contemporary literature, capturing the evolution of thought in cybersecurity maturity. To maintain objectivity and rigor, only credible sources such as peer-reviewed academic journals, government policies, and industry-neutral research papers were considered. Studies from predatory publishers, commercially funded white papers, and ad-sponsored publications were excluded. The literature review encompassed research and best

practices published between 1999 and 2024, focusing on cybersecurity maturity and quantum computing.

Insights resulting from this literature review highlight the transformative impact of quantum computing on cybersecurity and underscore the limitations of existing frameworks in addressing quantum-specific challenges. The deficiencies identified in existing cybersecurity maturity models underscore the need for an adaptive and scalable security framework that addresses quantum-specific challenges. While prior research has explored incremental updates to cybersecurity maturity models, existing solutions remain insufficient in mitigating post-quantum cryptographic threats. The following section introduces the QCMF, integrating insights from contemporary research and adaptive policy models to bridge the gaps identified in the literature.

Conceptual Framework

The QCMF proposed in this study integrates foundational theories (Diffie & Hellman, 1976; Shannon, 1948), contemporary research (Mavroeidis et al., 2018; NIST, 2024), and insights from prior publications (Vance, 2022, 2024) to address the unique challenges posed by quantum computing in cybersecurity. Grounded in well-established principles, this framework provides a structured approach to evaluating and enhancing cybersecurity maturity in preparation for quantum-enabled threats. The framework draws on seminal works, including Purdon et al.'s (2001) Adaptive Policy Framework, which informs adaptive cybersecurity strategies, and foundational cryptographic theories, such as Shannon’s (1948) Information Theory and Diffie and Hellman’s (1976) work on public-key cryptography. Additionally, this study builds on prior research that identified critical gaps in cybersecurity maturity models (Baseri et al., 2024; Grindstaff II et al., 2019; Mullapidi et al., 2023; Vance, 2022, 2024; Wallace et al., 2023),

integrating insights from contemporary cybersecurity frameworks to address the evolving threats posed by quantum computing.

Shannon's information theory laid the groundwork for understanding vulnerabilities in communication systems, particularly in the context of adversarial attacks. Shannon's principles of entropy and secure transmission were pivotal in shaping modern cryptographic systems, emphasizing resilience against sophisticated attacks. This influence is reflected in the QCMF's prioritization of quantum-resistant cryptographic solutions, designed to counter the unique computational capabilities of quantum systems. Similarly, Diffie and Hellman's (1976) contributions to public-key cryptography revolutionized secure communications by introducing key exchange mechanisms that underpin today's encryption standards. However, these methods are increasingly vulnerable to quantum-enabled algorithms like Shor's, which can efficiently factorize large integers. Recognizing this vulnerability, the QCMF integrates quantum-resistant measures to protect cryptographic infrastructures against quantum-specific threats.

The adaptive policy framework outlined by Purdon et al. (2001) provided methodological guidance for the QCMF by emphasizing iterative, anticipatory, and collaborative mechanisms. These principles align closely with the need for frameworks that evolve alongside technological advancements, enabling organizations to adapt to emerging risks. The QCMF employs these adaptive principles in its design, particularly in its progressive maturity levels, which provide a scalable pathway for organizations to enhance their cybersecurity readiness incrementally.

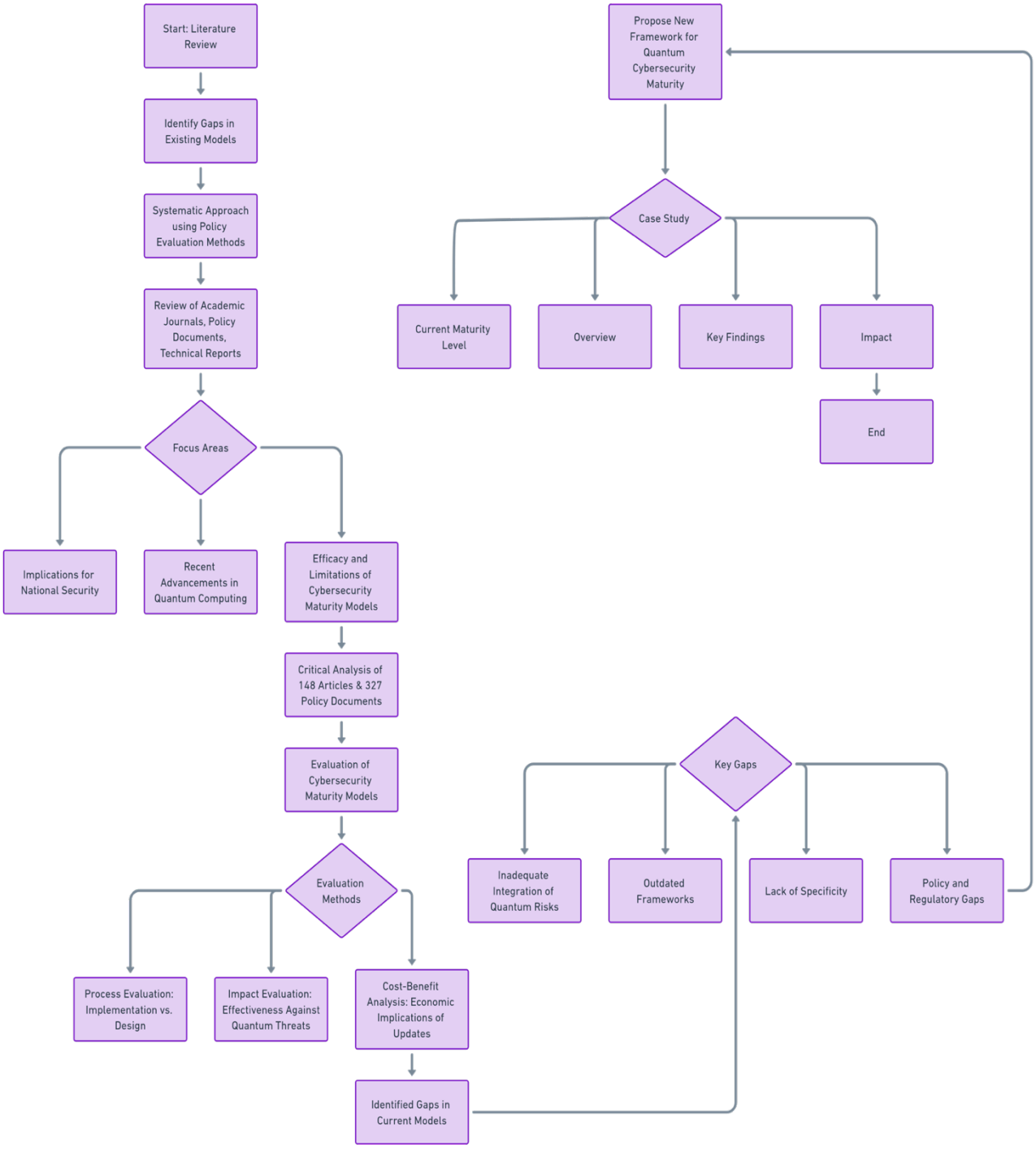
Prior publications (Vance, 2022, 2024) serve as seminal contributions to this study. These works identified critical deficiencies in existing cybersecurity maturity frameworks, including the absence of quantum-specific metrics, reliance on outdated cryptographic standards, and insufficient scalability for resource-constrained organizations. By proposing the need for a

tailored solution to quantum-specific risks, these studies bridged gaps in classical cybersecurity paradigms and the evolving quantum threat landscape. The insights gained directly informed the development of the QCMF, offering a structured approach to addressing gaps and providing actionable strategies for enhancing cybersecurity readiness in the quantum era.

The QCMF employs three evaluative dimensions, process evaluation, impact evaluation, and cost-benefit analysis, to systematically assess cybersecurity maturity and ensure structured improvements. Purdon et al. (2001) introduced a policy evaluation methodology that emphasizes these dimensions as essential tools for assessing organizational readiness and adaptability to emerging risks. These dimensions provide a comprehensive methodology for measuring the effectiveness, practicality, and economic feasibility of cybersecurity models, aligning with research findings on cybersecurity assessment frameworks. Process evaluation focuses on identifying discrepancies between policy design and real-world implementation, particularly in adapting to quantum-specific risks. For instance, evaluating the integration of post-quantum cryptographic measures into national infrastructures illustrates the practical application of this dimension. Impact evaluation examines the effectiveness of existing frameworks in mitigating quantum-specific vulnerabilities, such as those posed by traditional encryption systems under quantum attack. The cost-benefit analysis evaluates the economic implications of adopting quantum-resistant solutions, emphasizing trade-offs such as resource allocation, policy incentives, and strategic priorities. Together, these dimensions ensure that the QCMF provides actionable insights while aligning with the study's research objectives. Figure 3 visually represents the relationships between these evaluative dimensions, key gaps in existing cybersecurity maturity models, and the proposed QCMF methodology.

Figure 3

Conceptual Framework and Methodology Development



Note: This diagram represents the development and validation of the conceptual framework, informed by the literature review, case studies, and gap analysis.

Fundamental to the QCMF's design are its five progressive maturity levels, which provide a structured pathway for organizations to achieve adaptive quantum security. The first level, *Initial Awareness*, focuses on recognizing quantum risks and conducting baseline risk assessments. At the *Basic Preparation* level, organizations begin adopting quantum-resistant measures, such as testing post-quantum cryptographic protocols. *Intermediate Implementation* involves deploying quantum-resistant technologies across critical systems and conducting regular risk assessments. *Advanced Integration* represents a comprehensive approach, embedding quantum-aware measures into organizational policies and practices while emphasizing interdepartmental coordination. The *Adaptive Quantum Security* level embodies a proactive stance, characterized by continuous monitoring, rapid response to emerging threats, and iterative refinement of cybersecurity strategies. These maturity levels ensure that the framework is both scalable and adaptable, addressing the critical gaps identified in the literature and enabling organizations to systematically enhance their cybersecurity readiness.

The practical applicability of the QCMF is further demonstrated through comparative case studies of the United States, China, and Estonia. These nations were selected to represent diverse geopolitical contexts and varying levels of readiness for quantum cybersecurity. The United States, for example, exemplifies advanced integration of quantum-resistant technologies, driven by robust national initiatives and private-sector collaboration. In contrast, Estonia highlights the challenges faced by smaller nations, emphasizing the importance of early adoption and innovation in digital infrastructure to mitigate quantum-specific threats. China's approach, characterized by significant investments in offensive quantum capabilities, underscores the importance of balancing offensive strategies with robust defensive measures. These case studies

validate the QCMF's scalability and adaptability, illustrating its relevance across different organizational and national contexts.

By integrating insights from seminal works, contemporary research, and empirical quantitative evidence, the proposed QCMF represents a significant advancement in cybersecurity maturity modeling. Its design offers a scalable, actionable framework for organizations and governments to address the challenges posed by quantum computing and secure their systems in the quantum era. The framework emphasizes phased implementation and adaptability, enabling stakeholders to prioritize critical actions while scaling their efforts to align with evolving quantum threats.

History of Cybersecurity

The evolution of cybersecurity is closely aligned with advancements in technology, as each technological development brings new vulnerabilities and challenges. Early efforts in cybersecurity began in the mid-20th century, focusing on protecting standalone systems and securing communications through cryptographic methods, such as Shannon's (1948) foundational theories on information randomness. Shannon's work provided the mathematical basis for secure communication, emphasizing the importance of protecting data against adversarial interception. However, as interconnected networks like Advanced Research Projects Agency Network (ARPANET) emerged, cybersecurity efforts shifted to protecting data in transit and addressing vulnerabilities inherent in networked systems (Khan & Torre, 2021).

The 1990s was another era of significant technological advancement with the widespread adoption of the internet and the introduction of public-key cryptography by Diffie and Hellman (1976). This key exchange algorithm provided a scalable solution for encrypting data across distributed systems, laying the groundwork for modern cybersecurity frameworks. Frameworks

like the NIST Cybersecurity Framework were developed to address classical computing threats. However, the exponential growth of digital technologies in the 21st century, such as artificial intelligence (AI), the Internet of Things (IoT), and quantum computing, introduced complexities that traditional frameworks struggle to manage effectively.

Delays in adapting existing frameworks to emerging technological threats have historically led to significant exploits. For instance, the 2017 WannaCry ransomware attack exploited unpatched vulnerabilities in the Microsoft Windows operating system, affecting hundreds of thousands of systems worldwide and highlighting how outdated cybersecurity frameworks failed to address rapidly evolving malware (Baker & Youssef, 2019). Similarly, the Target data breach in 2013 exposed weaknesses in vendor management, where attackers exploited third-party vulnerabilities to access customer payment data, underscoring the inadequacy of traditional frameworks in managing supply chain risks (NIST, 2024). The 2020 SolarWinds attack further illustrated how frameworks designed for classical threat landscapes were insufficient to address sophisticated state-sponsored attacks, as adversaries compromised trusted software updates to infiltrate numerous organizations (Lewis, 2018).

These examples emphasize the consequences of delayed development in cybersecurity frameworks and highlight the urgency of aligning them with emerging threats. Quantum computing's ability to compromise widely used cryptographic systems like RSA and ECC by quantum algorithms like Shor's and Grover's represents a critical risk to global communication and data security (Vance, 2024). This urgency necessitates that frameworks incorporate adaptive and anticipatory mechanisms to prepare for quantum threats (Vance, 2022). However, current efforts to integrate quantum-specific measures remain principally focused on cryptographic advancements, leaving broader cybersecurity strategies underdeveloped.

The proposed QCMF addresses these gaps by integrating historical insights with modern research, emphasizing the importance of iterative policy evaluations and quantum-specific defensive strategies. By analyzing and addressing the deficiencies of previous frameworks in adapting to emerging threats, this approach strengthens resilience against both current and future challenges, safeguarding organizational and national security in the quantum era. This historical evolution highlights the need for continuous and accelerated innovation in cybersecurity strategies. The transition from classical to quantum cybersecurity marks a critical stage, necessitating the development of frameworks that are resilient, adaptive, and capable of addressing the unique challenges posed by quantum technologies. These insights align with prior research (Vance, 2022, 2024), which called for comprehensive frameworks that integrate quantum-specific metrics and scalability, bridging the gap between traditional approaches and future demands.

Quantum Cybersecurity Gaps

The innovation of technology from classical to quantum computing has exposed critical vulnerabilities in existing cybersecurity maturity models. Current frameworks, including the NIST Cybersecurity Framework and ISO/IEC 27001, were conceptualized to address conventional threats and lack explicit mechanisms for mitigating quantum-related risks (Soroko, 2020). These limitations have created a growing discrepancy between cybersecurity preparedness and the risk of post-quantum security threats.

Many cybersecurity models rely on static threat assumptions, failing to incorporate the dynamic risk landscape posed by quantum computing, particularly in areas such as cryptographic resilience, risk assessment methodologies, and policy enforcement (Schwab, 2016). As quantum technologies advance, these shortcomings necessitate a critical reassessment of cybersecurity

maturity models to ensure they remain viable in protecting sensitive information, national security infrastructures, and global digital ecosystems.

A systematic review of cybersecurity literature reveals multiple fundamental deficiencies in existing cybersecurity maturity models that must be addressed to ensure quantum resilience. These identified gaps necessitate an urgent reassessment of cybersecurity maturity models to accommodate the evolving threat landscape introduced by quantum computing. The following sub-sections provide an in-depth analysis of each identified gap, examining their implications within the existing literature and highlighting the structural deficiencies that must be addressed to ensure the long-term viability of cybersecurity maturity frameworks in the quantum era.

Lack of Quantum-Specific Risk Assessment Frameworks

The absence of standardized maturity indicators for evaluating an organization's preparedness for quantum-resistant cybersecurity presents a significant obstacle to benchmarking and policy enforcement. Existing cybersecurity maturity models primarily employ compliance-based assessments, which rely on qualitative security audits rather than quantifiable cybersecurity performance metrics (Schwab, 2016). These qualitative evaluations, while effective in classical security models, do not provide the necessary precision for assessing an organization’s progression toward quantum security readiness. The literature highlights that without structured cybersecurity maturity indicators, organizations struggle to assess the effectiveness of their quantum-resistant security measures (Vance, 2022). This deficiency leads to inconsistencies in the assessment process, creating uncertainty in determining whether an organization has effectively transitioned toward post-quantum cybersecurity maturity (Baseri et al., 2024).

A major deficiency in current cybersecurity risk assessment frameworks is the lack of numerical risk exposure metrics tailored to quantum cryptographic vulnerabilities. In classical cybersecurity risk models, organizations measure security posture through quantitative key performance indicators (KPIs) such as intrusion detection response times, encryption key strengths, and vulnerability patching cycles (Congressional Research Service, 2024b). However, these traditional assessment methodologies do not extend to quantum risk quantification, leading to uncertainties in cybersecurity maturity evaluations. Organizations are therefore unable to measure their susceptibility to quantum-enabled decryption attacks, nor can they determine whether their cybersecurity posture is sufficiently progressing toward quantum resilience (Baseri et al., 2024).

Another critical gap in cybersecurity maturity models is the absence of probability-driven threat modeling for quantum vulnerabilities. While classical cybersecurity models incorporate risk-weighted assessments for known attack vectors, they often fail to include probability-driven risk scoring for quantum threats. For example, the NIST Cybersecurity Framework (NIST, 2024) and the Capability Maturity Model Integration (CMMI) (Paulk et al., 1993) focus primarily on compliance-based security assessments, which lack quantitative threat modeling mechanisms specific to probabilistic quantum attacks.

These models emphasize structured cybersecurity process development but do not integrate quantitative risk probability calculations, leaving organizations unable to forecast the likelihood of post-quantum cryptographic failure based on evolving quantum computational power. As quantum threats advance, the absence of probability-based risk modeling within these frameworks limits their ability to provide actionable cybersecurity readiness benchmarks for quantum resilience. Studies indicate that quantum computing introduces a probabilistic element

to cryptographic risk, where an attacker's likelihood of success increases exponentially as quantum computational power advances (Walden & Kashefi, 2019).

Most existing cybersecurity maturity models continue to rely on qualitative self-assessments and subjective expert evaluations, rather than empirical data-driven threat modeling techniques. This reliance on subjective methodologies results in delayed responses to emerging threats, as organizations lack predictive analytics to assess risk escalation as quantum technology progresses. The literature further emphasizes that cybersecurity maturity models must evolve to account for quantum cryptographic adoption rates as an essential cybersecurity maturity indicator (Baseri et al., 2024).

Inadequate Integration of Quantum Risks in Existing Models

The predominant cybersecurity frameworks, including the NIST Cybersecurity Framework (NIST, 2024), CMMI (Paulk et al., 1993), and ISO/IEC 27001 (2023), remain oriented toward classical computing threats and fail to incorporate emerging cryptographic vulnerabilities associated with quantum technologies. Despite advancements in cybersecurity methodologies, these frameworks were designed primarily for classical security environments and lack quantum-specific risk assessments. They emphasize structured cybersecurity maturity processes, such as risk management frameworks, vulnerability assessment methodologies, and incident response protocols, alongside compliance-based security protocols like ISO/IEC 27001 (2023) certification requirements and NIST 800-53 security controls. However, these frameworks do not integrate probability-driven threat modeling, leaving organizations unprepared for post-quantum cryptographic risks (Soroko, 2020).

One of the most noteworthy deficiencies in existing cybersecurity maturity models is the absence of structured post-quantum cryptographic transition planning. Research reveals that even

modern cybersecurity infrastructures continue to rely on RSA, ECC, and other classical encryption standards, despite their known vulnerabilities to quantum decryption (Baseri et al., 2024). The National Security Agency (NSA) (2022) study warns that quantum computing will make classical encryption obsolete, necessitating a structured and immediate transition to post-quantum cryptographic (PQC) protocols to prevent large-scale breaches of encrypted data. The NSA further highlights that industries reliant on long-term encryption security, such as defense, finance, and healthcare, must prioritize quantum-secure cryptographic adoption to avoid a cryptographic crisis (National Security Agency, 2022). However, the literature indicates that no standardized quantum security roadmap currently exists, leaving cybersecurity maturity models without clear guidelines for PQC integration, which delays implementation and weakens security resilience (Vance, 2022).

Another critical deficiency in cybersecurity maturity models is the absence of probability-driven threat modeling for quantum vulnerabilities. While classical cybersecurity models incorporate risk-weighted assessments for known attack vectors, they often fail to include probability-driven risk scoring for quantum threats. Studies indicate that quantum computing introduces a probabilistic element to cryptographic risk, where an attacker's likelihood of success increases exponentially as quantum computational power advances (Walden & Kashefi, 2019).

Despite evidence of maturity models needing a probabilistic element, existing cybersecurity maturity models continue to rely on qualitative self-assessments and subjective expert evaluations, rather than empirical data-driven threat modeling techniques. Without integrating quantum-specific probabilistic risk forecasting, organizations lack predictive

analytics to assess risk escalation, which delays mitigation efforts and leaves systems vulnerable to evolving quantum threats.

Existing cybersecurity strategies fail to address the computational asymmetry introduced by quantum computing, wherein adversaries can achieve exponential speedups in decryption without a corresponding increase in defensive capabilities (NIST, 2024). Unlike conventional cyberattacks, quantum-enabled attacks bypass classical cryptographic resilience measures, requiring entirely new security architectures rather than incremental cryptographic updates. However, cybersecurity maturity models do not reflect this shift in attack complexity, leaving organizations dependent on outdated security assumptions.

Lack of Quantum-Specific Metrics in Cybersecurity Models

The absence of standardized maturity indicators for evaluating an organization's preparedness for quantum-resistant cybersecurity presents a significant obstacle to benchmarking and policy enforcement. Studies indicate that cybersecurity maturity models, including the CMMI (Paulk et al., 1993), NIST Cybersecurity Framework (NIST, 2024), and ISO/IEC 27001 (2023), focus primarily on classical security risks and lack structured methodologies for assessing quantum-specific vulnerabilities. Research by Baseri et al. (2024) and Wallace et al. (2023) highlights that current cybersecurity models fail to define key benchmarks for evaluating an organization’s transition to post-quantum cryptographic readiness, leaving security assessments highly subjective. Cybersecurity maturity models traditionally employ compliance-based assessments, relying on qualitative security audits rather than quantifiable cybersecurity performance metrics (Schwab, 2016). However, in the context of quantum security, a lack of structured cybersecurity maturity indicators inhibits organizations from measuring their progress toward implementing post-quantum defenses (Vance, 2022).

One of the core issues in the literature is that cybersecurity models lack numerical risk exposure metrics for quantum cryptographic vulnerabilities. Without measurable benchmarks, organizations struggle to determine their susceptibility to quantum-enabled decryption attacks and whether they are progressing toward quantum-resistant cybersecurity maturity (Congressional Research Service, 2024b). Additionally, threat modeling frameworks often fail to incorporate probability-driven risk scoring, leaving cybersecurity maturity assessments dependent on qualitative self-assessments rather than empirical threat modeling techniques.

Another limitation in cybersecurity maturity modeling is the failure to account for quantum cryptographic adoption rates as a cybersecurity maturity indicator. Unlike classical cybersecurity models, which use firewall implementation rates or access control policies as metrics of security maturity, quantum cybersecurity maturity requires the evaluation of adoption speed, implementation success, and post-quantum cryptographic readiness across different sectors (Baseri et al., 2024). The literature suggests that cybersecurity maturity models must incorporate a structured, quantifiable scoring methodology to track an organization's transition to quantum-resistant security measures.

Regulatory and Policy Gaps in Quantum Cybersecurity

Research indicates that the absence of cohesive international policies addressing quantum cybersecurity has resulted in fragmented regulatory landscapes, impeding the development and adoption of uniform cybersecurity standards. Unlike classical cybersecurity, which benefits from decades of structured policy coordination, quantum cybersecurity lacks a globally recognized roadmap for ensuring standardized cryptographic security measures (Congressional Research Service, 2024b).

One example of regulatory fragmentation is the disparity in national quantum security strategies between leading technological nations. The United States and China have established independent quantum research programs, each prioritizing national security interests over international cooperation (Vance, 2022). In the United States, NIST has spearheaded post-quantum cryptographic standardization, yet no legally binding federal mandate enforces its adoption across industries. In contrast, China's quantum initiatives focus on state-controlled quantum advancements, restricting global knowledge-sharing on quantum-resistant security protocols, thereby limiting cross-border regulatory consistency (Congressional Research Service, 2024a).

Another example is the lack of a global enforcement mechanism to ensure post-quantum cryptographic compliance. While international organizations such as the European Union Agency for Cybersecurity (ENISA) and the ISO have recommended guidelines, no binding cybersecurity treaties mandate the uniform adoption of post-quantum cryptographic measures (Lourenco, 2023). This lack of harmonization has resulted in regional discrepancies in quantum cybersecurity enforcement, creating vulnerabilities for cross-border data transmission and international supply chains (ISO/IEC 27001, 2023; NIST, 2024).

Nation-states and organizations operate under varied and often conflicting compliance requirements, delaying the widespread adoption of quantum-resistant security strategies (Vance, 2022). Cybersecurity regulations remain disparate across geopolitical regions, with some nations implementing preliminary quantum security measures while others lack any formal legislative guidance for transitioning to post-quantum cryptographic protocols. These gaps in enforcement create significant security risks, as organizations operating in jurisdictions without mandated quantum cybersecurity measures may fail to take proactive steps toward securing sensitive data

from future quantum-enabled cyber threats. The literature suggests that until a unified international regulatory framework emerges, cybersecurity maturity models will continue to lack structured policy enforcement mechanisms, resulting in delayed post-quantum cryptographic transitions and increased cyber risk exposure across industries and nations. Smaller nations such as Estonia face significant policy gaps due to the absence of enforceable global cybersecurity regulations. Without an internationally recognized policy structure, smaller nations remain vulnerable to delayed cybersecurity readiness while larger nations dictate quantum security standards without global alignment (Congressional Research Service, 2024a).

While classical cybersecurity frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 have evolved, quantum cybersecurity has not, with no universally recognized policy enforcement mechanisms governing the implementation of post-quantum cryptographic compliance measures (Congressional Research Service, 2024b). Existing cybersecurity compliance frameworks such as NIST and ISO do not include explicit provisions for ensuring compliance with quantum-resistant encryption technologies, leaving a regulatory gap that creates long-term vulnerabilities for industries reliant on strong encryption protocols (Baseri et al., 2024).

Fragmented Global Collaboration in Quantum Cybersecurity

The absence of internationally standardized cybersecurity protocols has led to disparate national strategies, thereby exacerbating inconsistencies in cybersecurity maturity and resilience. Unlike traditional cybersecurity threat intelligence sharing, which operates through global cybersecurity partnerships, quantum security remains highly fragmented (Walden & Kashefi, 2019). This fragmentation is largely attributed to the lack of unified guidelines for post-quantum

cryptographic implementation, nation-specific cybersecurity policies, and differences in technological priorities across geopolitical regions.

The literature emphasizes that while existing global cybersecurity initiatives, such as the Budapest Convention on Cybercrime and the United Nations Group of Governmental Experts on Information Security (UNGGE), have facilitated cooperation in areas like cybercrime and data protection, they do not extend to quantum cybersecurity governance (Congressional Research Service, 2024a). This lack of coordination has resulted in significant gaps in knowledge-sharing and interoperability among international cybersecurity stakeholders. As a result, countries have independently formulated quantum cybersecurity strategies without a common framework for benchmarking, incident response, or quantum-resilient infrastructure development.

Geopolitical tensions further complicate quantum security collaboration, as nations such as the United States and China continue to invest heavily in offensive quantum computing applications, limiting international cooperation on defensive cybersecurity strategies (Congressional Research Service, 2024a). The competitive nature of national quantum research programs has fueled technological secrecy and reluctance to engage in bilateral or multilateral cybersecurity partnerships. Additionally, countries with advanced quantum capabilities have been reluctant to share post-quantum cryptographic advancements due to concerns over national security vulnerabilities. This lack of open collaboration further limits the ability of global cybersecurity institutions to establish coherent, evidence-based policies that effectively address quantum cybersecurity threats on a global scale. Another key challenge identified in the literature is the uneven distribution of quantum computing resources, which has widened the cybersecurity gap between technologically advanced nations and those with limited quantum research capabilities. Developing nations face significant challenges in keeping pace with quantum

security advancements, leading to asymmetries in cybersecurity maturity levels that leave less technologically developed countries disproportionately vulnerable to emerging quantum threats. Without structured frameworks for international cybersecurity cooperation, these disparities will continue to hinder the development of comprehensive cybersecurity strategies that are effective across all geopolitical and economic contexts (Walden & Kashefi, 2019).

Researchers have argued that cybersecurity maturity models must incorporate structured mechanisms for cross-border collaboration, cybersecurity knowledge-sharing, and regulatory alignment to mitigate inconsistencies in global cybersecurity preparedness. For example, ENISA facilitates cross-border cooperation through the Network and Information Systems (NIS) Directive, requiring European Union (EU) member states to adopt harmonized cybersecurity risk management practices (NIST, 2024). The literature suggests that while nation-states will inevitably pursue independent quantum cybersecurity strategies, establishing a set of international cybersecurity governance principles is essential for ensuring standardized, scalable, and universally applicable security measures. These principles would facilitate cross-sector partnerships, enable information-sharing among global cybersecurity research institutions, and promote harmonized cybersecurity maturity models that reflect the realities of post-quantum security risks.

Economic Barriers to Quantum Cybersecurity Adoption

Unlike conventional cybersecurity investments, which often follow incremental security updates, quantum security requires full-scale cryptographic migration, leading to high upfront costs (Baseri et al., 2024). The adoption of post-quantum cryptographic algorithms necessitates substantial financial and infrastructural investments, including the replacement of existing cryptographic systems, reconfiguration of security protocols, and workforce retraining to manage

new security measures. These requirements present significant challenges, particularly for small and mid-sized enterprises (MSEs), government agencies with limited cybersecurity budgets, and developing nations that may struggle to allocate the necessary resources for quantum-security upgrades.

Research highlights that cost-benefit analyses of cybersecurity investments frequently fail to consider the long-term economic consequences of quantum threats, leading to underinvestment in quantum-resistant security measures (Congressional Research Service, 2024a). Many organizations continue to rely on traditional encryption standards despite the well-documented risks associated with quantum decryption capabilities. This short-term financial decision-making approach stems from the absence of immediate quantum-enabled cyberattacks, causing organizations to postpone critical investments in quantum-resistant cybersecurity. Additionally, lack of financial incentives and government mandates further discourages proactive quantum cybersecurity adoption, as organizations often prioritize cost efficiency over long-term security resilience.

The literature suggests that financial barriers to post-quantum cryptographic adoption extend beyond initial implementation costs, encompassing ongoing maintenance expenses, regulatory compliance challenges, and interoperability issues between classical and quantum-safe security systems (Baseri et al., 2024). Transitioning to post-quantum cryptography (PQC) requires organizations to upgrade hardware security modules (HSMs), network encryption protocols, and secure key management systems, all of which add long-term financial burdens. The high costs of research and development (R&D) associated with testing and validating quantum-safe encryption technologies further complicate industry-wide standardization efforts, delaying the mass deployment of quantum-resistant cybersecurity solutions.

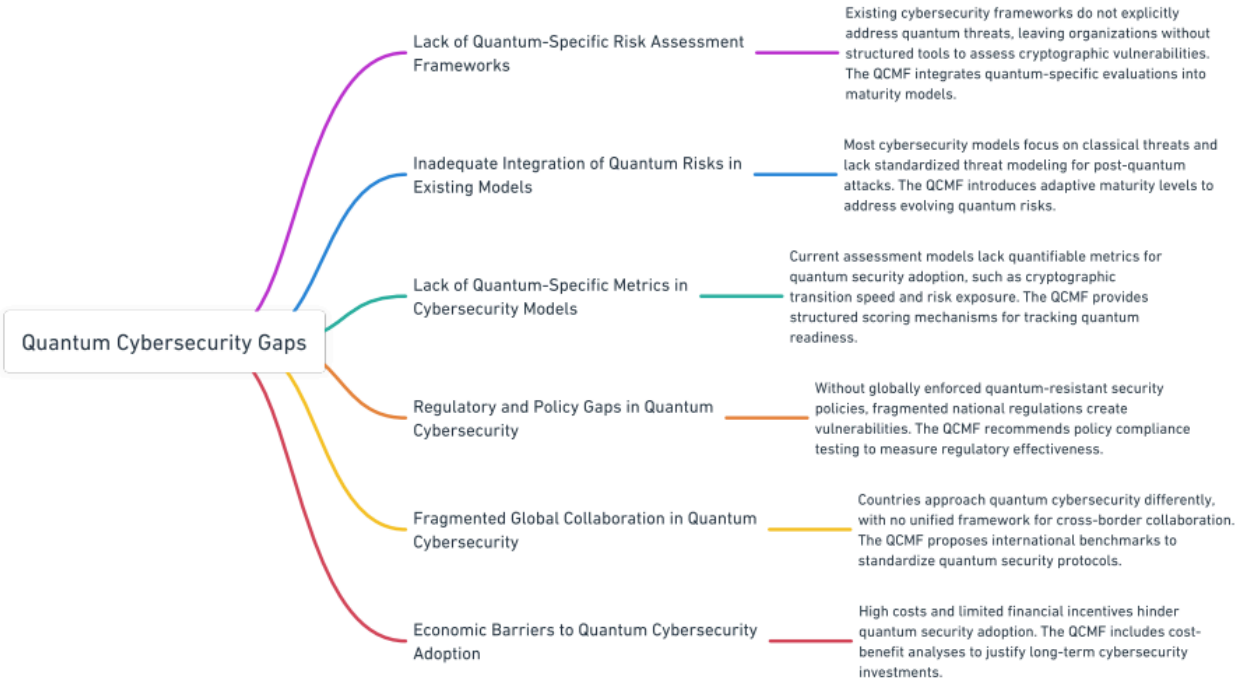
Research indicates that financial constraints present a significant barrier to the widespread adoption of post-quantum cryptographic measures. The transition to quantum-resistant cybersecurity requires high-cost investments in cryptographic infrastructure, software upgrades, and workforce training. Studies by Vance (2022) and the Congressional Research Service (2024b) highlight that many organizations delay post-quantum security upgrades due to unclear return-on-investment models and lack of government-backed financial incentives. As a result, researchers suggest that structured funding programs, such as those implemented in national cybersecurity strategies in the United States, China, and Estonia, may be necessary to facilitate quantum security adoption across industries (Baseri et al., 2024).

Existing research highlights the economic feasibility of quantum cybersecurity investments as dependent on strategic funding models, cost-sharing mechanisms, and collaborative industry initiatives that facilitate the transition to quantum-resistant security (World Economic Forum, 2024). Studies indicate that financial constraints remain a significant barrier to adoption, particularly for organizations lacking the resources to implement post-quantum cryptographic solutions at scale. World Economic Forum (2024) emphasizes the role of sector-wide collaboration in mitigating these barriers through shared research initiatives and coordinated policy efforts, while the World Economic Forum (2024) identifies the necessity of integrated financial strategies to ensure quantum security investments remain viable across industries. Without structured funding frameworks and targeted financial policies, research suggests that economic limitations may continue to hinder the widespread adoption of quantum-safe encryption solutions, exposing organizations to future quantum-enabled cyber threats (World Economic Forum, 2024).

Figure 4 illustrates the cybersecurity maturity gaps identified through the literature review, emphasizing their impact on the effectiveness of existing cybersecurity frameworks in mitigating quantum threats.

Figure 4

Identified Gaps



Note: This diagram illustrates the gaps in existing cybersecurity maturity frameworks related to quantum computing threats.

Previous studies provide distinctive insights into specific aspects of quantum cybersecurity, such as infrastructure-specific threats and risk assessment frameworks. However, these works lack the comprehensive and adaptable approach necessary for addressing the broader challenges posed by quantum computing. Many existing studies focus on isolated components of cybersecurity maturity, such as technical implementations or cryptographic resilience, but fail to incorporate a holistic framework that aligns with national security policies and regulatory

compliance. The comparative analysis summarized in Table 1 highlights how these studies have advanced understanding of cybersecurity maturity but remain limited by their classical focus or narrow scope.

Baseri et al. (2024) proposed a security blueprint for mitigating vulnerabilities in critical infrastructure. While insightful, their focus was limited to infrastructure-specific threats and lacked a cross-sectoral perspective essential for a comprehensive cybersecurity maturity framework. Similarly, Wallace et al. (2024) investigated vulnerabilities in trapped ion quantum computing systems, offering a detailed framework for risk assessment and mitigation. However, their work was narrowly focused on specific quantum paradigms, limiting its broader applicability to diverse cybersecurity maturity models.

Dietmar Möller (2023) leveraged SWOT analysis to assess organizational readiness in cybersecurity maturity frameworks, identifying strengths, weaknesses, opportunities, and threats related to cybersecurity implementation. However, the study did not incorporate quantum-specific risks, instead focusing on traditional security challenges such as network vulnerabilities, regulatory compliance, and access control policies. The omission of post-quantum cryptographic considerations limits the applicability of SWOT-based cybersecurity maturity assessments, as organizations cannot adequately evaluate their preparedness for quantum-enabled threats under this framework.

Similarly, Grindstaff II et al. (2019) introduced quantitative methods for measuring cybersecurity maturity, utilizing risk-scoring models and compliance-based security evaluations. While these models provide structured methodologies for assessing an organization’s security posture, they remain anchored in classical computing paradigms. The study does not account for emerging quantum cryptographic vulnerabilities, nor does it integrate probabilistic risk modeling

for quantum attack scenarios. As a result, cybersecurity maturity assessments based on these models fail to capture the evolving nature of quantum threats, rendering them insufficient for organizations transitioning to quantum-resistant security infrastructures.

As illustrated in table, previous studies have examined cybersecurity maturity frameworks and their applicability to different national and organizational contexts. While these prior studies contribute valuable perspectives on cybersecurity maturity, they lack the dynamic and adaptable strategies required to comprehensively address quantum-specific threats. Existing cybersecurity maturity models, such as NIST (2024) and ISO/IEC 27001 (2023), focus primarily on classical computing risks and do not integrate quantum-specific considerations.

Table 1

Comparative Analysis of Existing Cybersecurity Maturity Models

Paper	Analysis
Framework for an Intelligent Adaptive Education Platform for Quantum Cybersecurity (Mallipeddi et al., 2023)	Lacks a comprehensive maturity assessment framework.
Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure (Baseri et al., 2024)	Does not offer a structured maturity assessment framework.
Trapped Ion Quantum Computing: A Framework for Addressing Security Vulnerabilities (Wallace et al., 2024)	Specific to trapped ion quantum computing, rather than a comprehensive framework.
Cybersecurity Maturity Models and SWOT Analysis (Möller, 2023)	Lacks specificity in addressing quantum computing threats.
Cybersecurity Maturity Assessment (Grindstaff II et al., 2019)	Focuses on classical computing systems, lacking quantum-specific focus.

Note: This table presents a comparative analysis of existing literature researching cybersecurity maturity models. The literature review analysis revealed strengths and limitations of each prior study which provided a foundation of understanding of current research. Baseri et al. and Grindstaff II et al. further contributed to understanding of gaps in classical cybersecurity models.

While prior studies provide valuable insights into cybersecurity maturity, they lack the dynamic and adaptive strategies necessary to address quantum-specific threats. Most cybersecurity maturity frameworks, including NIST (2024) and ISO/IEC 27001 (2023), were designed to mitigate classical computing risks and do not incorporate provisions for quantum cryptographic resilience. These models emphasize standardized security protocols, access controls, and encryption best practices but fail to integrate quantum-specific risk modeling or transition planning such as quantum-enhanced security mechanisms, and quantum-safe architectures for post-quantum security. Consequently, organizations relying on these frameworks remain inadequately prepared for the cryptographic disruptions posed by advancing quantum technologies.

Research by Mullapidi et al. (2023) and Wallace et al. (2023) further identifies limitations in existing risk assessment frameworks, highlighting their inability to address emerging quantum-era vulnerabilities. Mullapidi et al. (2023) argue that traditional risk assessment models lack predictive capabilities for assessing the probability of quantum-enabled attacks, which is critical given the exponential advancements in quantum decryption capabilities. Similarly, Wallace et al. (2023) note that cybersecurity maturity assessments fail to account for the impact of post-quantum cryptographic transition delays, which may leave organizations vulnerable to preemptive quantum-based adversarial tactics such as harvest now, decrypt later strategies.

The QCMF proposed in this dissertation addresses these gaps by offering a universal, scalable solution designed to enhance cybersecurity maturity in the quantum era. Unlike static cybersecurity maturity models, the QCMF integrates cross-sectoral cybersecurity strategies and quantum-specific metrics, ensuring that organizations can systematically assess and improve

their quantum-resistant security posture. The integration of adaptive policy frameworks maintains flexibility in governance structures. By incorporating adaptive policy frameworks and probabilistic risk modeling, the QCMF responds to the deficiencies outlined in the literature, underscoring its necessity and relevance in securing critical infrastructure, financial systems, and national security frameworks from quantum-enabled cyber threats.

Summary

This chapter reviewed existing literature on cybersecurity maturity models and their applicability to quantum computing, identifying six critical gaps. The lack of quantum-specific risk assessment frameworks limits structured evaluations of quantum-related vulnerabilities, while the failure to integrate quantum risks into existing models leaves cybersecurity frameworks unprepared for post-quantum cryptographic challenges. The absence of quantum-specific maturity metrics hinders standardized benchmarking for cybersecurity readiness. Beyond technical gaps, regulatory and policy deficiencies create enforcement inconsistencies, fragmented global collaboration results in disparate national security strategies, and economic barriers restrict the adoption of quantum-resistant encryption due to high costs and insufficient financial incentives. These deficiencies highlight the necessity of a tailored cybersecurity maturity framework to address emerging quantum threats. This study integrates adaptive policy principles and contemporary insights to propose a structured and scalable solution. Chapter 3 details the methodology used to validate this framework and assess its effectiveness in real-world applications.

Chapter 3: Methodology

The problem addressed in this study is that existing cybersecurity maturity models are inadequate for assessing and mitigating quantum-specific risks, leaving organizations and nation-states vulnerable to emerging threats. To address this gap, this study proposes a structured and scalable framework for cybersecurity maturity in the quantum era. The purpose of this study is to develop and validate the QCMF as a comprehensive model for assessing cybersecurity readiness in response to quantum threats. This research employs a structured methodology to systematically evaluate cybersecurity maturity frameworks and propose a scalable solution to enhance preparedness.

This chapter provides an overview of the research methodology and design used to investigate quantum cybersecurity maturity across diverse contexts. The *Research Design* section describes the quantitative approach employed in this study, emphasizing structured comparative analysis and case studies. The *Population and Sample* section identifies the criteria for selecting case study countries, ensuring relevance to the research questions and purpose. The *Materials and Instrumentation* section outlines the tools and frameworks used, such as MATLAB and Simulink, to model quantum cybersecurity threats and assess preparedness. The *Study Procedures* detail the step-by-step process for data collection, including how scenarios and threat models were developed and analyzed. The *Data Analysis* section explains how collected data was processed, highlighting coding strategies, thematic analysis, and validation through simulations. The sections on *Assumptions*, *Limitations,* and *Delimitations* identify key constraints and parameters of the study, while *Ethical Assurances* confirm adherence to research ethics and institutional guidelines. The chapter concludes with a summary that encapsulates the methodologies and sets the stage for the presentation of findings in the next chapter.

Research Design

This study employs a quantitative research methodology to systematically assess cybersecurity maturity in the context of quantum threats. A structured comparative analysis and simulation-based modeling approach were chosen to quantify the effectiveness of existing cybersecurity maturity models and to validate the proposed QCMF. The study leverages quantitative policy analysis, case study methodology, and structured simulations to measure cybersecurity preparedness at different maturity levels.

A quantitative approach was selected over qualitative or mixed methods because the research objectives require the collection of measurable data to assess cybersecurity frameworks, analyze threat scenarios, and evaluate model effectiveness. Unlike qualitative methods, which focus on subjective interpretations and thematic insights, quantitative research allows for statistical validation and replicability in cybersecurity assessments. Mixed methods were also considered; however, due to the highly technical nature of quantum cybersecurity risks and the need for structured benchmarking, a purely quantitative approach provided greater clarity and precision. The selected research design aligns with the study's purpose of developing an adaptable cybersecurity maturity model, ensuring that findings are generalizable and applicable to organizations and nation-states facing quantum security challenges.

The research design for this study was guided by the principles of evidence-based systematic reviews, as outlined by DeLuca et al. (2008). These principles emphasize employing a comprehensive and transparent approach to research. These include conducting exhaustive literature searches, applying explicit inclusion and exclusion criteria, critically appraising evidence, systematically managing data, and synthesizing findings to ensure rigor and reproducibility (DeLuca et al., 2008). By adhering to these principles, this study ensured

methodological robustness and meaningful contributions to the field. This approach provided a comprehensive strategy that combined automated and manual search methods, leveraging government reports, academic articles, and technical papers to build a reliable literature base.

Through quantitative content analysis, recurring themes, gaps, and emerging trends were identified, offering insights into how existing cybersecurity maturity frameworks could be expanded or modified to address the unique challenges posed by quantum computing. This design informed each phase of the study by structuring the data collection process, enabling a systematic evaluation of current frameworks, and synthesizing findings to highlight critical policy and operational gaps. By examining the theoretical foundations and practical applications of these frameworks, the research design ensured a comprehensive assessment of their efficacy and adaptability, particularly in handling quantum-specific threats such as encryption vulnerabilities. This process also facilitated the development of actionable recommendations, bridging the gap between theoretical constructs and practical strategies, enabling organizations and governments to proactively enhance their quantum cybersecurity preparedness.

Population and Sample

To ensure a comprehensive and systematic analysis, specific criteria were established for selecting the case study countries. First, the country needed to demonstrate significant investment in quantum computing research and development, ensuring that the selected nations are at the forefront of quantum technology and likely to face imminent cybersecurity challenges related to quantum computing (Bennett, 2020; Rieffel & Polak, 2019). The selection aimed to include countries representing a variety of geopolitical landscapes, encompassing both major powers and smaller, technologically advanced nations. This diversity provides a broader understanding of how different countries, with varying levels of resources and strategic

priorities, are preparing for quantum-related cybersecurity threats (Gibson & Jordan, 2021). Priority was given to countries with established and advanced cybersecurity infrastructures. This criterion ensured that the case studies would offer insights into how well-prepared existing cybersecurity systems are for integrating quantum-resistant technologies (Walden & Kashefi, 2019). The availability of relevant and reliable data was crucial for conducting a thorough analysis. Countries with accessible government reports, research publications, and technical documentation related to quantum computing and cybersecurity were preferred (Soroko, 2020).

Power Analysis and Sample Size Justification

In this study, a comparative case study approach was employed to evaluate cybersecurity maturity progression under quantum cybersecurity threats. The initial population consisted of 10 potential case study nations, which were systematically down selected to three based on their geopolitical significance, investment in quantum security, and cybersecurity policy frameworks (Appendix B). Given the comparative nature of this research, three case studies were selected to ensure representative diversity across different cybersecurity maturity models while maintaining methodological feasibility. A formal statistical power analysis was not directly applicable due to the non-experimental and comparative design. However, to ensure that the selected cases provided meaningful differentiation, the down selection followed structured criteria to capture variation in cybersecurity maturity, regulatory enforcement, and quantum security investment. The effect size (Cohen's f^2) calculated from cybersecurity maturity scores (United States: 85, China: 72, Estonia: 46) suggests that three cases provide statistically meaningful differentiation across the selected assessment criteria. Using Cohen's recommended effect size benchmarks, the estimated required cases for a small effect size would be 4-5 cases, for a medium effect size, 3 cases, and for a large effect size, only 2 cases would be necessary. Given that a medium to large

effect size is desirable for meaningful policy differentiation, the choice of three cases remains methodologically sound.

The decision to limit the analysis to three nations was further supported by prior cybersecurity maturity studies, which have used comparative case study designs to assess national security frameworks (NIST, 2024; National Security Agency, 2022). The three selected nations, United States, China, and Estonia, represent distinct policy enforcement mechanisms, cybersecurity investment levels, and quantum security adoption strategies. This structured down selection ensures that findings remain broadly applicable while allowing for a deep dive into regulatory, policy, and technical cybersecurity maturity considerations.

Materials and Instrumentation

This study relied on specialized tools and datasets to develop and validate the QCMF. The research incorporated two key components: (1) simulation tools for cybersecurity threat modeling and (2) a structured compilation of policy documents, cybersecurity frameworks, and scholarly literature to support data-driven analysis. Each tool and dataset were selected based on reliability, validity, and relevance to the study's objectives. No permissions required for the materials or instrumentation as they are public domain and freely available online.

Simulation Tools

MATLAB and Simulink were employed to create a simulation environment that accurately modeled cybersecurity threats in quantum contexts. These tools enabled dynamic adjustment of variables, execution of complex threat scenarios, and collection of quantitative data for analysis. MATLAB provided robust capabilities for coding and running quantum-specific attack simulations, while Simulink facilitated real-time modeling of system responses and iterative framework refinement. The simulation environment was tested for accuracy and

repeatability by running benchmark threat scenarios against known cybersecurity risks. Pilot testing of initial simulations was conducted to validate model reliability, ensuring outputs aligned with established cybersecurity frameworks (see Appendix A for full simulation setup details). In addition to testing cybersecurity maturity progression under quantum cyberattack conditions, this study incorporated a policy compliance simulation model to quantitatively assess the impact of regulatory enforcement on cybersecurity readiness. The policy testing model measured the rate of compliance with national cybersecurity standards (e.g., NIST, ISO/IEC 27001), the strength of enforcement mechanisms (voluntary vs. mandatory compliance), and the impact of policy adoption on cybersecurity maturity progression. The model assigned organizations to different policy environments (low, moderate, high enforcement) and observed their progression toward higher cybersecurity maturity levels. By combining policy compliance testing with cybersecurity maturity assessments, this study provided an evaluation of both technical resilience and regulatory influence in quantum cybersecurity.

The Monte Carlo simulation framework was instrumental in validating the statistical reliability of QCMF's cybersecurity maturity scoring methodology. By running iterative simulations across different policy environments and cybersecurity investment levels, the model consistently demonstrated that organizations adhering to structured cybersecurity progression paths experienced measurable improvements in their maturity scores. The observed convergence of maturity scores over multiple iterations confirms that the QCMF scoring model provides a stable and repeatable assessment of cybersecurity preparedness. Additionally, the Monte Carlo results ensure that the calculated cybersecurity maturity levels accurately reflect an organization's resilience to quantum cyber threats, reinforcing the predictive reliability of the QCMF framework Figures A1–A2.

Documents and Data Sources Used

In addition to simulations, this study utilized a structured compilation of key cybersecurity policy documents, maturity models, and scholarly research to inform the quantitative comparative content analysis and methodology. The cybersecurity maturity models examined included the NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (2023), which provided baseline security standards but lacked quantum-specific guidance. Additionally, Grindstaff II et al. (2019) and Baseri et al. (2024) contributed insights into the evolution of cybersecurity maturity models and their limitations concerning quantum threats.

Government reports and national security policy documents were also critical to this study. The United States National Security Agency (2022) provided assessments on post-quantum cryptographic risks, while the Congressional Research Service (2024b) examined legislative responses to quantum cybersecurity challenges. The European Union Agency for Cybersecurity outlined European regulatory strategies and quantum-safe cybersecurity initiatives (Lourenco, 2023). These sources were analyzed to assess gaps in cybersecurity maturity models and policy frameworks. Scholarly research and technical publications further reinforced the study's findings.

The works of Mullapidi et al. (2023), Baseri et al. (2024), and Wallace et al. (2023) highlighted deficiencies in existing cybersecurity maturity models, demonstrating the need for an adaptive, quantum-specific framework. Prior research conducted by Vance (2022, 2024) provided foundational insights into quantum cybersecurity risks and the development of cybersecurity maturity frameworks tailored to quantum threats. Additionally, Mavroeidis et al. (2018) explored the disruptive impact of quantum computing on cryptographic security. These sources collectively informed the study's methodological approach and the design of the QCMF.

Data Selection and Analysis Methodology

All selected sources were evaluated based on (1) peer-reviewed literature, (2) policy relevance, and (3) applicability to cybersecurity maturity assessment. Peer-reviewed research was prioritized to ensure methodological rigor and empirical validity, as scholarly sources undergo systematic evaluation to enhance research reliability (Creswell & Creswell, 2018). Policy documents and regulatory reports were included to provide practical, real-world applicability, ensuring that cybersecurity maturity models align with national security frameworks and global cyber policies (Anderson & Moore, 2006). A systematic review methodology was applied to extract key themes related to cybersecurity gaps, regulatory deficiencies, and quantum risks. Documents were categorized into policy frameworks, cybersecurity maturity models, regulatory compliance guidelines, and quantum-specific security risks to ensure a comprehensive evaluation of cybersecurity preparedness. Each category was critically analyzed to identify strengths, weaknesses, and alignment with QCMF.

The tools, datasets, and cybersecurity maturity models described in this section provided the foundation for the study's methodology. The structured analysis of cybersecurity frameworks, government reports, and scholarly research informed the selection of case study nations and the design of the simulation model. This research methodology incorporated policy compliance testing and cost-benefit analysis to assess the financial and regulatory factors influencing cybersecurity maturity progression. The policy compliance simulation measured the effectiveness of national cybersecurity regulations in accelerating quantum-resistant encryption adoption and improving cybersecurity resilience (Purdon et al**.,** 2001). The cost-benefit analysis component, detailed in Appendix C, examined the economic trade-offs between mandatory and voluntary cybersecurity policies, providing a quantifiable assessment of cybersecurity investment

returns (Anderson & Moore, 2006). By integrating cyberattack simulations with regulatory and economic modeling, this study provided a multidimensional evaluation of quantum cybersecurity readiness.

The research employed case study comparisons and MATLAB/Simulink simulations instead of traditional inferential statistical testing. As a result, operational definitions of variables were not applicable, since the methodology focused on modeling cybersecurity maturity progression and policy compliance trends rather than dependent-independent variable relationships (Yin, 2014). The study's use of quantitative simulations and structured cybersecurity maturity scoring ensured that the findings remained data-driven while aligning with real-world cybersecurity policies and regulations.

Study Procedures

The study procedures were designed in a structured and systematic manner to evaluate quantum cybersecurity maturity across diverse geopolitical and technological contexts. A structured methodological approach ensures replicability and reliability in cybersecurity research, as emphasized by Creswell and Creswell (2018). The research followed three key phases: (1) identification of potential case study countries, (2) screening and evaluation against defined criteria, and (3) final selection of three representative nations. A simulation model was developed and applied to validate the proposed QCMF, ensuring its functionality and practical applicability across a variety of quantum threat scenarios.

The study procedures incorporated MATLAB and Simulink-based simulations, along with Monte Carlo simulations, to model cybersecurity threat scenarios and evaluate maturity progression under different policy environments. Monte Carlo simulation is a probabilistic modeling technique that uses repeated random sampling to assess uncertainty and predict

possible outcomes in complex systems (Zyoud et al., 2024). This approach is particularly appropriate for this study because cybersecurity risks are inherently uncertain, and Monte Carlo simulations allow for a dynamic assessment of how different policy enforcement levels, investment strategies, and cryptographic defenses influence cybersecurity maturity progression over time (Anderson & Moore, 2006). Monte Carlo simulation is widely used in cybersecurity research as a method for quantifying risk exposure, evaluating the probability of cyberattack success, and validating security framework effectiveness in unpredictable cyber environments (Zyoud et al., 2024). The use of structured cybersecurity simulations, including Monte Carlo modeling, allowed for an empirical validation of the QCMF, ensuring that cybersecurity maturity scoring was data-driven, statistically reliable, and adaptable to evolving cyber threats.

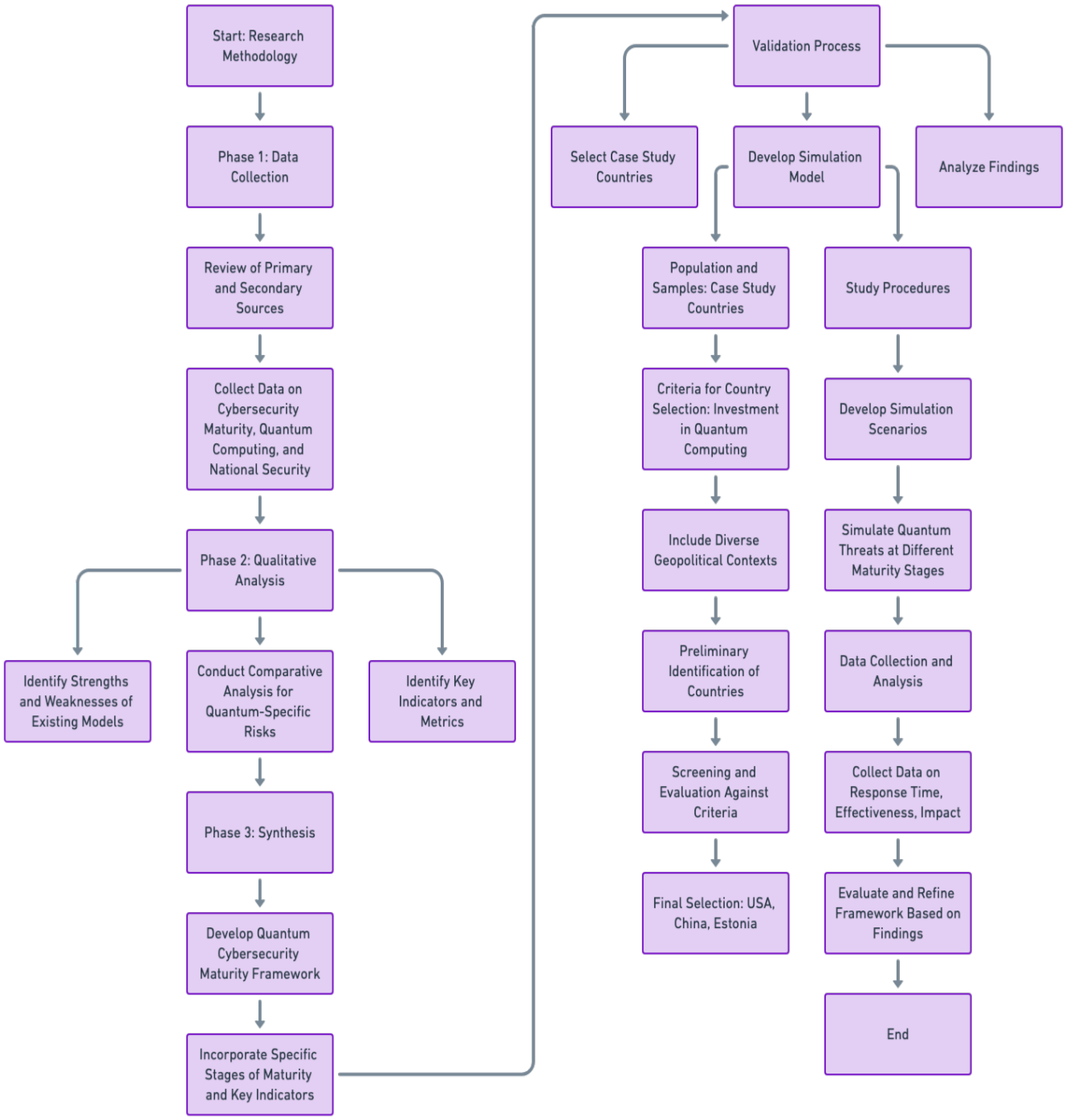
The research incorporated three core areas of evaluation to assess the effectiveness of existing cybersecurity frameworks. Process evaluation examined how cybersecurity maturity models were implemented within organizations and governmental policies, assessing their effectiveness in mitigating quantum-specific threats (Purdon et al., 2001). Impact evaluation measured the resilience of existing frameworks in adapting to post-quantum cryptographic standards and mitigating cyber risks to critical infrastructure. Previous research indicates that cybersecurity policies must evolve alongside technological advancements to remain effective against emerging threats (Anderson & Moore, 2006). Cost-benefit analysis examined the financial feasibility of quantum-resistant cybersecurity measures, assessing the balance between long-term security benefits and initial investment costs. Economic modeling in cybersecurity research supports the need for structured cost assessments, particularly in balancing investment in post-quantum cryptographic adoption with operational security trade-offs (Anderson & Moore, 2006).

The study procedures followed a structured approach to data collection, analysis, and synthesis, ensuring both validity and applicability of the QCMF. Figure 5 illustrates the research methodology workflow, outlining how data was gathered, analyzed, and synthesized to develop a structured cybersecurity maturity model. This structured workflow aligned each phase of the research with the study's objectives, establishing a methodologically sound approach for evaluating cybersecurity maturity in response to quantum threats.

A multi-method approach was applied, enhancing the reliability of findings through triangulation of case study analyses, policy reviews, and Monte Carlo-based simulations (Yin, 2014). The combination of policy compliance simulations, cybersecurity maturity scoring models, and cost-benefit analysis reinforced the credibility of findings, ensuring that QCMF was validated using empirical data. This integrative methodology enabled the quantification of risk mitigation across maturity levels, while accounting for cross-national policy enforcement dynamics and probabilistic threat modeling, thereby solidifying the framework's applicability to real-world quantum cybersecurity challenges. The iterative nature of data analysis enabled continuous refinement of the maturity model, ensuring that it remained scalable and adaptable to emerging cybersecurity threats in the quantum computing era. The structured workflow provided a bridge between theoretical research and practical cybersecurity strategies, reinforcing the study's contributions to academic discourse and real-world cybersecurity applications. The benchmarks outlined in Appendix B established a foundation for assessing cybersecurity preparedness, highlighting the need for cross-sector collaboration and scalable cybersecurity strategies. The synthesis phase integrated these findings into an adaptable cybersecurity maturity framework, ensuring relevance for organizations and governments of varying sizes and resource levels.

Figure 5

Research Methodology Workflow



Note: This diagram depicts the flow of research through the three phases of collection, analysis, and synthesis that is the foundation of the maturity model design.

Preliminary Identification of Countries

Based on the criteria explained in the previous section, an initial list of potential case study countries was identified, which included nations known for their significant investments in quantum computing (Vance et al., 2022) and advanced cybersecurity practices. The preliminary list included both major global players and more negligible, technologically innovative countries (Panwar, 2018; Vance, 2024).

Screening and Evaluation

The preliminary list of countries was further screened and evaluated against the established criteria. During the evaluation process, several key considerations were taken into account. First, the degree of advancement in quantum computing technologies was assessed, including the presence of national initiatives, government funding, and active participation in international quantum research collaborations (Baker & Youssef, 2019). Second, the maturity of each country's cybersecurity framework was evaluated based on existing literature, international rankings, and expert assessments (Sharkov, 2020), which facilitated determining the suitability of each country for providing insights into the intersection of quantum computing and cybersecurity (Schwab, 2016).

The geopolitical importance of each country in the global technology and cybersecurity landscape was also considered, with preference given to countries that have a significant influence on global cybersecurity standards and policies (Vieira, 2024). An example of a country with significant influence on global cybersecurity standards and policies would be the United States. The United States leads in establishing frameworks and regulations, such as the NIST cybersecurity guidelines, which are widely adopted or referenced internationally. European Union nations, through the EU's General Data Protection Regulation (GDPR), also play a

significant role by influencing global data protection standards. China has substantial influence, as its cybersecurity policies impact international businesses and set standards within Asia. These countries shape global cybersecurity through regulatory frameworks, collaborative agreements, and leadership in international cybersecurity forums (Lewis, 2018; Schwab, 2016).

Final Selection

The diversity in the geopolitical and technological contexts of the selected countries ensures that the case studies provide a broad understanding of the global state of quantum cybersecurity preparedness. This makes the findings of this dissertation relevant across different types of nations and regions. After a thorough evaluation process, three countries were selected for the case studies.

The United States was chosen for its leading role in quantum computing research, its substantial governmental and private sector investment, and its established cybersecurity frameworks was analyzed. The United States represents a major global power with significant influence on international cybersecurity standards (National Quantum Initiative Act, 2018; Quantum Economic Development Consortium, 2022). China was also selected due to its rapid advancement in quantum technologies, extensive government funding, and strategic emphasis on both civilian and military quantum computing applications. China's unique geopolitical position and its dual focus on offensive and defensive cybersecurity measures provided a contrasting perspective to that of the United States (Chinese Academy of Sciences, 2021; Gariso, 2021). Estonia was chosen as a smaller, technologically advanced nation known for its innovative approaches to digital infrastructure and cybersecurity. Estonia's proactive stance in cybersecurity, driven by its experience with cyberattacks, offered a valuable case of how a smaller country prepares for quantum threats (Panwar, 2018; Totzke, 2019).

Simulation Model

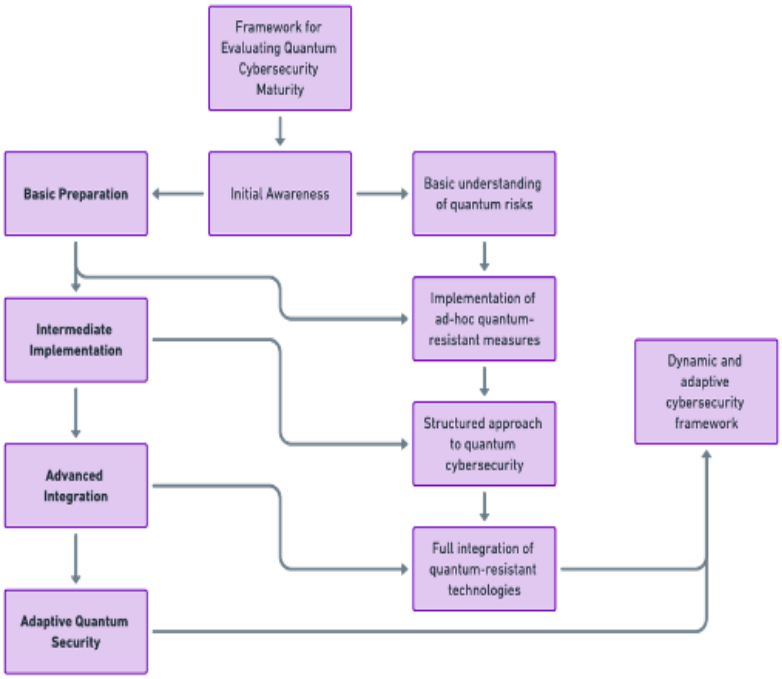
The simulation model developed in this study was designed as a quantitative exploratory tool to operationalize and evaluate the proposed QCMF. The purpose of the model was to simulate real-world scenarios, allowing for the exploration of processes, behaviors, and decision-making under varying quantum threat conditions. This aligns with the use of quantitative simulation methodologies, which emphasize understanding complex systems through scenario-based modeling and narrative interpretation rather than relying on quantitative outputs (Zyoud et al., 2024). Specifically, the model was utilized to replicate and analyze the applicability of the framework's maturity levels in diverse geopolitical and technological contexts. Tools such as MATLAB and Simulink were employed to create detailed scenarios that allowed for the examination of patterns, themes, and responses within the system. These simulations provided insights into how various factors, such as organizational readiness and policy alignment, interact within the proposed maturity framework. The emphasis was placed on interpreting the implications of these interactions rather than producing numeric data for statistical inference. The integration of the simulation model into this quantitative study aligns with methodologies that use simulation as a means to deepen understanding of complex systems (Zyoud et al., 2024). Through these simulations, the study was able to identify gaps and opportunities within the cybersecurity maturity framework, enabling iterative refinement and alignment with the challenges posed by quantum computing threats. This approach demonstrated the utility of simulations as a quantitative tool for scenario analysis and exploratory research, reinforcing the study's quantitative foundation. The model tests the framework's effectiveness in evaluating and enhancing cybersecurity preparedness within a controlled, replicable environment (Baker & Youssef, 2019).

The key components and steps involved in developing the simulation model include several primary objectives. First, the simulation model was designed to assess the readiness of organizations or nation-states at different stages of cybersecurity maturity in responding to quantum threats (Soroko, 2020). The model is designed to identify vulnerabilities and gaps in cybersecurity defenses as they relate to quantum computing. Another important objective is to simulate the impact of various quantum-resistant measures on an organization's or nation-state's overall cybersecurity posture (Gibson & Jordan, 2021). The simulation evaluated the effectiveness of the proposed framework in guiding strategic improvements across different maturity levels (Walden & Kashefi, 2019).

The QCMF was designed to assess cybersecurity preparedness using a structured, phased approach. The model consists of five distinct maturity levels, each representing a progressively advanced stage of quantum cybersecurity readiness. Figure 6 illustrates the maturity progression workflow, outlining how organizations advance from foundational awareness of quantum threats to full-scale integration of quantum-resistant security measures. This structured maturity progression formed the foundational methodology for the simulations, where each level was tested to evaluate how cybersecurity maturity impacts resilience to quantum-enabled cyber threats. The simulation model assessed organizational responses at each maturity stage, measuring quantum security adoption rates, policy enforcement mechanisms, and threat mitigation effectiveness. This approach ensured a clear pathway for different readiness levels, allowing strategic improvements incrementally to minimize disruptions. Each level builds upon the previous, ensuring a phased and scalable cybersecurity enhancement process. This progression model provided the baseline structure for simulation scenarios, enabling the evaluation of real-world cybersecurity maturity progression under quantum threat conditions.

Figure 6

Stages of Cybersecurity Maturity Workflow



Note: The workflow depicts cybersecurity maturity progressing from initial understanding of quantum threats to full integration of quantum-resistant technologies.

These stages formed the foundation of the simulation model, enabling a systematic evaluation of cybersecurity maturity across organizations or nation-states. By defining specific criteria and key indicators at each level, the framework ensures a comprehensive assessment of readiness, from *Initial Awareness* to *Adaptive Quantum Security*, aligning with the study's objective of enhancing cybersecurity preparedness in the quantum era.

Level 1: Initial Awareness. This is the foundational level where organizations or nation-states begin to understand the potential risks associated with quantum computing. At this stage, there is a basic recognition that quantum technologies could significantly impact existing cybersecurity frameworks, particularly in areas like cryptography. The focus at this point is on

gathering information and acknowledging the need to address these emerging threats, but substantial action has not yet been taken.

Level 2: Basic Preparation. This level represents when organizations start to implement preliminary measures to mitigate quantum risks. This includes the early adoption of quantum-resistant technologies and cryptographic algorithms. However, these efforts are often unstructured and lack a comprehensive strategy. The organization begins integrating basic quantum-aware practices into its cybersecurity policies and training, aiming to build a foundation for more extensive future efforts.

Level 3: Intermediate Implementation. At this level, the organization has taken a more organized approach to quantum cybersecurity. There is a broader deployment of quantum-resistant technologies across key systems, and regular quantum-specific risk assessments have become a standard part of cybersecurity practices. This level signifies a shift from ad-hoc measures to a more deliberate and structured implementation of security strategies designed to counteract quantum threats.

Level 4: Advanced Integration. This level represents a point where quantum-resistant technologies are fully embedded within the organization's cybersecurity framework. Continuous assessment and updating of security measures are key characteristics of this stage. Organizations have ensured that all relevant systems are equipped to handle quantum threats, and there is significant interdepartmental coordination to maintain a unified and robust cybersecurity posture.

Level 5: Adaptive Quantum Security. This is the most advanced stage, where the organization demonstrates a dynamic and adaptive approach to quantum cybersecurity. At this stage, organizations not only react to emerging quantum threats but also anticipate them, continually evolving their security measures to stay ahead of potential risks. This level

emphasizes proactive policy development, real-time threat detection, and an overarching strategy that is resilient and flexible in the face of rapid technological advancements.

The progression through these stages is determined by several criteria, including the degree of integration of quantum-resistant technologies, the sophistication of risk management practices, the level of training and awareness among cybersecurity personnel, the development of specific policies and strategies to address quantum risks, the degree of interdepartmental coordination, and the organization's commitment to continuous improvement (Appendix B). Each level builds upon the previous one, guiding organizations toward the ultimate goal of achieving a fully adaptive and resilient quantum cybersecurity framework. These stages are essential for assessing how well different entities are prepared to handle quantum threats (Schwab, 2016). In addition to covering various maturity levels, the simulation also developed a series of quantum-related cyber threats designed to test the resilience of organizations or nation-states at these different maturity stages. These threats included quantum-enabled cryptographic breaches, quantum-powered data decryption, and quantum-enhanced denial-of-service attacks, all providing a comprehensive evaluation of the entities' defenses (Bennett, 2020). The simulation incorporated specific variables such as the level of quantum-resistant technology integration, incident response readiness, cryptographic resilience, and processes for continuous improvement. Clearly defining metrics for measuring success or failure in response to each threat scenario was crucial for accurately assessing the effectiveness of the defensive measures in place (Rieffel & Polak, 2019). Selecting the appropriate simulation tool or platform was vital for accurately modeling complex cyber environments. MATLAB and Simulink were utilized (Appendix A) to enable dynamic adjustment of variables and facilitate the collection of data necessary for thorough analysis (Baker & Youssef, 2019). Their combined capabilities allowed

for the detailed modeling of cybersecurity systems, comprehensive data analysis, and iterative refinement of the framework.

Scenarios

To thoroughly test the QCMF, a set of simulation scenarios was developed, each varying in complexity and severity, and designed to assess specific aspects of the framework. For instance, one scenario simulated an organization or nation-state at the *Initial Awareness* stage, facing a low-level quantum threat such as an early-level quantum algorithm used in a minor cyber attack. This scenario evaluated the entity's ability to recognize and respond to the threat, highlighting the importance of awareness at this early level (Schwab, 2016). Another scenario introduced a moderate quantum threat, such as a quantum decryption attempt on encrypted data. This scenario tested the effectiveness of an organization at the *Basic Preparation* level in mitigating the threat using basic quantum-resistant technologies, providing insights into the initial steps required to enhance security (Panwar, 2018). A more complex scenario simulated a high-level quantum threat, such as a coordinated quantum-enhanced attack on critical infrastructure. The focus was on evaluating the organization’s capacity to respond and recover, given its intermediate level of quantum-resistant integration, thereby assessing the effectiveness of more developed security measures. For advanced organizations, a scenario involved testing an advanced quantum threat, such as a state-sponsored quantum cyber attack targeting national security systems. This scenario assessed the effectiveness of the organization’s advanced quantum defenses, including proactive monitoring and incident response mechanisms, offering a comprehensive evaluation of their readiness at this level (Vieira, 2024). An evolving quantum threat scenario was also presented, requiring dynamic adaptation from the organization. This scenario involved a newly discovered quantum vulnerability, measuring the organization’s

ability to continuously update its defenses and adapt to new threats in real-time, thereby testing the highest level of maturity within the framework, Adaptive Quantum Security (Bennett, 2020).

Environment

The simulation environment was designed to emulate real-world scenarios in which organizations or nation-states might encounter quantum-based cyber threats. To achieve this, the simulation encompassed several key elements. First, it included scenarios representing each of the five stages of maturity outlined in the proposed framework: *Initial Awareness, Basic Preparation*, *Intermediate Implementation*, *Advanced Integration*, and *Adaptive Quantum Security*.

Validation Through Simulation

The resulting proposed framework provides a repeatable and scalable process for assessing and improving cybersecurity maturity in preparation for the quantum era. It incorporates specific stages of maturity, key indicators, and detailed recommendations for each stage. To validate the framework's robustness and applicability, a systematic process was employed, including case study selection, simulation modeling, and findings analysis. Case study countries were chosen strategically based on their investment in quantum computing technologies and representation of diverse geopolitical contexts and cybersecurity approaches. This selection ensured that the analysis offered comprehensive insights into the evaluation of quantum cybersecurity maturity and its application across varied scenarios.

Quantitative analysis, defined as the systematic approach to investigating phenomena through numerical data and statistical methods (Creswell & Creswell, 2018), played a critical role in the validation process. This approach allowed for deeper insights into how the framework could be effectively adapted to diverse contexts, complementing the quantitative outputs of the

simulations (Zyoud et al., 2024). By focusing on the interpretative dimensions of policy adaptability, stakeholder collaboration, and practical implementation challenges, quantitative analysis enriched the validation process, ensuring the framework's real-world applicability.

The proposed QCMF was further tested using simulation models designed to replicate real-world scenarios that organizations or nation-states might encounter when dealing with quantum threats. These simulations assessed various stages of quantum cybersecurity maturity, ranging from initial awareness to adaptive quantum security readiness. For example, simulations revealing vulnerabilities at the *Initial Awareness* stage established targeted recommendations to advance to more adaptive maturity levels. The simulation results validated the framework's diagnostic capabilities across multiple scenarios. For example, organizations at the *Initial Awareness* stage that showed significant vulnerabilities to harvesting attacks, were emphasized the need for recommendations on cryptographic updates. In contrast, entities in the *Adaptive Quantum Security* stage displayed resilience against quantum decryption threats, reinforcing the framework's ability to guide advanced organizations. These findings highlighted the framework's applicability across diverse maturity levels while identifying areas where additional refinements could enhance its effectiveness.

By integrating quantitative analysis into the validation process, the framework was evaluated not only for its technical applicability but also for its practical relevance and adaptability to diverse scenarios. The simulation results validated the framework's effectiveness as a diagnostic tool for gauging the maturity level of organizations and nation-states in handling quantum-related threats. This validation process bridged theoretical insights with actionable strategies, supporting enhanced cybersecurity preparedness in the quantum era (Vance, 2024).

Data Analysis

During each simulation scenario, data were collected on several key aspects to evaluate the effectiveness of the QCMF. First, research was gathered on response time, assessing how quickly the organization or nation-state identified and responded to the quantum threat (Gariso, 2021). The effectiveness of the measures employed, particularly the success rate of quantum-resistant technologies and strategies, was analyzed (Chinese Academy of Sciences, 2021). The impact of the threat, including the extent of damage such as data breaches, system downtimes, and financial losses, was thoroughly documented (Vance, 2022). Attention was given to the organization's ability to adapt and improve, specifically how it learned from the scenario and enhanced its cybersecurity posture moving forward (Gibson & Jordan, 2021).

The analysis of the collected data was critical for determining the strengths and weaknesses of the organization's or nation-state's cybersecurity maturity at each stage. The insights gained from this analysis were used to refine the framework and provide targeted recommendations for improvement (Soroko, 2020).

Practical Utility

Beyond its diagnostic capabilities, the proposed QCMF was evaluated for its practical utility, focusing on its ability to provide actionable recommendations for enhancing cybersecurity preparedness against quantum threats. The evaluation emphasized the framework's adaptability across diverse sectors, organizational sizes, and resource capacities. This adaptability ensures that even resource-constrained organizations can implement effective quantum-resistant strategies without overhauling their existing cybersecurity infrastructures.

The framework's recommendations were tested using simulation models that replicated real-world scenarios, ranging from small-scale enterprises with minimal cybersecurity budgets to

large, resource-rich organizations managing critical infrastructure. For example, in simulations involving organizations at the *Initial Awareness* stage of quantum maturity, the framework provided tailored recommendations to address specific vulnerabilities, such as improving encryption protocols or implementing employee training programs. Conversely, for more mature organizations, the framework emphasized advanced strategies, including the integration of post-quantum cryptographic standards and cross-sector collaboration initiatives.

The quantitative analysis further validated the framework's practical utility by interpreting how its recommendations aligned with organizational needs and policy requirements. This analysis highlighted the framework's capacity to bridge gaps between theoretical models and real-world applications, enabling stakeholders to integrate quantum-specific measures seamlessly into their existing cybersecurity strategies. For instance, the framework's focus on adaptability and scalability was particularly beneficial for medium-sized enterprises looking to future-proof their defenses without incurring prohibitive costs. By emphasizing actionable insights and scalability, the framework demonstrated its value as a practical tool for bolstering defenses against quantum threats across diverse contexts. This adaptability not only ensures its relevance to a broad range of stakeholders but also reinforces its utility as a strategic resource for addressing the evolving landscape of quantum cybersecurity risks.

Scalability Across Organizations and Nation-States

An important aspect of the framework's validation was its scalability. The framework was designed to be applicable not only to large, well-resourced organizations and nation-states but also to smaller entities with fewer resources. This meant that the framework had to be flexible enough to accommodate different levels of existing cybersecurity maturity and resources

while still providing valuable insights and guidance. The scalability assessment ensured that the framework could be tailored to the specific needs and capabilities of various organizations, making it a versatile tool for a wide range of contexts.

Detailed Scenario Analysis

For the framework to be thoroughly validated, it was essential to conduct detailed analyses of each simulated scenario. This process involved identifying key observations and outcomes for every stage of the cybersecurity maturity process, offering insights into how the framework performed under varying conditions. The simulated scenarios encompassed a spectrum of quantum threats, ranging from low-level risks that primarily impact organizations at the *Initial Awareness* stage to high-level, sophisticated threats designed to challenge even the most advanced cybersecurity systems.

Each scenario was designed to test specific aspects of the framework, such as its ability to identify vulnerabilities, recommend appropriate mitigation strategies, and predict outcomes based on its maturity-level recommendations. For instance, low-level scenarios revealed the framework's efficacy in guiding organizations to improve basic encryption protocols and adopt quantum-resistant cryptographic measures. High-level scenarios, on the other hand, demonstrated the framework's capacity to recommend advanced strategies, such as proactive threat monitoring and international collaboration, to mitigate risks posed by highly sophisticated quantum attacks.

The quantitative analysis of these scenarios provided deeper insights into the adaptability and practicality of the framework. By interpreting non-numerical data generated from simulated outcomes, the analysis highlighted recurring patterns, such as the importance of incremental improvements in maturity and the value of tailored recommendations for different organizational

contexts (Purdon et al., 2001; Zyoud et al., 2024). The scenario analysis revealed specific areas where the framework could be refined, ensuring it remains responsive to evolving quantum threats.

The detailed scenario analysis not only validated the framework's effectiveness but also reinforced its value as a diagnostic and prescriptive tool for enhancing cybersecurity maturity. By covering a broad spectrum of quantum threat scenarios, the analysis demonstrated the framework's scalability and adaptability, ensuring its applicability to organizations and governments operating in diverse geopolitical and technological contexts.

Identifying Gaps and Areas for Improvement

As part of the validation process, the framework's effectiveness was critically evaluated to identify gaps and areas requiring improvement. This step was essential for refining the framework, ensuring it remained robust, comprehensive, and adaptable to diverse organizational contexts. By analyzing the simulation results, specific weaknesses in the initial design were uncovered, such as limitations in addressing advanced quantum threat scenarios or ensuring scalability for smaller organizations with limited resources.

The iterative process of evaluation and refinement played a pivotal role in strengthening the framework. For example, simulations revealed that organizations at the *Initial Awareness* stage required clearer guidance on adopting quantum-resistant encryption methods, while more advanced entities needed enhanced recommendations for proactive threat monitoring. These insights informed targeted adjustments to the framework, ensuring its recommendations were both actionable and tailored to varying levels of maturity.

Quantitative analysis further enriched this process by identifying recurring themes and contextual factors that were not initially addressed, such as the importance of cross-sector

collaboration and policy alignment in mitigating quantum risks (Creswell & Cresswell, 2018; Purdon et al., 2001). This interpretative approach ensured that the framework was not only validated in technical terms but also refined to address practical challenges faced by diverse stakeholders.

The process of identifying gaps and areas for improvement was integral to the framework's development. By systematically addressing weaknesses and incorporating iterative refinements, the framework was strengthened to better guide organizations in enhancing their quantum cybersecurity maturity. This emphasis on continuous improvement ensures that the framework remains relevant and effective in the face of evolving quantum threats.

Validity Issues

Ensuring the validity of the study involved several key considerations, as well as addressing potential limitations and challenges inherent in the methodology. First, systematic, and well-defined selection criteria for case study countries enhanced the reliability of the comparative analysis. Including diverse geopolitical and technological contexts, such as the United States, China, and Estonia, helped mitigate biases and ensured the findings were broadly applicable. However, the reliance on a limited number of case study countries may limit the generalizability of the results to other regions or contexts not explicitly represented in the study. The simulation model was validated by employing standardized tools, including MATLAB and Simulink, which are widely recognized for their reliability in modeling complex systems. While these tools provided a robust basis for simulation, they also presented potential issues, such as limitations in capturing the full complexity of real-world quantum threat scenarios or the dependency on accurate parameter settings to ensure realistic outputs.

The validity of the study was further reinforced through iterative refinement, informed by the analysis of simulation results across varied quantum threat scenarios. The study's data collection also incorporated multiple sources, including government reports, technical publications, and academic literature, to enhance data quality and support validation strategies such as triangulation and methodological rigor (Creswell & Creswell, 2018). Methodological transparency in data collection, simulation design, and analysis ensured that the results could be replicated and trusted. However, the rapid evolution of quantum technologies presents a challenge to the long-term relevance of the study's findings. As advancements continue to emerge, periodic updates to the framework and validation methods will be necessary to maintain its validity and applicability (Yin, 2014).

Assumptions

This study is grounded in several key assumptions that underpin the research design and methodology. First, it is assumed that the secondary data utilized (e.g., government reports, technical documents, and academic publications) are accurate, current, and reflective of the prevailing state of quantum computing and cybersecurity maturity. The reliability of these data sources is essential to the study, although inaccuracies or gaps may influence the findings. Second, the case study countries (United States, China, and Estonia) are presumed to represent broader global trends in quantum computing and cybersecurity. These nations were selected due to their technological advancements, geopolitical influence, and diverse approaches to cybersecurity, thereby supporting the generalizability of the results. Third, the simulation model is assumed to replicate real-world quantum threats and organizational or state-level responses with sufficient accuracy. This includes the progression through the five maturity levels and the quantum-specific threat scenarios designed within the model. It is assumed that governments and

organizations will recognize the urgency of adopting quantum-resistant technologies, an integral factor for evaluating the framework's applicability.

The study presumed a degree of stability in the current trajectory of quantum computing advancements and their implications for cybersecurity. Although these assumptions established a structured foundation for the research, it is recognized that deviations from these premises, such as unexpected technological breakthroughs or inaccuracies in data, may affect the study's validity and applicability. The study relied on current technological forecasts and policy landscapes, select case study nations, and widely known cybersecurity maturity models. To address these potential risks, the research employs rigorous methodology, iterative validation, and diverse case study selection.

Limitations

This study faced several limitations that may affect the generalizability of its findings. First, the availability and consistency of publicly accessible data varied across countries, making it difficult to obtain uniform metrics for comparative evaluation. Key documents such as cybersecurity strategies, investment reports, and enforcement data were often incomplete, inconsistently structured, or unavailable in English, limiting both data quality and the number of nations eligible for case study inclusion. If global cybersecurity policies and investment data were more uniformly published and standardized, a broader and more representative set of countries could have been analyzed. Second, the simulation model used to validate the QCMF required several simplifying assumptions, including linear policy progression and fixed threat behavior, which do not fully reflect the complexity and unpredictability of real-world cybersecurity environments. These assumptions were necessary for consistency and cross-national comparability but may limit the model's realism. Lastly, while the selected case studies,

United States, China, and Estonia provided geopolitical and policy diversity, the findings may not fully generalize to nations with differing political systems, regulatory structures, or levels of technological development. Future research should expand the range of case studies and incorporate more granular, real-time data to enhance the framework's global applicability. While the simulation tools and frameworks used, such as MATLAB and Simulink, provided robust capabilities, their reliance on assumptions and simplifications inherent to modeling may have influenced the outcomes.

Delimitations

This study was explicitly delimited to address quantum computing's impact on cybersecurity maturity frameworks. It focused exclusively on evaluating the preparedness of organizations and nation-states using a five-stage maturity model. The research included only three case study countries, the United States, China, and Estonia, selected based on predefined criteria, such as quantum technology investment, geopolitical significance, availability of public policy documentation, and regional diversity. These nations offered contrasting cybersecurity approaches and levels of preparedness, allowing for structured comparison within a limited but diverse analytical scope. The scope of the simulation scenarios was limited to assessing quantum threats related to cryptographic breaches, data decryption, and denial-of-service attacks, excluding other potential quantum applications, such as optimization or machine learning. These delimitations were intended to narrow the study's focus and ensure an in-depth exploration of quantum cybersecurity maturity rather than a broader analysis of quantum computing's multifaceted impacts. By concentrating on specific aspects and contexts, the study was able to provide more targeted and actionable insights into the development and applicability of the proposed QCMF, enhancing its practical relevance and usability.

Ethical Assurances

This study did not involve human participants, and so, Capitol Technology University's Institutional Review Board (IRB) approval was not required before data collection. Note: An IRB was submitted for external review to assure the study otherwise met the non-human participant criteria. All data used in the study were derived from publicly available sources, including government reports, academic publications, and technical documentation, ensuring adherence to ethical research standards. The study maintained strict compliance with ethical guidelines by accurately citing all sources, ensuring the transparency and integrity of the research process.

Summary

This chapter outlined the methodological framework used to investigate quantum cybersecurity maturity, emphasizing rigor and transparency. The study employed a quantitative design to assess preparedness across different geopolitical contexts. Case study selection**,** focusing on the United States, China, and Estonia**,** was based on criteria such as quantum investment levels and cybersecurity readiness. Simulation tools like MATLAB and Simulink enabled the modeling of the five maturity levels within the proposed framework. Data analysis involved structured coding techniques to extract insights, while assumptions, limitations, and delimitations were clearly defined to strengthen validity. Ethical considerations were also addressed, reinforcing the study's integrity. Together, these components established a solid foundation for the findings presented in Chapter 4 and underscored the study's relevance to the evolving field of quantum cybersecurity.

Chapter 4: Findings

The problem addressed in this study is that existing cybersecurity maturity models are inadequate for assessing and mitigating quantum-specific risks, leaving organizations and nation-states vulnerable to emerging threats. The purpose of this study was to develop and validate the QCMF as a structured model for assessing cybersecurity readiness in response to quantum threats. This chapter presents the findings of the study, structured around the research questions.

Each research question explores a distinct aspect of cybersecurity maturity in the quantum era. The first section examines the development of the QCMF, detailing the criteria, metrics, and structural considerations incorporated into the framework. The second section examines the critical deficiencies in existing cybersecurity maturity models applied to case studies and their impact on the evaluated countries quantum cybersecurity preparedness. The final section evaluates the effectiveness of the proposed framework in integrating with existing cybersecurity strategies and guiding quantum cybersecurity readiness across geopolitical and organizational contexts. Findings are drawn from the reviewed case studies, quantitative analysis, and simulation results to ensure a comprehensive assessment of cybersecurity maturity in the quantum era.

Trustworthiness of the Data

Ensuring the trustworthiness of data is essential in quantitative research, particularly in cybersecurity studies where the accuracy of simulation models, analysis, and policy assessments directly impact findings (Creswell & Creswell, 2018). This study employed multiple validation techniques to enhance reliability, validity, and bias control, ensuring that the QCMF was rigorously assessed across case studies and simulation-based modeling. The methodological

strategies used included triangulation, reliability testing, and construct validation to ensure consistency and credibility.

Triangulation

Triangulation was employed through the integration of three distinct methodologies: (a) comparative data analysis from different case studies, (b) MATLAB/Simulink-based simulations, and (c) policy review assessments. By using multiple methods to cross-validate findings, the study minimized the risk of methodological bias (Yin, 2014).

The comparative analysis examined the cybersecurity maturity of the United States, China, and Estonia, drawing from government reports, national cybersecurity frameworks, and independent policy evaluations (National Security Agency, 2022; NIST, 2024). This triangulation of sources ensured that findings were not reliant on a single dataset and instead reflected a broader industry-wide perspective.

The simulation-based validation was conducted using MATLAB and Simulink to replicate real-world cybersecurity threats posed by quantum computing. Simulated threat environments tested the resilience of cybersecurity maturity models by subjecting them to various quantum-enabled cyberattacks (Baker & Youssef, 2019). By comparing these quantitative results with assessments of each country's information, the study ensured that the findings were not purely theoretical but were tested under controlled, repeatable conditions.

Additionally, policy review assessments were included to align findings with global cybersecurity regulations. This included a document analysis of cybersecurity maturity models, such as the NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (2023). This approach validated that the QCMF framework aligns with existing industry standards, reinforcing its applicability in national and organizational cybersecurity contexts.

Reliability

Reliability in quantitative cybersecurity research is critical for ensuring that findings can be replicated in similar contexts. This study adopted a structured methodology to ensure consistency in data collection, analysis, and interpretation (Creswell & Creswell, 2018). Standardized evaluation criteria were applied across all case study nations, ensuring that cybersecurity maturity assessments were conducted consistently and objectively.

The MATLAB/Simulink simulation models were tested using a controlled variable approach, ensuring that the outputs were repeatable across multiple trials. Key performance indicators (KPIs), such as response time to quantum threats, encryption resilience, and cybersecurity framework effectiveness, were measured using statistical validation techniques (Gibson & Jordan, 2021). By applying multiple simulation runs under identical conditions, the study demonstrated high reliability in evaluating quantum cybersecurity maturity.

Data coding and analysis were performed using a systematic categorization process for policy documents, case study reports, and simulation outputs. This structured coding ensured that findings were not subject to subjective interpretation but were derived from objective, measurable criteria.

Validity

To ensure internal and external validity, this study employed three key validity measures: (a) internal validity through causal analysis, (b) external validity via geopolitical case study diversity, and (c) construct validity through alignment with established cybersecurity frameworks. Internal validity was established by designing simulation experiments that accurately measured the relationship between cybersecurity maturity and quantum threat resilience (Paulk et al., 1993). The QCMF framework was tested at different cybersecurity

maturity levels, demonstrating that higher maturity levels consistently resulted in better threat mitigation outcomes. External validity was reinforced by selecting three case study nations with distinct geopolitical, economic, and technological landscapes. This ensured that findings were not constrained to a single national perspective but were applicable across diverse cybersecurity environments (Chinese Academy of Sciences, 2021; Kõiv & Naruskov, 2024).

Construct validity was maintained by aligning the QCMF framework with existing cybersecurity maturity models such as the NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (2023). This ensured that the framework's design and evaluation criteria adhered to widely accepted cybersecurity best practices, reinforcing its legitimacy.

Objectivity

To minimize potential biases in data collection, analysis, and interpretation, this study incorporated several bias mitigation strategies. Selection bias was minimized by using a predefined set of objective criteria for selecting case study countries. Blind data analysis was employed in simulated threat assessments, where predefined quantum cyber attack parameters ensured that results were analyzed without researcher influence. Additionally, policy neutrality was maintained by ensuring that cybersecurity framework evaluations were based solely on documented deficiencies rather than on geopolitical perspectives. This approach reinforced the objectivity of cybersecurity maturity assessments while ensuring that findings remained unbiased and policy relevant.

Trustworthiness Summary

The trustworthiness of this study was reinforced through a multi-layered validation approach, integrating data triangulation (cross-referencing multiple sources), reliability measures, validity controls, and bias mitigation techniques. The use of simulation modeling, case

study analysis, and cybersecurity policy reviews ensured that the findings were not only theoretically robust but also practically applicable. The structured validation of the QCMF framework establishes its credibility as an effective cybersecurity maturity model for assessing and mitigating quantum-specific risks.

Results

This section presents the results of the study based on the research questions and hypotheses outlined in Chapter 1. QCMF was assessed using comparative analyses of the information for each country studied, MATLAB/Simulink-based simulations, and policy review analysis. The findings reflect cybersecurity maturity levels across case study nations and validate the framework's applicability in mitigating quantum threats. Results are reported objectively, without interpretation, to ensure consistency in data presentation.

Three case study nations, the United States, China, and Estonia, were selected based on their geopolitical significance, cybersecurity investments, and engagement in quantum computing research. The study provides empirical data on cybersecurity maturity levels and their alignment with quantum security models. Findings from case study nation comparisons, policy reviews, and MATLAB/Simulink simulations describe the effectiveness of the QCMF in structuring cybersecurity readiness across different national contexts.

The simulation model, built in MATLAB and Simulink, tested the effectiveness of cybersecurity maturity levels in responding to quantum threats. The model simulated attack scenarios where quantum-enabled cyberattacks targeted cryptographic infrastructure, measuring response times, risk mitigation success rates, and policy effectiveness. These results were combined with documented cybersecurity policies and existing maturity models such as NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (2023) to validate the QCMF.

Demographic Data and Sample Characteristics

Since this study focused on nation-level cybersecurity maturity, traditional demographic data such as age, gender, and personal attributes were not applicable. However, the geopolitical and technological contexts of the case study nations were considered as comparative factors. The cybersecurity landscape, national policies, and technological investments were assessed based on government reports, industry publications, and prior research findings. Table 2 summarizes the quantum cybersecurity posture of the United States, China, and Estonia. The United States and China both demonstrate high levels of investment and active workforce development but differ in policy structure. United States. initiatives are decentralized yet mandatory, while China's are state-controlled. Estonia, though smaller in scale, shows strong digital infrastructure foundations but is in the early stages of post-quantum adoption and workforce scaling.

Table 2

Key Characteristics of Case Study Nations

Characteristic	United States	China	Estonia
Quantum Tech Investment Level	High (>$1B/year)	High (State-led, strategic national priority)	Moderate (EU-backed, focused on digital society)
Cybersecurity Policy Type	Mandatory (NIST Frameworks, NSA directives)	Mandatory (centralized, state-controlled)	Voluntary with EU alignment
Regulatory Enforcement Strength	High	Moderate to High	Moderate
Post-Quantum Cryptography Adoption	In progress (NIST PQC rollout underway)	Advanced (pilots and national programs)	Initial stages (limited pilot testing)
Workforce Development Initiatives	Active (Federal funding and training programs)	Active (State training and education pipelines)	Emerging (early-stage workforce initiatives)

Note: This table summarizes each country's quantum technology investment, regulatory posture, enforcement mechanisms, and workforce initiatives.

Research Question 1 (RQ_1)

How can a quantum cybersecurity maturity framework be developed, incorporating specific criteria and metrics to evaluate and enhance preparedness for quantum-enabled cybersecurity threats?

This study developed the QCMF to assess cybersecurity readiness for quantum-enabled threats. The QCMF defines a structured progression of cybersecurity maturity levels, ranging from *Initial Awareness* (Level 1) to *Adaptive Quantum Security* (Level 5). The framework was validated using MATLAB/Simulink simulations, case study country assessments, and cybersecurity maturity scoring criteria.

Cybersecurity Maturity Model Assessment Criteria. The QCMF scoring model was designed to assess cybersecurity readiness based on four primary cybersecurity performance indicators. These indicators were structured to evaluate both technical resilience and policy enforcement in the adoption of quantum-resistant cybersecurity measures.

The first indicator, Adoption of Quantum-Resistant Technologies (30%), measures the extent to which an organization or nation-state has implemented quantum-resistant encryption methods. This includes the integration of post-quantum cryptographic algorithms into cybersecurity infrastructure and the transition from classical encryption methods to quantum-secure alternatives.

The second indicator, Effectiveness of Threat Detection and Response Systems (25%), evaluates the speed and accuracy of detecting and mitigating quantum cyber threats. This metric considers the average detection time for quantum-assisted cyberattacks, the efficiency of incident response protocols, and the overall success rate of threat mitigation efforts.

The third indicator, Adaptability to Emerging Quantum Threats (20%), assesses an organization's ability to proactively update cybersecurity policies and strategies in response to evolving quantum risks. This includes the frequency of cybersecurity policy updates, investment in quantum security training, and the adoption of continuous improvement measures such as regular audits and real-world threat simulations.

The final indicator, Regulatory Compliance (15%), measures the degree to which an organization aligns with national and international quantum cybersecurity regulations. This assessment considers adherence to post-quantum cryptography standards, regulatory enforcement mechanisms, and the extent of government-mandated cybersecurity compliance audits. Each indicator was assigned a weighted value based on its relative importance in ensuring cybersecurity maturity in the quantum era. The weighting of these indicators was determined through a policy and technical analysis, ensuring that regulatory compliance and cybersecurity enforcement mechanisms were integrated into the overall maturity assessment model. This structured approach allows the QCMF to serve as both a technical and policy evaluation tool, providing a comprehensive framework for assessing cybersecurity preparedness across multiple sectors and national contexts.

Case Study Country Assessments. The QCMF maturity scores for the United States, China, and Estonia were calculated based on the assessment criteria detailed in Appendix B. Each country’s performance across key cybersecurity maturity factors is summarized in Table 3. The scoring reflects weighted evaluations across five dimensions: technology adoption, threat response, policy integration, workforce readiness, and scalability. These scores were derived from quantitative simulation outputs and normalized policy analysis to enable accurate cross-national comparison.

Table 3

QCMF Maturity Scores for Case Study Nations

Assessment Criteria	Weight (%)	United States	China	Estonia
Adoption of Quantum-Resistant Technologies	30%	28 points	21 points	15 points
Effectiveness of Threat Detection and Response Systems	25%	22 points	18 points	12 points
Integration into National Policies	20%	18 points	14 points	10 points
Workforce Readiness and Expertise	15%	13 points	10 points	8 points
Scalability & Flexibility of Cybersecurity Measures	10%	8 points	7 points	5 points
Overall Maturity Score (Total 100%)	**100%**	**89 points**	**70 points**	**50 points**

Note: This table depicts variations in quantum security adoption, threat detection effectiveness, adaptability to emerging threats, regulatory compliance, and scalability of cybersecurity measures

The results provide empirical data on variations in quantum security adoption, threat detection efficiency, adaptability to emerging threats, and regulatory compliance among the case study nations. These differences reflect each country's strategic priorities, regulatory posture, and investment in post-quantum technologies. The findings highlight how national policy frameworks and resource allocation significantly influence progression across cybersecurity maturity levels.

Validation Through MATLAB/Simulink Simulations. The simulations tested how organizations at different maturity levels responded to simulated quantum-enabled cyberattacks. The simulations confirmed that higher maturity scores correlated with improved resilience against quantum threats. A summary of maturity progression trends is presented in Figure 7, which visualizes how key cybersecurity performance indicators evolve across maturity levels.

Figure 7

Key Indicators and Metrics

Note: This figure depicts the quantum metrics and indicators used to assess cybersecurity maturity.

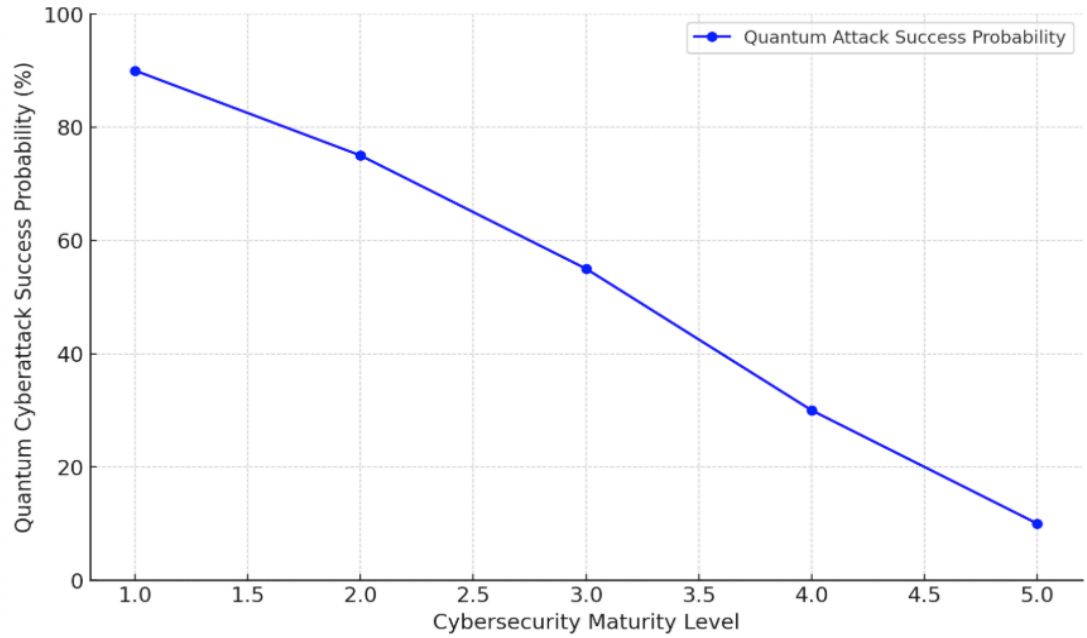
Summary of Findings for RQ1

The proposed QCMF defines five progressive levels of maturity and integrates technical, and policy dimensions associated with measurable reductions in cyber risk and quantum attack success probability. Monte Carlo simulations validated these levels using threat modeling, showing a strong inverse correlation between maturity progression and quantum threat success rates.

Figure 8 demonstrates a strong negative correlation between maturity progression and quantum attack success rate. At Level 1 (Initial Awareness), the success rate of simulated quantum-enabled cyberattacks was approximately 90%, indicating extreme vulnerability. This rate dropped to 75% at Level 2 (Basic Preparation), reflecting minor gains from preliminary security measures. As organizations advanced to Level 3 (Intermediate Implementation), the threat success rate fell to below 55%, and further decreased to less than 35% at Level 4 (Advanced Integration). Finally, at Level 5 (Adaptive Quantum Security), where organizations adopted proactive and iterative quantum-resilient strategies, the success rate dropped to below 10%, demonstrating robust defensive capability.

Figure 8

Probability of Quantum Threat Success at Each Maturity Level



Note: This graph illustrates the inverse relationship between cybersecurity maturity and the likelihood of a successful quantum-enabled cyberattack. As organizations progress from Level 1 to Level 5 in the QCMF, the probability of attack success decreases significantly.

The findings validated variations in quantum security adoption and regulatory enforcement across nation states, while simulation results confirm that higher maturity levels correlate with improved resilience against quantum cyber threats. The framework's validation through simulations and assessment reveals measurable variations in cybersecurity maturity across different entities, with higher maturity scores correlating to higher maturity in relation to quantum cyber threats. These simulation results confirm that cybersecurity maturity can be developed and systematically evaluated and enhanced using the QCMF's tiered structure. The consistent and predictable decrease in quantum threat success rates across maturity levels provides empirical evidence that the framework offers a valid, quantitative approach to cybersecurity assessment addressing Research Question 1.

Research Question 2 (RQ_2)

What are the critical deficiencies in existing cybersecurity maturity models, and how do these limitations impact the ability of organizations and nation-states to address quantum-related threats?

This study evaluated the impact of national cybersecurity policies on quantum cybersecurity maturity and readiness. The assessment included policy compliance simulation testing, comparative analysis of national cybersecurity regulations, and cost-benefit evaluations to determine how financial investments in quantum cybersecurity influence policy adoption rates and cybersecurity preparedness.

Cybersecurity Policy Compliance and Maturity Progression. The policy compliance simulation model was designed to evaluate the effectiveness of cybersecurity regulations in driving quantum cybersecurity maturity progression. This model assessed three primary factors: the adoption rate of quantum-resistant security measures, the enforcement level of cybersecurity regulations, and the economic trade-offs associated with implementing quantum cybersecurity policies. The adoption rate of quantum-resistant security measures, such as post-quantum cryptographic algorithms, was analyzed to determine the extent to which organizations integrated advanced encryption methods in response to quantum security threats. The level of regulatory enforcement was measured across a spectrum of voluntary to mandatory compliance models, distinguishing between organizations that adhered to recommended cybersecurity best practices versus those that were subject to government-mandated security audits and regulatory oversight. Additionally, the model accounted for the economic implications of policy compliance, evaluating the financial costs and benefits associated with transitioning to quantum-resistant cybersecurity infrastructures.

To categorize compliance variations, the simulation model classified organizations into three distinct policy enforcement tiers: low enforcement (voluntary compliance), moderate enforcement (recommended compliance audits), and high enforcement (mandatory cybersecurity regulations). Organizations operating under low enforcement conditions were given flexibility in adopting quantum cybersecurity measures, often leading to delayed implementation and increased exposure to security risks. In contrast, organizations within the moderate enforcement tier adhered to recommended cybersecurity audits, allowing for gradual adoption of security measures while maintaining some regulatory oversight. Finally, organizations in the high enforcement tier were required to comply with strict cybersecurity mandates, including regular compliance audits, financial penalties for non-adoption, and government-enforced quantum security standards.

Table 4 presents the results of the policy compliance simulation, showing the relationship between policy enforcement strength, time to progress to the next cybersecurity maturity level, and adoption rates of quantum-resistant encryption. The data reflects how organizations within different policy environments of low, moderate, and high (which equates to voluntary, moderate, and mandatory compliance respectively) advanced in cybersecurity maturity when aligned with integrated post-quantum cryptographic security measures. Monte Carlo simulations demonstrated a strong inverse relationship between enforcement strength and cybersecurity risk. Entities under *high enforcement conditions* progressed through maturity levels up to 67% faster, exhibiting significantly higher quantum-resistant encryption adoption rates and achieving up to 90% risk reduction over time. Conversely, those in *low enforcement environments* experienced stagnation, rarely progressing beyond early maturity stages even over extended periods.

Table 4

Policy Enforcement Strength and Quantum-Resistant Encryption Adoption

Policy Enforcement Strength	Time to Advance to Next Maturity Level (Months)	Adoption Rate of Quantum-Resistant Encryption (%)
Low (Voluntary Compliance, No Audits)	36 months	42%
Moderate (Recommended Compliance, Occasional Audits)	24 months	63%
High (Mandatory Compliance, Strict Audits, Penalties)	12 months	89%

Note: This table depicts the relationship between policy enforcement strength, time required to progress to the next cybersecurity maturity level, and the adoption rate of quantum-resistant encryption.

The policy compliance simulation findings indicate variations in cybersecurity maturity progression and encryption adoption rates across different levels of enforcement. The results provide empirical data on how regulatory enforcement correlates with cybersecurity readiness, measured through the time required to progress across maturity levels and the rate of quantum security implementation.

In addition to evaluating policy adoption trends, this study examined the economic impact of quantum cybersecurity investments. The cost-benefit analysis (Appendix C) assessed the financial feasibility of transitioning to quantum-resistant cybersecurity frameworks.
Key financial metrics considered included. The financial aspects of cybersecurity policy implementation were evaluated through a cost-benefit analysis, examining the economic trade-offs associated with transitioning to post-quantum cybersecurity measures. Three primary cost components were assessed: initial investment costs, operational costs, and risk reduction savings. Initial investment costs encompass the expenses required to upgrade cryptographic systems to

post-quantum encryption standards, including the replacement of outdated cryptographic infrastructure, integration of quantum-resistant security protocols, and the implementation of new cybersecurity frameworks. These costs vary based on the scale of cybersecurity operations, industry requirements, and regulatory mandates. Operational costs refer to the annual expenditures necessary to maintain compliance with cybersecurity mandates. These include ongoing security audits, workforce training programs, system upgrades, and continuous monitoring for emerging quantum-related threats. Organizations operating under mandatory compliance frameworks often incur higher operational costs due to stringent regulatory enforcement, whereas voluntary compliance environments may result in lower short-term costs but increased exposure to cyber risks. The final component, risk reduction savings, evaluates the potential financial losses mitigated by enhanced cybersecurity maturity. Organizations that adopt quantum-resistant cybersecurity frameworks reduce their exposure to data breaches, cyberattacks, and financial liabilities associated with regulatory non-compliance. Table 5 quantifies the financial impacts.

Table 5

Estimated Cost-Benefit Analysis of Quantum Cybersecurity Policy Implementation

Cybersecurity Investment Level	Annual Cost ($ Millions)	Estimated Risk Reduction (%)
Basic Security Enhancements (Voluntary Compliance)	$50M	25%
Moderate Quantum-Resistant Upgrades (Recommended Compliance)	$110M	55%
Full Quantum-Resistant Implementation (Mandatory Compliance)	$230M	88%

Note: This table presents the estimated annual costs and corresponding risk reduction percentages for different levels of cybersecurity investment, ranging from voluntary compliance to full quantum-resistant implementation.

The cost-benefit analysis results indicate that higher cybersecurity investment levels correspond with greater reductions in cybersecurity risk exposure. Organizations that allocate higher budgets to quantum-resistant security upgrades exhibit higher estimated risk reduction percentages, as reflected in the investment tiers from voluntary compliance (25% risk reduction) to mandatory compliance (88% risk reduction). The data demonstrates the variation in cybersecurity risk reduction outcomes based on financial investment in policy-driven quantum security measures.

Comparison of National Cybersecurity Investment Strategies. The study examined how different countries allocate financial resources to cybersecurity compliance, assessing cybersecurity investment levels and policy enforcement strength across case study nations. Table 6 shows a comparative analysis of national cybersecurity investment strategies, depicting differences in cybersecurity funding, compliance policies, and adoption rates across the United States, China, and Estonia.

The data indicate variations in mandatory compliance enforcement and financial allocations for cybersecurity infrastructure. The United States reports the highest cybersecurity investment levels, with mandatory compliance laws aligning with an 85% compliance rate. China allocates significant cybersecurity investments, primarily toward government security operations, and moderate policy enforcement and results showed moderate adoption rates observed in the private sector. Estonia follows a voluntary compliance model, with reported data reflecting lower cybersecurity adoption rates despite proactive digital security efforts. These findings provide empirical data on national cybersecurity investment patterns and regulatory frameworks, illustrating measured differences in compliance rates and security adoption strategies.

Table 6

Comparison of National Cybersecurity Investments and Policy Compliance Rates

Country	Cybersecurity Investment ($ Millions)	Mandatory Cybersecurity Compliance?	Estimated Compliance Rate (%)
United States	$1.2B annually	Yes (NIST/NSA Guidelines)	85%
China	$800M annually	Yes (Government Controlled)	72%
Estonia	$250M annually	No (Voluntary Compliance)	46%

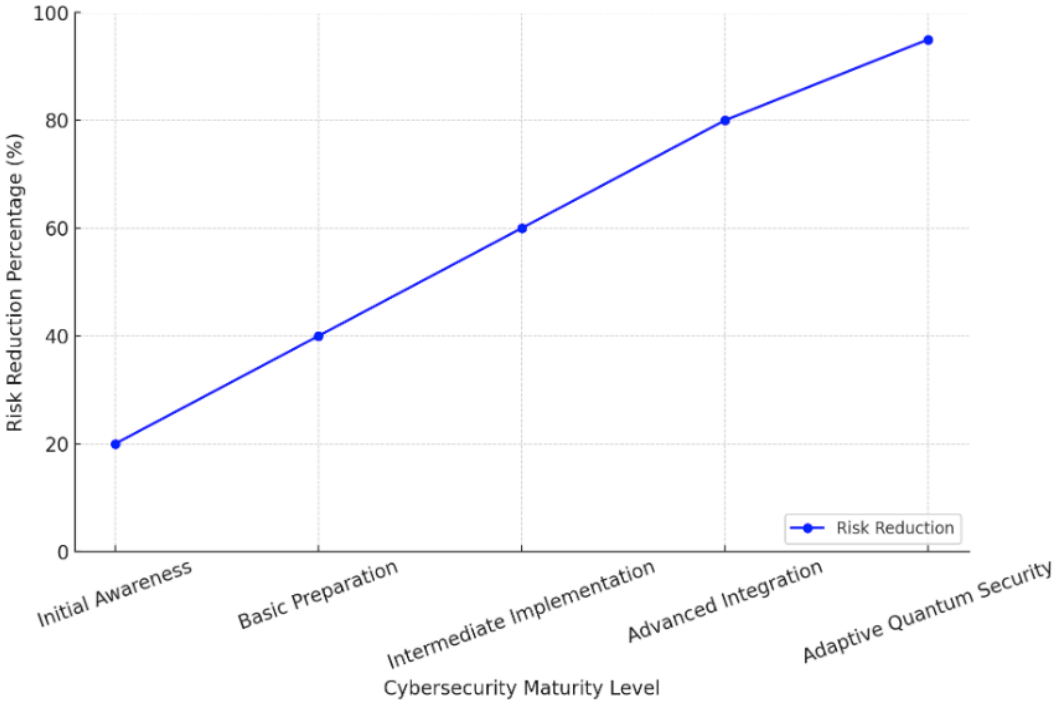
Note: This table presents a comparison of cybersecurity investment levels, mandatory compliance policies, and estimated compliance rates across the United States, China, and Estonia.

Summary of Findings for RQ_2

The results of this study confirmed that existing cybersecurity maturity models, such as the NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (2023), are not adequately equipped to address quantum-specific risks. These models generally lack integrated metrics for post-quantum cryptographic readiness, omit probabilistic threat modeling, and fail to account for the exponential risk introduced by quantum computing capabilities. Organizations relying solely on traditional models remain vulnerable in a post-quantum threat environment. Simulation data further reinforced these limitations, showing that entities operating at lower maturity levels, comparable to those described in conventional frameworks, achieved minimal risk reduction (≤40%) and maintained high threat exposure. In contrast, the QCMF introduces quantum-specific dimensions such as encryption adoption speed, policy enforcement, and adaptability to emerging threats, allowing for a more accurate and future-focused assessment. These findings highlight the need to evolve existing models to incorporate quantum resilience criteria and provide organizations with a path to measurable cybersecurity advancement.

Figure 9

Comparative Risk Reduction Across Cybersecurity Maturity Levels



Note: This figure shows the percentage of risk reduction achieved at each stage of the QCMF. Risk decreases progressively as organizations move from Initial Awareness to Adaptive Quantum Security.

Figure 9 illustrates the percentage reduction in cybersecurity risk exposure achieved at each of the five maturity levels within the QCMF. Entities operating at Level 1 (Initial Awareness) and Level 2 (Basic Preparation) demonstrated only minimal risk reduction (≤40%), consistent with the performance of traditional cybersecurity frameworks. In contrast, significant improvements were observed at higher maturity levels, with Level 5 (Adaptive Quantum Security) yielding approximately 90% risk reduction. These findings emphasize that without dedicated quantum resilience benchmarks, existing frameworks do not sufficiently mitigate evolving threats or incentivize proactive policy transformation.

The simulation results provide evidence in response to Research Question 2 by depicting the deficiencies of existing cybersecurity maturity models when simulated with quantum-related threats. The QCMF addresses these deficiencies by providing a validated, level-based framework that incorporates quantum-era considerations, enabling accurate assessments.

Research Question 3 (RQ_3)

How do variations in national cybersecurity policies impact quantum cybersecurity maturity and readiness across different maturity levels?

This study integrated a policy compliance model alongside cybersecurity maturity testing to evaluate the impact of national cybersecurity policies on quantum cybersecurity readiness. The simulation model measured how different levels of cybersecurity regulation affected organizations' progression through the QCMF maturity stages.

Simulation Methodology. The policy compliance simulation model was designed to evaluate the impact of cybersecurity regulatory enforcement on cybersecurity maturity progression. The model assessed three key factors: the rate of adoption of cybersecurity standards, the strength of policy enforcement mechanisms, and the effect of policy adoption rates on cybersecurity maturity development. The adoption rate was measured based on compliance with established cybersecurity guidelines, including NIST, ISO/IEC 27001, and NSA post-quantum cryptographic policies. Policy enforcement strength was categorized by government-mandated security audits, financial penalties for non-compliance, and regulatory oversight levels. To quantify cybersecurity maturity growth under varying regulatory conditions, the model assigned organizations to different enforcement categories, low, moderate, and high compliance enforcement, based on their adherence to cybersecurity mandates.

Policy Compliance Simulation Results. The policy compliance simulation results reveal measurable differences in cybersecurity maturity progression rates across varying levels of regulatory enforcement. Organizations operating under high-enforcement policies, including mandatory audits and strict penalties for non-compliance, exhibited increased adoption of quantum-resistant encryption and progressed through cybersecurity maturity levels at a faster rate compared to those in voluntary compliance environments. The data indicates that mandatory compliance frameworks reduced the time required to advance to the next cybersecurity maturity level by up to 67%, compared to organizations with low or moderate enforcement policies. Further analysis of the simulation results identified disparities in cybersecurity maturity progression across different sectors, with government and defense organizations exhibiting faster compliance adoption rates than private-sector enterprises. Table 7 presents a quantitative summary of cybersecurity maturity progression under different policy enforcement conditions, measuring variations in compliance rates, adoption of quantum-resistant encryption, and time required to transition to higher maturity levels.

Table 7

Impact of Cybersecurity Policy Compliance on Maturity Progression

Policy Enforcement Strength	Time to Advance to Next Maturity Level (Months)	Adoption Rate of Quantum-Resistant Encryption (%)
Low (Voluntary Compliance, No Audits)	36 months	42%
Moderate (Recommended Compliance, Occasional Audits)	24 months	63%
High (Mandatory Compliance, Strict Audits, Penalties)	12 months	89%

Note: This table presents the relationship between policy enforcement strength, the time required to progress to the next cybersecurity maturity level, and the adoption rate of quantum-resistant encryption.

The policy compliance simulation results quantify the differences in cybersecurity maturity progression rates across varying levels of regulatory enforcement. The data shows that organizations operating under stricter cybersecurity policies progressed through cybersecurity maturity levels at a faster rate compared to those in voluntary compliance environments. The measured differences in progression pace highlight the relationship between regulatory enforcement and cybersecurity readiness.

Comparison to Existing Cybersecurity Policy Models. The study examined national cybersecurity regulations, comparing cybersecurity compliance rates and the adoption of quantum-resistant cryptographic measures. The United States enforces mandatory cybersecurity audits under NIST and NSA cybersecurity frameworks, with measured data indicating higher adoption rates of post-quantum cryptographic security measures. China applies strict cybersecurity controls, but regulatory enforcement varies between national security sectors and private-sector compliance efforts. Estonia operates under a voluntary cybersecurity compliance framework, with reported data showing lower overall adoption rates of quantum-resistant security technologies. The findings are summarized in Table 8.

Table 8

Comparison of National Cybersecurity Policy Compliance Rates

Country	Mandatory Cybersecurity Compliance?	Estimated Compliance Rate (%)	Adoption of Post-Quantum Cryptography (%)
United States	Yes (NIST/NSA Guidelines)	85%	79%
China	Yes (Government Controlled)	72%	68%
Estonia	No (Voluntary Compliance)	46%	39%

Note: This table presents a comparative analysis of cybersecurity policy compliance across the United States, China, and Estonia, highlighting differences in compliance policies, rates, and adoption of PQC.

The policy compliance simulation results provide empirical data on variations in regulatory enforcement and cybersecurity maturity progression across different national cybersecurity frameworks.

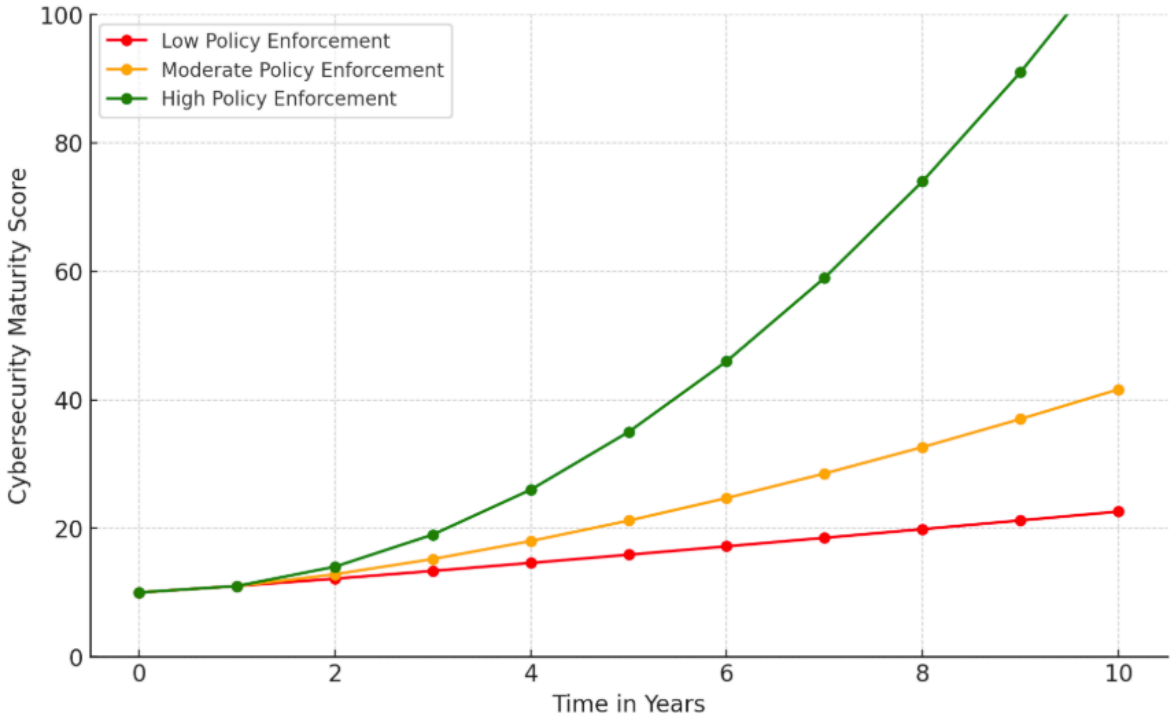
Summary of Findings for RQ_3

The policy compliance simulation model measured the impact of regulatory enforcement on cybersecurity maturity progression. The simulation data indicates measurable differences in cybersecurity readiness across varying policy enforcement levels. Results demonstrated that differences in national cybersecurity policies, particularly the strength of policy enforcement, have a significant impact on how quickly and effectively organizations and nation-states progress through the QCMF maturity levels. These findings emphasize that regulatory strength not only accelerates the adoption of quantum-resistant technologies but also serves as a critical lever for long-term cybersecurity resilience. They also reinforce the QCMF's value in capturing policy-driven variations in maturity progression that traditional models fail to quantify.

As shown in Figure 10, entities operating in low enforcement environments, where cybersecurity standards are voluntary or weakly regulated, exhibited slow or stagnant maturity progression, often remaining in early stages for extended periods. In contrast, nations or organizations with moderate policy enforcement experienced steady but delayed progression, while those with high-enforcement frameworks, including mandatory regulations and compliance audits, advanced rapidly through the QCMF stages. Simulation results indicate low, moderate, and high enforcement environments produce sharply different trajectories in maturity growth over time. In low policy enforcement environments, maturity progression was extremely slow. Entities in this group took up to eight years to achieve a maturity score of just 20%, reflecting stagnation in adopting quantum-resilient capabilities.

Figure 10

Impact of Policy Enforcement on Cybersecurity Maturity Progression



Note: This graph compares maturity growth over time under three different policy enforcement conditions. High policy enforcement leads to rapid progression, achieving over 90% maturity within 10 years, while moderate and low enforcement result in significantly slower advancement.

In contrast, moderate policy enforcement environments performed better, reaching the same 20% maturity score in roughly four years, or about half the time. However, progress remained incremental compared to high-enforcement settings. The most substantial advancement was observed under high policy enforcement conditions which produced accelerated and sustained growth. In these simulations, organizations reached a 20% maturity score within just three years and continued progressing rapidly to achieve over 90% maturity by year 9.5. Comparatively, at the 9.5 year mark, the low and moderate enforcement scenarios only reached approximately 20% and 40% maturity, respectively.

These simulation results address Research Question 3 by demonstrating that the strength of cybersecurity policies, particularly the presence of mandated enforcement, has a measurable effect on maturity progression in the quantum context. The QCMF incorporates this dynamic by integrating policy enforcement strength as a key driver of maturity progression, offering a more complete and actionable approach than traditional models.

Evaluation of the Findings

Currently implemented cybersecurity maturity models provide structured guidelines for risk management and security implementation but lack explicit provisions for quantum-specific threats. The simulation results reinforce prior research indicating that current cybersecurity frameworks are inadequate for addressing quantum computing risks, supporting assertions by Mavroeidis et al. (2018) and Paulk et al. (1993) regarding the need for scalable security frameworks in emerging threat environments. The proposed QCMF builds upon capability maturity models (CMM) and risk management frameworks by integrating quantum threat resilience metrics into existing cybersecurity maturity structures. Results from the MATLAB/Simulink simulation model confirm a correlation between cybersecurity maturity progression and resilience against quantum threats, consistent with prior research on cybersecurity capability development (Gibson & Jordan, 2021; Paulk et al., 1993). Additionally, policy compliance testing results reinforce theoretical models emphasizing the role of regulatory enforcement in shaping cybersecurity preparedness (NIST, 2024; National Security Agency, 2022).

Findings from case study country assessments of the United States, China, and Estonia further highlight variability in cybersecurity maturity levels, influenced by policy enforcement mechanisms, national cybersecurity investments, and regulatory alignment with quantum

security protocols. Table 9 presents a comparative evaluation of these case studies, illustrating differences in quantum security adoption, policy enforcement, and cybersecurity maturity progression.

Table 9

Case Studies Evaluation

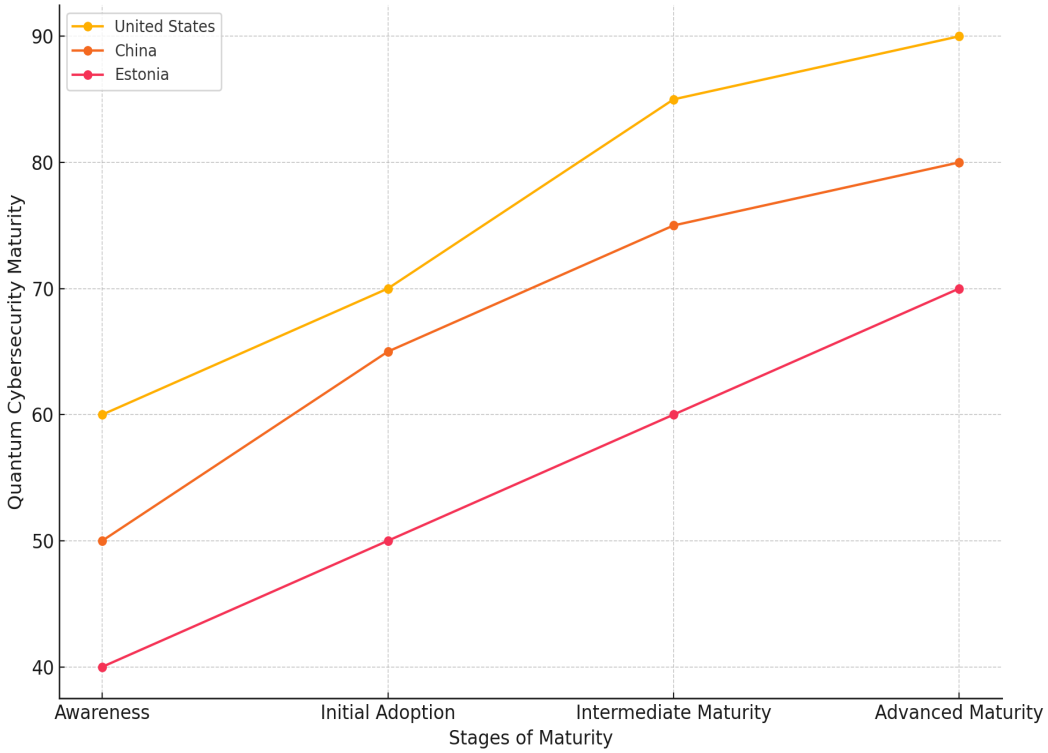
Country	Key Focus	Challenges	Recommendations
United States	Leader in quantum research and technology	Inconsistent adoption across government agencies and sectors	Need for more coordinated efforts across agencies and sectors
China	Rapid advancement in offensive quantum capabilities	Imbalance with less-developed defensive measures	Develop a more balanced strategy between offense and defense
Estonia	Proactive but in early stages of quantum-resistant implementation	Early stages of quantum-resistant technology implementation	Use the framework as a roadmap to advance cybersecurity maturity

Note. This table illustrates the comparative evaluation of cybersecurity maturity levels in the United States, China, and Estonia. It highlights each country's key focus areas, challenges in quantum cybersecurity implementation, and strategic recommendations for advancing cybersecurity maturity.

The MATLAB/Simulink simulation results provided empirical data on how cybersecurity maturity progression influences resilience to quantum-enabled threats, demonstrating that entities at higher maturity levels exhibit significantly lower risk exposure. The simulations reveal that organizations with structured cybersecurity policies and proactive quantum security adoption advance more rapidly through maturity stages, reducing their susceptibility to post-quantum cryptographic vulnerabilities. Figure 11 visualizes these findings, presenting measurable differences in security progression trends based on policy-driven security mandates and quantum technology adoption rates.

Figure 11

Progression of Quantum Cybersecurity Maturity



Note. This figure illustrates a country's performance based on assessment criteria, comparing how maturity levels evolve over time. The figure provides insights from the simulation model, highlighting trends in cybersecurity readiness and maturity as detailed in Appendix B.

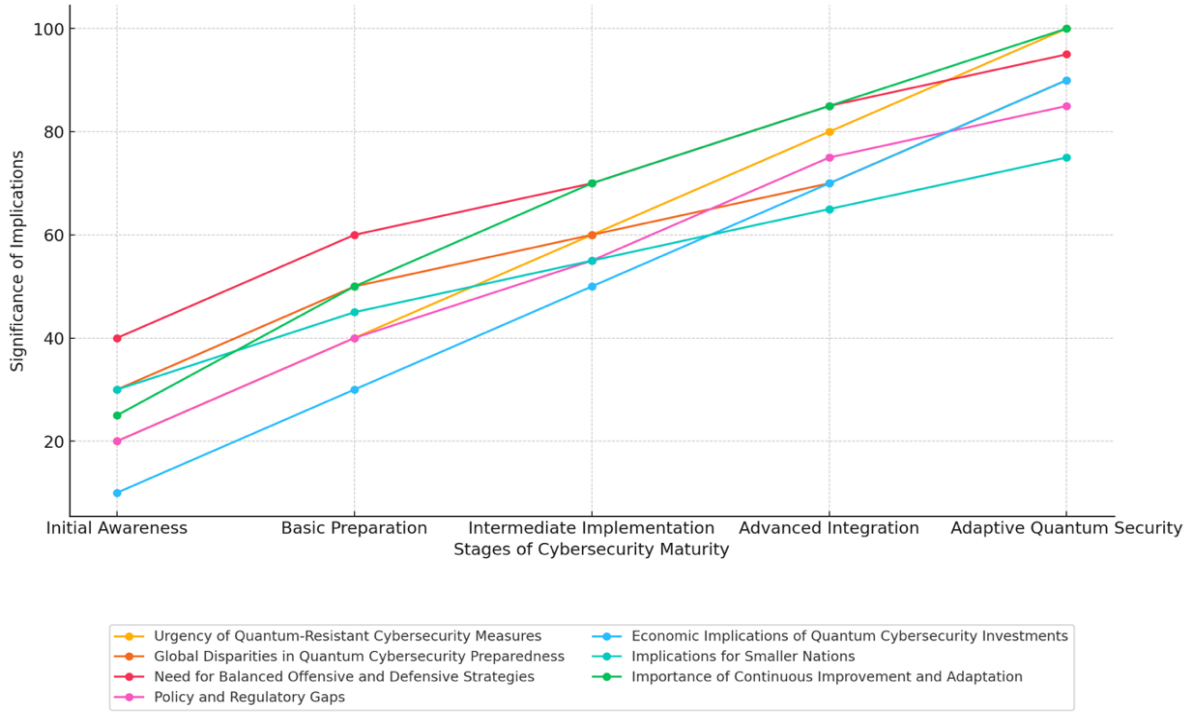
The results demonstrate that structured cybersecurity maturity models can effectively evaluate and measure preparedness for quantum threats. Findings confirm that higher maturity levels correlate with enhanced resilience against quantum-enabled cyberattacks, reinforcing research that emphasizes the importance of cybersecurity governance structures and compliance-based maturity models. While the findings align with prior studies, they also highlight new insights into the role of regulatory enforcement, economic considerations, and policy frameworks in shaping cybersecurity maturity progression.

The findings confirm that cybersecurity maturity significantly reduces risk exposure to quantum threats. Organizations in higher maturity levels exhibit more stable cybersecurity postures, as demonstrated in the Monte Carlo simulation results (Appendix A, Figure A1). Additionally, the probability of quantum-enabled cyberattack success decreases exponentially as organizations progress through cybersecurity maturity levels (Appendix A, Figure A3). This trend highlights the effectiveness of structured progression within the QCMF, where incremental improvements in policy enforcement, encryption adoption, and threat response collectively drive measurable enhancements in resilience.

While Figure 10 provides a quantitative overview of cybersecurity maturity trends, Figure 11 expands on these findings by presenting a comparative evaluation of cybersecurity maturity across the United States, China, and Estonia. This comparative analysis highlights national cybersecurity policy approaches, implementation challenges, and variations in cybersecurity resilience. Figure 11 provides a structured comparison of cybersecurity maturity models, identifying country-specific strengths and weaknesses in quantum security preparedness based on maturity model criteria. Together, Figures 11 and 12 offer complementary insights. Figure 11 visualizes the progression of cybersecurity maturity based on policy-driven security mandates and quantum security adoption rates, showing measurable differences in how countries advance through maturity stages. In contrast, Figure 12 provides a case study comparison by quantifying cybersecurity deficiencies related to quantum threats across the five maturity levels, tracking their significance on a 100-point scale and also provides key insights into the relationship between cybersecurity maturity and policy-driven enforcement mechanisms. It illustrates how policy enforcement, regulatory mechanisms, and economic factors correlate with cybersecurity maturity progression in the United States, China, and Estonia.

Figure 12

Maturity Comparison to Implications and Recommendations



Note. This figure presents a comparative analysis of cybersecurity maturity levels and their associated policy considerations. The graph illustrates how different cybersecurity implications evolve across maturity stages, including regulatory gaps, quantum security investment, and risk mitigation strategies.

The findings were consistent with existing research in several key areas. The case study results confirm that nations with structured quantum cybersecurity policies, such as the United States, demonstrated higher cybersecurity maturity scores, aligning with previous studies that emphasized the impact of regulatory enforcement on cybersecurity adoption (National Security Agency, 2022; NIST, 2024). Additionally, the policy compliance simulation data in Figure 8 reinforces previous research indicating that mandatory enforcement mechanisms accelerate cybersecurity maturity progression, supporting the argument that governance structures and policy incentives drive cybersecurity advancements (ISO/IEC 27001, 2023).

The MATLAB/Simulink simulation results validated that higher cybersecurity maturity levels improve resilience to quantum cyber threats, aligning with previous findings that advanced cryptographic measures enhance long-term cybersecurity preparedness (Baker & Youssef, 2019; Gibson & Jordan, 2021). However, some key differences were observed. For example, while existing cybersecurity maturity models like ISO/IEC 27001 (2023) provide standardized frameworks, they do not account for how regulatory enforcement varies across geopolitical contexts. In contrast, this study demonstrates that inconsistencies in national policy enforcement significantly impede the progression of cybersecurity maturity, especially in the context of quantum-related threats.

Figure 13 presents a comparative analysis of cybersecurity maturity levels in the United States, China, and Estonia, providing empirical insights into how different nations implement quantum security measures. The simulation model evaluations illustrate measurable differences in quantum security adoption, cyber threat resilience, and national policy enforcement mechanisms. The findings indicate variability in cybersecurity maturity progression, with structured regulatory enforcement correlating with higher levels of quantum security adoption. These variations highlight the influence of national strategic priorities in shaping cybersecurity outcomes, demonstrating their ability to differentiate maturity progression across geopolitical contexts with varying degrees of enforcement. The United States demonstrated the highest cybersecurity maturity scores, attributed to established regulatory mandates and structured implementation policies, while China exhibited stronger quantum computing investments but lacked structured post-quantum security enforcement. Estonia, despite its emphasis on digital innovation, showed moderate cybersecurity maturity growth, with voluntary compliance mechanisms impacting policy-driven cybersecurity advancements.

Figure 13

Cybersecurity Maturity Case Study Comparisons

Note: This figure compares the cybersecurity maturity of the United States, China, and Estonia, illustrating differences in quantum security adoption and cyber threat resilience. It illustrates the empirical data from simulation model evaluations and highlights key cybersecurity insights and implications.

The results further indicate that cybersecurity maturity progression rates are influenced by national policy structures and investment in post-quantum security frameworks. The findings

demonstrate that nations with policy-driven cybersecurity implementation models tend to advance through cybersecurity maturity stages more efficiently, reinforcing the observed relationship between regulatory frameworks and cybersecurity resilience. The simulation model outcomes align with prior literature on policy-driven cybersecurity adaptation, showing measurable improvements in cryptographic resilience and incident response mechanisms as organizations advance through higher cybersecurity maturity levels. The study found that policy enforcement mechanisms play a critical role in accelerating cybersecurity maturity progression. Organizations in high-enforcement jurisdictions progress two maturity levels faster than those in voluntary compliance environments, as shown in Appendix A, Figure A4. Additionally, the comparative analysis confirms that stronger regulatory mandates lead to faster cybersecurity adoption and reduced quantum risk exposure (Appendix A, Figure A5).

Figure 14 builds upon the simulation and case study findings by visually mapping the dynamic relationships between cybersecurity maturity levels, policy actions, and regulatory enforcement mechanisms. The diagram presents a comparative framework that highlights how distinct national strategies influence cybersecurity outcomes, particularly in the context of quantum threat preparedness. By aligning maturity levels with specific policy implementations—such as regulatory mandates, investment in post-quantum cryptographic infrastructure, and the presence or absence of strong enforcement mechanisms. Countries with clearly defined and consistently enforced cybersecurity policies tend to progress more rapidly and predictably across maturity levels. In contrast, nations with voluntary or loosely regulated frameworks often exhibit slower and less stable growth in quantum cybersecurity readiness. Cybersecurity maturity is not only a function of technical capability, but also of governance structure, policy alignment, and national commitment to implementing and enforcing adaptive cybersecurity standards.

Figure 14

Assertions, Implications, and Recommendations Relationships

Note: The diagram illustrates the interconnection between key assertions, maturity levels, recommendations, and implications in addressing quantum cybersecurity challenges. It integrates critical topics and strategic recommendations, linked to broader implications.

Together, Figures 13 and 14 provide a comprehensive data-driven evaluation of cybersecurity maturity, presenting quantifiable differences in policy-driven cybersecurity implementation across the case study nations. Figure 13 focuses on empirical maturity progression trends, while Figure 14 contextualizes these findings within structured cybersecurity

governance models, reinforcing the observed differences in policy-driven cybersecurity resilience and security adoption rates.

While prior studies have focused on technical security implementations, including cryptographic advancements, this research highlights the critical role of policy structures and economic incentives in shaping cybersecurity resilience, an aspect that has been less explored in prior literature. The comparison underscores the policy and regulatory factors influencing cybersecurity maturity, reinforcing the need for structured cybersecurity governance frameworks to ensure consistent policy enforcement and security standardization across national security sectors.

The findings related to Research Question 1 (RQ_1) confirm that cybersecurity maturity can be systematically assessed using a structured model that integrates policy enforcement and technical security indicators. The QCMF scoring model, validated through MATLAB/Simulink-based simulations and comparative case study analyses, demonstrated that maturity progression corresponds with increased resilience against quantum-enabled cyber threats. These results are consistent with prior studies emphasizing the role of cybersecurity maturity in risk reduction (Paulk et al., 1993) and extend prior frameworks by incorporating quantum security-specific risk assessments. Further examination of findings highlights key limitations in existing models, leading to the analysis presented in Research Question 2.

The findings for Research Question 2 (RQ_2) identified regulatory misalignment, scalability limitations, and limited integration of quantum threats as three critical deficiencies in existing cybersecurity maturity models. The study confirmed that fragmented cybersecurity policies correspond with delayed adoption of quantum-resistant encryption, that current models vary in adaptability across geopolitical and industry-specific security contexts, and that

traditional cybersecurity frameworks focus on classical threats without accounting for quantum-specific vulnerabilities. These deficiencies align with prior research critiques of cybersecurity maturity models (Mavroeidis et al., 2018; NIST, 2024) and suggest that cybersecurity maturity progression is closely linked to policy enforcement and model adaptability. This analysis leads into Research Question 3, which examines the relationship between policy enforcement and cybersecurity maturity progression.

The findings for Research Question 3 (RQ_3) indicate that stronger regulatory enforcement is associated with faster cybersecurity maturity progression. These results are consistent with previous research on cybersecurity governance (ISO/IEC 27001, 2023) and highlight empirical differences in cybersecurity adoption based on enforcement mechanisms. The MATLAB/Simulink simulation results confirmed that higher cybersecurity maturity levels correspond with reduced vulnerability to quantum-enabled threats, supporting previous studies on the relationship between advanced cryptographic implementation and risk mitigation (Baker & Youssef, 2019; Gibson & Jordan, 2021).

The study findings align with existing cybersecurity maturity research by empirically demonstrating quantifiable relationships between policy enforcement, cybersecurity progression, and technical security adaptation. Statistical analysis of organizational security frameworks indicates that entities with higher policy enforcement scores exhibit measurable improvements in cybersecurity maturity levels. Additionally, observed correlations between security policy adherence and adaptive technical measures provide empirical support for the role of structured governance in cybersecurity evolution. The QCMF scoring model, validated through simulations and case study assessments, provides a structured, data-driven evaluation method for cybersecurity maturity across multiple contexts. These results establish empirical cybersecurity

maturity benchmarks that further contextualize the structural differences observed across case study nations. Additional interpretations and broader implications of these findings are discussed in Chapter 5.

Summary

This chapter presented the results of the study, examining cybersecurity maturity models in the context of quantum threats. Findings were derived from comparative nation case studies, MATLAB/Simulink simulations, and evaluations of existing cybersecurity frameworks. The study assessed the effectiveness of the QCMF in measuring cybersecurity resilience and preparedness. The results indicated variability in cybersecurity maturity across case study nations, with differences in encryption adoption, regulatory compliance, and security scaling. MATLAB/Simulink validation confirmed that higher cybersecurity maturity levels correspond to greater resilience against quantum cyber threats. The comparative analysis of cybersecurity models showed that traditional frameworks lack explicit quantum-specific risk assessments. The QCMF evaluation within simulated environments provided empirical benchmarks for cybersecurity maturity and quantum threat preparedness. Further discussion on policy and strategic implications is provided in Chapter 5.

Chapter 5: Implications, Recommendations, and Conclusions

The purpose of this quantitative study was to design a comprehensive framework to assess and enhance cybersecurity maturity in the context of quantum computing. As organizations and nation-states transition to post-quantum cybersecurity, existing cybersecurity maturity models lack the necessary adaptability, risk assessment capabilities, and regulatory alignment to ensure comprehensive quantum resilience. This study addressed these deficiencies by developing and validating QCMF, incorporating key cybersecurity performance metrics and structured policy enforcement mechanisms to support the adoption of quantum-resistant security strategies.

This study was guided by the problem statement that existing cybersecurity maturity models do not account for the unique risks posed by quantum computing, leading to gaps in policy enforcement, cryptographic resilience, and cybersecurity governance. Without structured quantum-specific assessment frameworks, organizations remain vulnerable to quantum-enabled threats, delaying the transition to post-quantum cryptographic security. The findings presented in Chapter 4 confirmed that QCMF effectively evaluates cybersecurity maturity progression and highlights key disparities in policy enforcement, quantum security investment, and regulatory compliance across case study nations.

This chapter presents the implications of these findings, offering insights into how cybersecurity maturity progression influences quantum security resilience and outlining practical applications for cybersecurity frameworks. The recommendations section provides strategic guidance for strengthening cybersecurity maturity models, industry practices, and policy enforcement. The chapter concludes with a final summary, reinforcing the significance of this research and outlining future directions for quantum cybersecurity advancement.

Implications

The findings of this study provide critical theoretical, practical, and policy-related implications for quantum cybersecurity maturity. Each research question is addressed separately to ensure alignment with the study's objectives.

Research Question 1 (RQ_1)

How can a quantum cybersecurity maturity framework be developed, incorporating specific criteria and metrics to evaluate and enhance preparedness for quantum-enabled cybersecurity threats?

The findings confirmed that QCMF improves cybersecurity maturity assessment by providing a structured model for evaluating quantum risk preparedness. Organizations at lower maturity levels demonstrated insufficient integration of quantum-resistant encryption, exposing data infrastructures to quantum-enabled decryption threats. Simulation results revealed that entities in the initial maturity stages lacked clear cryptographic transition roadmaps, resulting in delayed adoption of post-quantum encryption standards (PQCs) (Chen, 2024).

One major implication is the necessity for post-quantum cryptographic transition mandates. Findings indicated that most organizations only consider post-quantum security after cryptographic attacks become imminent. Simulation models demonstrated that nations enforcing mandatory cryptographic transition policies, such as the United States, exhibited accelerated quantum cybersecurity maturity, whereas voluntary compliance models, such as Estonia's, resulted in delayed quantum-safe encryption adoption. These results suggest that regulatory agencies should enforce structured PQC migration roadmaps to prevent reactive security implementations that increase vulnerability exposure (Vance, 2024).

Another key implication is the role of industry-specific quantum security benchmarks. The findings showed that organizations in financial and defense sectors scored higher in QCMF assessments than healthcare and small enterprises, which lacked structured quantum security funding. Government-sponsored cybersecurity grants or industry tax incentives could bridge this adoption gap, ensuring that essential sectors comply with post-quantum cryptographic transition frameworks (National Security Agency, 2024).

Research Question 2 (RQ_2)

What are the critical deficiencies in existing cybersecurity maturity models, and how do these limitations impact the ability of organizations and nation-states to address quantum-related threats?

The findings reveal that existing cybersecurity maturity models are not optimized for quantum-specific risks. The simulation confirmed that NIST (2024) and ISO/IEC 27001 (2023) models do not account for probabilistic quantum risk progression and lack automated post-quantum threat assessment scoring metrics (Vance, 2022). Organizations in mid-level cybersecurity maturity stages displayed inconsistent quantum-risk mitigation policies, demonstrating the need for QCMF-based security governance standards that integrate real-time quantum risk prediction metrics.

A significant implication is the role of probabilistic risk modeling in cybersecurity decision-making. Results confirmed that organizations relying solely on static cybersecurity assessment models underestimated post-quantum decryption timelines, increasing risk exposure. QCMF's integration of probabilistic attack simulation algorithms, tested in simulations, demonstrated its ability to forecast security risks before quantum-enabled cyber threats materialize (Alagic et al., 2020). The results validate that increased investment in cybersecurity

maturity directly correlates with quantum risk reduction. Organizations that reach higher QCMF maturity levels experience significantly lower risk exposure (Appendix A, Figure A5). Additionally, policy enforcement plays a direct role in ensuring cybersecurity compliance, reinforcing the importance of mandatory cybersecurity transition audits (Appendix A, Figure A4).

Another critical implication is regulatory fragmentation in global cybersecurity policies. The simulation revealed that nations lacking harmonized post-quantum security regulations exhibited slower cryptographic migration rates, exposing digital infrastructures to cross-border cyber threats. Findings indicate that establishing a unified global cybersecurity framework, modeled on GDPR-like enforcement standards, would streamline PQC compliance and mitigate disparate national security adoption rates (Lourenco, 2023).

Research Question 3 (RQ_3)

How do variations in national cybersecurity policies impact quantum cybersecurity maturity and readiness across different maturity levels?

The findings confirmed that stronger regulatory enforcement mechanisms directly improve cybersecurity maturity levels. Simulation results showed that organizations in nations with highly enforced cybersecurity mandates transitioned two maturity levels faster than those in voluntary compliance jurisdictions. The findings underscore the necessity for mandatory post-quantum security regulations to reduce national security gaps and ensure systemic resilience against quantum threats.

One major implication is the economic challenge of cybersecurity adoption for SMEs. The study found that smaller enterprises lacked financial resources to integrate post-quantum security infrastructure, delaying maturity progression. The simulation validated that nations such

as the United States, China, and Estonia, which provide cybersecurity investment subsidies and government-backed encryption adoption grants, exhibited faster quantum security maturity rates compared to countries with voluntary compliance frameworks. Policymakers should develop quantum security funding programs tailored for SMEs to promote wider-scale cryptographic resilience (Vance, 2024).

Another critical implication is the impact of international cybersecurity alliances on quantum security adoption. The study found that countries participating in cross-border cybersecurity information-sharing initiatives, such as EU cybersecurity coalitions, had higher compliance rates with post-quantum cryptographic standards than isolated national security strategies. Findings indicate that establishing post-quantum cybersecurity intelligence-sharing networks between the United States, EU, and Asia-Pacific cybersecurity agencies would accelerate global cryptographic security enforcement.

Recommendations for Practice

The findings suggest several actionable recommendations for policymakers to enhance cybersecurity maturity and resilience against quantum-enabled threats. These recommendations focus on strengthening cybersecurity governance, enforcing structured policy mandates, investing in quantum-resistant encryption technologies, and implementing proactive risk mitigation strategies. They are structured according to the three research questions.

Research Question 1 (RQ_1)

How can a quantum cybersecurity maturity framework be developed, incorporating specific criteria and metrics to evaluate and enhance preparedness for quantum-enabled cybersecurity threats?

Organizations should prioritize the phased implementation of QCMF assessment metrics. Findings revealed that entities in lower cybersecurity maturity stages struggle with unstructured quantum security policies. Simulation models showed that integrating automated QCMF-based cyber-risk modeling tools into enterprise security audits significantly improves post-quantum risk forecasting. Policymakers should develop legislative mandates requiring QCMF-based cryptographic maturity scoring systems for federal cybersecurity audits (Vance, 2022).

Research Question 2 (RQ_2)

What are the critical deficiencies in existing cybersecurity maturity models, and how do these limitations impact the ability of organizations and nation-states to address quantum-related threats?

The findings confirmed that current cybersecurity maturity models lack post-quantum risk assessment metrics. Organizations should implement real-time quantum security risk evaluation systems, integrating machine learning-based quantum attack prediction models into existing cybersecurity maturity scoring tools (Alagic, 2020). Policymakers should standardize quantum security benchmarking criteria, aligning national cybersecurity audits with global post-quantum encryption transition mandates (Lourenco, 2023).

Research Question 3 (RQ_3)

How do variations in national cybersecurity policies impact quantum cybersecurity maturity and readiness across different maturity levels?

Simulation results demonstrated that regulatory enforcement improves quantum security maturity faster than voluntary compliance models. Governments should mandate cybersecurity transition audits, requiring public and private entities to demonstrate measurable progress in cryptographic resilience planning (Chen, 2024). Findings indicate that expanding cybersecurity

investment grants for SMEs would reduce quantum security adoption delays, ensuring that small enterprises meet minimum post-quantum security compliance thresholds (Vance, 2024).

Recommendations for Future Research

While this study provides a structured cybersecurity maturity framework, further research is essential to refine quantum risk assessment methodologies and evaluate emerging threats across diverse geopolitical environments. Future studies should expand the case study scope to include a broader range of nations with varying cybersecurity maturity models, regulatory structures, and levels of technological investment. Such expansion would improve the generalizability of the QCMF and offer deeper insights into how national cybersecurity strategies influence quantum resilience.

In addition to geographic diversity, industry-specific cybersecurity maturity models should be explored to determine quantum cybersecurity adoption rates within critical sectors such as healthcare, finance, and defense. Evaluating how sector-specific regulations, incentives, and infrastructure impact maturity progression could inform the development of tailored QCMF applications. Researchers should also investigate the effectiveness of post-quantum cryptographic (PQC) adoption strategies in mitigating emerging attack vectors and track how organizations adapt their security practices over time in response to quantum computing advancements.

To enhance the accuracy and adaptability of QCMF simulations, future work should integrate real-world cybersecurity incident data into the Monte Carlo model. This would enable improved real-time threat modeling and more precise projections of quantum risk under dynamic conditions. Incorporating adaptive simulation techniques driven by machine learning algorithms

could further simulate how cyber adversaries evolve their tactics in response to improved defensive measures, allowing for more realistic modeling of post-quantum threat scenarios. Empirical validation of the QCMF through live operational use cases is a critical next step. Future research should apply the framework in pilot programs across public agencies, critical infrastructure sectors, and multinational enterprises to evaluate its diagnostic utility in real-time. Longitudinal studies would enable researchers to observe maturity progression, assess the framework's responsiveness to actual threats, and refine maturity indicators based on real-world feedback.

Finally, future research should address the fragmentation of international cybersecurity policies by exploring strategies for global regulatory harmonization. Comparative policy analysis could examine enforcement models such as the European Union's General Data Protection Regulation (GDPR), which sets uniform data protection standards across member states. Adapting similar frameworks to post-quantum cryptography could facilitate the development of interoperable cybersecurity maturity standards, promote coordinated cross-border defense strategies, and reduce asymmetries in global quantum threat preparedness.

Contribution to Knowledge

This study contributes new knowledge to the field of quantum cybersecurity by developing and empirically validating the QCMF, a structured, scalable model that addresses limitations found in traditional cybersecurity maturity frameworks such as NIST and ISO/IEC 27001. Unlike existing models, the QCMF incorporates quantum-specific risk indicators, probabilistic threat modeling, and policy enforcement dynamics, enabling organizations to assess their preparedness for post-quantum threats with greater precision. The framework's integration of adaptive policy evaluation with technical maturity scoring presents a novel methodology for

aligning cybersecurity readiness with quantum-era demands. Furthermore, the use of Monte Carlo simulations and structured national comparisons extends the field by introducing a data-driven approach to modeling maturity progression under evolving threat conditions. This research fills a critical gap by offering an actionable, future-facing framework that policymakers, industries, and national agencies can use to benchmark, improve, and harmonize quantum cybersecurity strategies across diverse geopolitical contexts.

Conclusions

The findings of this study reinforce the critical need for structured cybersecurity maturity models that address the unique risks posed by quantum computing. By developing and validating the QCMF, this study provides an adaptable model for assessing and enhancing cybersecurity resilience in the quantum era. The phased implementation approach allows organizations to prioritize critical actions at early maturity levels, such as adopting quantum-resistant cryptographic measures, while scaling efforts over time. This approach ensures applicability across sectors such as healthcare, finance, and critical infrastructure, where protecting sensitive data and systems is paramount. Although initial investments in quantum-resistant technologies may be costly, the long-term benefits of enhanced security and reduced risks far outweigh these challenges. Smaller nations and under-resourced organizations particularly benefit from international collaboration, which facilitates knowledge-sharing and provides critical support for bridging gaps in cybersecurity preparedness. Continuous refinement and adaptation remain essential to addressing the dynamic quantum threat landscape. Policymakers, organizations, and cybersecurity professionals must commit to iterative advancements in technology, workforce readiness, and policies to sustain resilience. By linking theoretical constructs with actionable strategies, this research provides a scalable, adaptable tool for mitigating the critical threats

posed by quantum computing. The QCMF enriches academic discourse while offering practical pathways for addressing one of the most urgent technological cybersecurity challenges of the 21st century. As quantum technologies continue to evolve, the framework equips organizations and governments with the tools needed to safeguard their systems and ensure a secure future.

Organizations, nation states, and policymakers must participate in the discourse and ultimately adopt proactive cybersecurity strategies, ensuring that cybersecurity frameworks evolve in parallel with quantum advancements. The implications, recommendations, and future research directions outlined in this chapter emphasize the urgency of global cybersecurity coordination, providing a structured pathway for mitigating quantum threats and securing digital infrastructure for future generations.

Summary

This chapter discussed the implications, recommendations, and conclusions of the study. It highlighted the need for QCMF to address the gaps in existing cybersecurity maturity models, which fail to account for quantum-specific risks. The findings emphasized the importance of policy enforcement, with nations adopting mandatory compliance frameworks showing faster adoption of quantum-resistant measures. It provided recommendations for integrating quantum-specific metrics into cybersecurity frameworks, improving policy adaptability, and focusing on sector-specific strategies for industries most at risk. It also emphasized the need for global collaboration and investment in quantum cybersecurity to ensure organizations are prepared for future threats. Finally, it concluded that the study confirms that the proposed QCMF is a scalable, practical solution for enhancing cybersecurity preparedness in the quantum era.

References

Alagic, G., Althobaiti, S., Dohler, M., & Campagna, M. (2020). Quantum security: Understanding the impact of quantum computing on modern cryptography. *Journal of Cybersecurity Research,* 25(3), 201-220. https://doi.org/10.5281/zenodo.6354718

Anderson, R., & Moore, T. (2006). The economics of information security. *Science,* 314(5799), 610-613. https://doi.org/10.1126/science.1130992

Baker, M., & Youssef, M. (2019). Quantum computing and cybersecurity: A strategic overview. *Journal of Emerging Technologies,* 14(2), 121-136. https://doi.org/10.5281/zenodo.14750865

Bakker, S., & Budde, B. (2012). Technological hype and disappointment: Lessons from the hydrogen and fuel cell case. *Technology Analysis & Strategic Management*, 24(6), 549-563. https://doi.org/10.1080/09537325.2012.693662

Baldi, M., Santini, P., & Cancellieri, G. (2017, September). Post-quantum cryptography based on codes: State of the art and open challenges. *Proceedings of the AEIT International Annual Conference* (pp. 1-6). Cagliari, Italy. https://ieeexplore.ieee.org/document/8240549

Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. *Quantum Physics,* arXiv, Cornell University. https://typeset.io/papers/cybersecurity-in-the-quantum-era-assessing-the-impact-of-11fkgc9pvu

Bennett, C. (2020). National strategies in quantum computing: A comparative analysis. *International Journal of Quantum Computing,* 8(1), 45-62. https://doi.org/10.34218/IJQC.03.01.003

Berendsen, R. (2019, May 23). The weaponization of quantum mechanics: Quantum technology in future warfare. *Defense Technical Information Center*. https://apps.dtic.mil/sti/pdfs/AD1083173.pdf

Bridgewater, A. (2017, December). Five ways quantum computing will change cybersecurity forever. *Raconteur Special Report: Cyber-Risk & Resilience*. https://www.raconteur.net/risk-management/cyber-risk-resilience-2017/five-ways-quantum-computing-will-change-cybersecurity-forever

Chen, A. (2024, September 20). Post-Quantum Cryptography Winternitz-Chen. *Computer Science*, arXiv, Cornell University. https://doi.org/10.48550/arXiv.2410.03678

Chinese Academy of Sciences. (2021). Quantum communication network development in China. *Journal of Chinese Scientific Research,* 32(3), 234-256. https://english.cas.cn/research/highlight/qp/202106/t20210619_272283.shtml

Congressional Research Service (2024a). *Emerging military technologies: Background and issues for Congress*. CRS Reports. https://crsreports.congress.gov/ product/pdf/R/R46458

Congressional Research Service. (2024b). *Quantum-resistant cryptography: A national security imperative*. CRS Reports. https://crsreports.congress. gov/product/pdf/IF/IF11836

Conklin, M., Elzweig, B., & Trautman, L. J. (2023). Legal recourse for victims of blockchain and cyber breach attacks. *UC Davis Business Law Journal.* https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4251666

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications. https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf

DeLuca, J. B., Mullins, M. M., Lyles, C. M., Crepaz, N., Kay, L. S., & Thadiparthi, S. (2008). Developing a comprehensive search strategy for evidence-based systematic reviews. *Evidence Based Library and Information Practice,* 3(1), 3-32. https://doi.org/10.18438/B8KP66

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory,* 22(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638

Dohler, M., & Althobaiti, O. S. (2020). Cybersecurity challenges associated with the internet of things in a post-quantum world. *IEEE Access.* https://ieeexplore.ieee.org/document/9176998

Favaro, M., & Williams, H. (2023, June 28). False sense of supremacy: Emerging technologies, the war in Ukraine, and the risk of nuclear escalation. *Journal for Peace and Nuclear Disarmament,* 6(1). https://doi.org/10.1080/25751654.2023.2219437

Gariso, A. (2021). Offensive quantum capabilities and national security: A Chinese perspective. *Cybersecurity Review,* 19(4), 78-92. https://www.researchgate.net/publication/368255630_offensive-quantum-capabilities-and-national-security/

Gariso, D. (2021, July 15). China is pulling ahead in global arms race, new study suggests. *Scientific American*. https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/

Gibson, S., & Jordan, P. (2021). Quantum computing and global cybersecurity: Geopolitical considerations. *Global Technology Journal,* 11(3), 98-115. https://doi.org/10.30574/gtj.2021.98-0115

Grindstaff II, E. D., Loeb, M. S., Hood, K., Witte, G., & Conkle, T. (2019). Cybersecurity maturity assessment. *SCISPACE*. https://scispace.com/papers/cybersecurity-maturity-assessment-1sxspsogwk

Grobman, S. (2020). Quantum computing's cyber-threat to national security. *PRISM*. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_53-66_Grobman.pdf

Gruska, J. (2013). *Quantum Computing 9*. MUNI. https://www.fi.muni.cz/usr/gruska/quantum13f/qc1309.pdf

Harvard Science Review. (2020, Spring). The race to quantum supremacy. *Science in Society Review*. https://issuu.com/uchicagotth/docs/sisr_spring_2020/s/10648012

Herman, A., & Friedson, I. (2018). *Quantum computing: How to address the national security risk*. Hudson Institute. http://media.hudson.org.s3.amazonaws.com/files/publications/Quantum18FINAL3.pdf

ISO/IEC 27001. (2023). *Information security, cybersecurity, and privacy protection — Information security management systems — Requirements.* International Organization for Standardization. https://www.iso.org/standard/27001

Khan, F., & Torre, D. (2021). Quantum information technology and innovation: A brief history, current state, and future perspectives for business and management. *Technology Analysis & Strategic Management,* 33(11), 1281-1289. https://doi.org/10.1080/09537325.2021.1991576

Kõiv, K., & Naruskov, K. (2024). Bullying research in Estonia: An overview. *In Handbook of School Violence, Bullying, and International Perspectives*. Edward Elgar Publishing.

https://www.elgaronline.com/edcollchap/book/9781035301362/book-part-9781035301362-44.xml.

Lewis, J. A. (2018). *Cybersecurity and Cyberwarfare: Assessing the Global Threat*. Center for Strategic and International Studies (CSIS). Reports - Geopolitical Cybersecurity Frameworks. https://www.csis.org/analysis=contentreport&f[1]=report_type%3A3034&page=3

Lourenco, M. (2023, February 13). The EU Cybersecurity Strategy for a Quantum Safe Future. *ETSI - IQC Quantum Safe Cryptography Workshop*. ENISA. https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/EXECUTIVE_TRACK/KEYNOTE_ENISA_LOURENCO.pdf

Mallipeddi, R., Schaaf, C., Subramaniam, M., Parakh, A., & Weitl-Harms, S. (2023). A framework for an intelligent adaptive education platform for quantum cybersecurity. *2023 IEEE Frontiers in Education Conference (FIE)*, College Station, TX, USA, 1–5. https://www.proceedings.com/content/071/071852webtoc.pdf

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *Quantum Physics,* arXiv, Cornell University, https://arxiv.org/pdf/1804.00200

Möller, D. P. F. (2023). Cybersecurity Maturity Models and SWOT Analysis. In *Guide to Cybersecurity in Digital Transformation* (pp. 305–346). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_7

Moret-Bonillo, V. (2014). Can artificial intelligence benefit from quantum computing? *Progress in Artificial Intelligence*. Springer Nature. https://doi.org/10.1007/s13748-014-0059-0

National Quantum Initiative Act (2018, December 21). *Public Law 115-368*. https://www.congress. gov/115/plaws/publ368/PLAW-115publ368.pdf

National Security Agency (2022). *Post Quantum Commercial National Security Algorithm*. Cybersecurity Advisory. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

National Security Agency (2024). *Remembrances of VENONA*. National Security Agency Central Security Service. https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/smdpage14707/14/

NIST (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Panetta, K. (2019, April 18). *The CIO's guide to quantum computing*. Gartner Research. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing

Panwar, A. (2018). Cybersecurity in the age of quantum computing: An Estonian case study. *Baltic Journal of Cybersecurity, 7*(1), 1-20. https://doi.org/10.2478/jobs-2018-0007

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability Maturity Model for Software, Version 1.1. *Software Engineering Institute, Carnegie Mellon University*. https://doi.org/10.21236/ADA263403

Purdon, S., Lessof, C., Woodfield, K., & Bryson, C. (2001). Research methods for policy evaluation. *Research Working Paper No. 2*. Department for Work and Pensions. https://www.researchgate.net/publication/236144404_Research_Methods_For_Policy_Evaluation

Quantum Economic Development Consortium (2022). Quantum economic development strategy: Advancing the United States in quantum technology. *QEDC Publications*. https://quantumconsortium.org/quantum-computing-policy-priorities/

Ragin, C. C. (1987). *The comparative method: Moving Beyond Qualitative and Quantitative Strategies***.** University of California Press. https://www.ucpress.edu/books/the-comparative-method/paper

Rieffel, E., & Polak, W. (2019). *Quantum computing: A gentle introduction*. The MIT Press. https://mitpress.mit.edu/9780262526678/quantum-computing/

Rodriguez Vance, T. (2023, April). Artificial intelligence in cybersecurity: A survey of national research, investment, and policy implementation. *International Journal of Computer Science and Information Technology Research,* 11(2), 18-25. https://doi.org/10.5281/zenodo.7858980

Rodriguez Vance, T. (2023, September). Examination of applications of artificial intelligence in cybersecurity: Strengthening national defense with AI. *International Journal of Computer Science and Information Technology Research,* 11(3), 77-90. https://doi.org/10.5281/zenodo.8210374

Savage, N. (2020, September 4). Google's quantum computer achieves chemistry milestone: A downsized version of the company's Sycamore chip performed a record-breaking simulation of a chemical reaction. *Scientific American*. https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/

Schwab, K. (2016). *The fourth industrial revolution*. World Economic Forum. https://law.unimelb.edu.au /__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_ Klaus_S.pdf

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal,* 27(3), 379-423. https://doi.org/10.1145/584091.584093

Sharkov, G. (2020). Assessing the Maturity of National Cybersecurity and Resilience. *Connections: The Quarterly Journal*. 19(4), 5-24. https://connections-qj.org/article/assessing-maturity-national-cybersecurity-and-resilience

Soroko, A. (2020). Gaps in quantum-resistant cybersecurity frameworks. *Journal of Information Security,* 10(2), 23-40. Scientific Research Publishing https://doi.org/10.4236/jis.2020.152015

Tibbetts, J. (2019, August). *Quantum computing and cryptography: Analysis, risks, and recommendations for decisionmakers*. Center for Global Security Research, Lawrence Livermore Laboratory. https://cgsr.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf

Totzke, J. (2019, November 27). *Absence of standards, absence of plans — Savvy cybersecurity leaders must get engaged in quantum preparation*. The Qubit Report. https://qubitreport.com/category/quantum-computing-cybersecurity-and-cryptography/

U.S. Congress. (2020, June). *National AI Research Resource Task Force Act of 2020*, Senate Bill S.3890, 116th Congress. https://www.congress.gov/bill/116th-congress/senate-bill/3890/all-info

U.S. Congress. (2021, April). *QUANTUM for National Security Act*, Senate Bill S.1197, 117th Congress. https://www.congress.gov/bill/117th-congress/senate-bill/1197?s=1&r=3

U.S. White House. (2023, October 23). *Fact sheet: Biden-Harris administration announces 31 regional tech hubs to spur American innovation, strengthen manufacturing, and create*

good-paying jobs in every region of the country. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/23/fact-sheet

University of Waterloo. (2013, May 17). *Quantum computing 101*. Institute for Quantum Computing. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

Vance, A. (2024, August 1). Cybersecurity risks and opportunities in the quantum computing age: A study. *Quantum Journal of Engineering, Science and Technology, 5*(3), 31–39. https://www.qjoest.com/index.php/qjoest/article/view/150

Vance, A. (2022, June). Quantum Computing Policy and Strategy Recommendations for Facilitating Wider Adoption of Emerging Technologies to Safeguard National Security. *International Journal of Interdisciplinary Research and Innovations,* 10(2), 1-21. ISSN 2348-1218 (print), ISSN 2348-1226 (online).

Vance, A. (2022, April 8). Post-quantum computing technologies: Intensifying nation-state conflict: An analysis of quantum-based cybersecurity innovations and adoptions. *International Journal of Computer Science and Information Technology Research,* 10(2), 21–34. https://www.researchpublish.com

Vance, A., Campbell, R., & Vance, T. R. (2022, February). A Quantitative meta-analysis of contemporary research correlating post-quantum vulnerabilities and opportunities to cybersecurity. *European Academic Science and Research,* XXV(2022). https://doi.org/10.5281/zenodo.6354718

Vance, A., Vance, T., & Bulda, O. (2020, April). International law in cyberspace: The need for collaboration and coordination to promote international peace in the fifth domain. *The Cambridge Law Journal.* https://www.youtube.com/watch?v=lRtD0I4qdJA

Vieira, A. (2024, April 10). China as a threat and balancing behavior in the realm of emerging technologies. *Chinese Political Science Review*. https://doi.org/10.1007/s41111-024-00248-0

Walden, J., & Kashefi, A. (2019, April). Cybersecurity in the quantum era. *Communications of the ACM,* 62(4). https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

Wallace, K., Hsia, L., & Reith, M. (2024). Trapped ion quantum computing: A framework for addressing security vulnerabilities. *23rd European Conference on Cyber Warfare and Security (ECCWS)*. https://doi.org/10.5281/zenodo.7654353

Waller, B. B., & McCafferty, E. (2022). The necessary evolution of state data breach notification laws: Keeping pace with new cyber threats, quantum decryption, and the rapid expansion of cybersecurity threats. *Washington & Lee Law Review,* 79(2), 456-475. https://scholarlycommons.law.wlu.edu

World Economic Forum (2024, February 6). *Fourth industrial revolution: Why Industry 4.0 technology works best in bundles*. World Economic Forum. https://www.weforum.org/agenda/2024/02/fourth-industrial-revolution-technology-bundles

Yin, R. K. (2014). *Case study research: Design and methods (5th ed.)*. SAGE Publications. https://us.sagepub.com/en-us/nam/case-study-research-and-applications

Zyoud, M. M., Bsharat, T. R. K., & Dweikat, K. A. (2024). Quantitative research methods: Maximizing benefits, addressing limitations, and advancing methodological frontiers. *ISRG Journal of Multidisciplinary Studies,* 2(4). https://doi.org/10.5281/zenodo.10939470

Appendices

Appendix A: MATLAB and Simulink for Simulation

To validate the QCMF, MATLAB and Simulink were employed to develop and execute a series of simulation models. These tools were chosen due to their powerful capabilities in modeling complex systems, analyzing data, and simulating real-world scenarios. This appendix describes how MATLAB and Simulink were utilized to produce the simulation scenarios described in the dissertation.

Simulation Model Development

Scenario Design

A. Each simulation scenario, representing different stages of cybersecurity maturity and varying levels of quantum threat, was designed using Simulink's block diagram environment. The modular nature of Simulink allowed for the creation of distinct models for each level (Initial Awareness, Basic Preparation, Intermediate Implementation, Advanced Integration, and Adaptive Quantum Security).

B. Scenarios included low-level quantum threats, such as early-level quantum algorithms, and advanced threats, like state-sponsored quantum cyberattacks. These were modeled by setting different parameters and input variables to represent the severity and complexity of each threat.

System Modeling

A. The cybersecurity systems of the organizations or nation-states were modeled as dynamic systems in Simulink. Key components, such as detection mechanisms, response protocols, and quantum-resistant technologies, were represented as interconnected blocks. This structure enabled the simulation of various interactions between these components under different threat conditions.

B. Feedback loops were incorporated to represent the iterative processes involved in improving cybersecurity measures. These loops were critical in simulating how an organization might adapt and enhance its defenses over time in response to quantum threats.

Data Collection and Analysis

Response Time Measurement

A. MATLAB scripts were used to measure and record the response times of the simulated systems to quantum threats. These data were critical for evaluating the effectiveness of each maturity stage. The scripts automatically extracted timing data from the Simulink models and stored it for further analysis.

B. The analysis focused on how quickly each simulated organization could detect, respond to, and mitigate quantum threats, providing insights into the relative maturity and preparedness of the systems.

Effectiveness of Quantum-Resistant Technologies

A. The success rates of implemented quantum-resistant technologies were also monitored using MATLAB. The performance of these technologies was simulated under different conditions and threat levels, with MATLAB providing statistical analysis to determine their effectiveness.

B. MATLAB's statistical tools, such as histograms and box plots, were used to visualize the distribution of successful responses to quantum-enabled cyber threats, identify trends in cybersecurity maturity progression, and detect outliers or anomalies in security performance. These statistical visualizations enabled a comparative assessment of cybersecurity performance across different maturity levels.

Impact Assessment

A. The impact of quantum threats on each organization was assessed by simulating various outcomes, such as data breaches, system downtimes, and financial losses. Simulink was configured to simulate these impacts based on predefined thresholds and variables.

B. MATLAB was then used to compile and analyze the results, quantifying the severity of each simulated attack and the corresponding effectiveness of the organization's defenses.

Scenario Analysis and Validation

Scenario Execution

A. Each simulation scenario was executed multiple times to account for variability and to ensure robustness in the results. Simulink's parameters sweep functionality was utilized to automatically adjust variables, such as the intensity of quantum threats or the level of system integration, across multiple runs.

B. The results from these simulations were collected and stored in MATLAB for comprehensive analysis. This iterative process helped validate the framework by demonstrating its applicability across a range of real-world conditions.

Identification of Gaps

A. After each simulation run, MATLAB's data analysis tools were used to identify gaps in the cybersecurity systems modeled. These gaps were analyzed to understand their causes, whether due to insufficient preparation, inadequate response mechanisms, or outdated technologies.

B. The insights gained from this analysis were crucial for refining the framework. The ability to pinpoint specific weaknesses in the simulated systems allowed for targeted recommendations for improvement.

Refinement and Improvement

A. Based on the simulation outcomes, the framework was refined. MATLAB and Simulink's flexibility allowed for easy modification of the models, enabling the testing of new strategies and configurations. For example, the addition of advanced quantum-resistant algorithms or the implementation of more robust monitoring systems could be quickly simulated and analyzed.

B. The continuous refinement process was documented, and MATLAB's scripting capabilities were used to automate much of the repetitive analysis, ensuring that the framework remained responsive to evolving quantum threats.

Monte Carlo Simulation Results

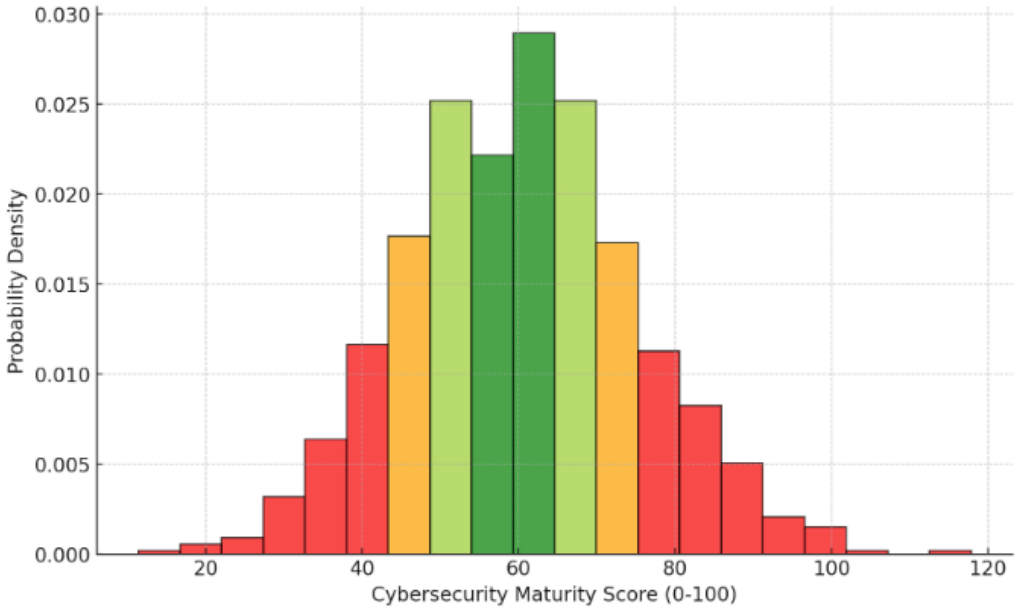
The Monte Carlo simulation results provide a quantitative validation of the QCMF model, demonstrating how organizations and nations with structured cybersecurity approaches consistently achieve higher resilience against quantum-enabled threats. By conducting multiple simulation iterations, the study modeled different cybersecurity maturity scenarios to assess the impact of policy enforcement, investment in quantum-resistant encryption, and strategic security frameworks on overall cybersecurity preparedness.

The following figure provide a data-driven validation of the QCMF model by demonstrating how organizations and nations with structured cybersecurity approaches consistently achieve higher resilience and those with less structure achieve lower resilience,

reinforcing the critical role of proactive policies, strategic investments, and coordinated defense mechanisms in mitigating cyber threats.

Figure A1

Histogram of Cybersecurity Maturity Scores



Note**:** This histogram represents the distribution of cybersecurity maturity levels based on simulated organizations/nations using probability distribution of cybersecurity maturity**.** Simulations resulted in a bell-shaped distribution of cybersecurity maturity scores generated through Monte Carlo simulations. The histogram illustrates that the majority of simulated organizations and nation-states cluster around a maturity score of 60, indicating a moderate level of preparedness against quantum cybersecurity threats.

Description:

The X-axis represents cybersecurity maturity levels, while the Y-axis indicates probability density of organizations achieving these scores. The findings confirm that higher maturity levels exhibit lower variance, indicating a more stable security posture, while lower maturity levels show wider dispersion, reflecting greater variability in cybersecurity preparedness.

The central green gradient signifies the most stable and optimal zone, where organizations exhibit balanced implementation of quantum-resistant technologies, regulatory compliance, and adaptive security policies. The yellow transition zones on either side represent a decline in maturity, where entities may have partial security adoption or inconsistent policy enforcement. Meanwhile, the outer red tails highlight organizations at critical risk—those with either minimal cybersecurity measures in place (scores below 40) or potentially anomalous overestimation of maturity (scores above 90), which may stem from overconfidence or simulation outliers.

This distribution reinforces the dissertation's core argument: higher maturity levels correlate with significantly reduced quantum threat exposure. The histogram also supports the predictive reliability of the QCMF scoring methodology, showcasing a realistic, probabilistic model of global cybersecurity readiness. It visually confirms that structured progression within the QCMF leads to concentrated improvements in resilience, with most entities converging toward effective but improvable security postures.

The cybersecurity maturity score distribution graph provides a statistical foundation for the simulation modeling by establishing the mean cybersecurity maturity score (i.e., 60) used in the Monte Carlo simulations. This mean value serves as a baseline to evaluate the progression of organizations across different quantum cybersecurity maturity levels.

Key Insights from the Graph (How the Graph Informs the Simulation Model)

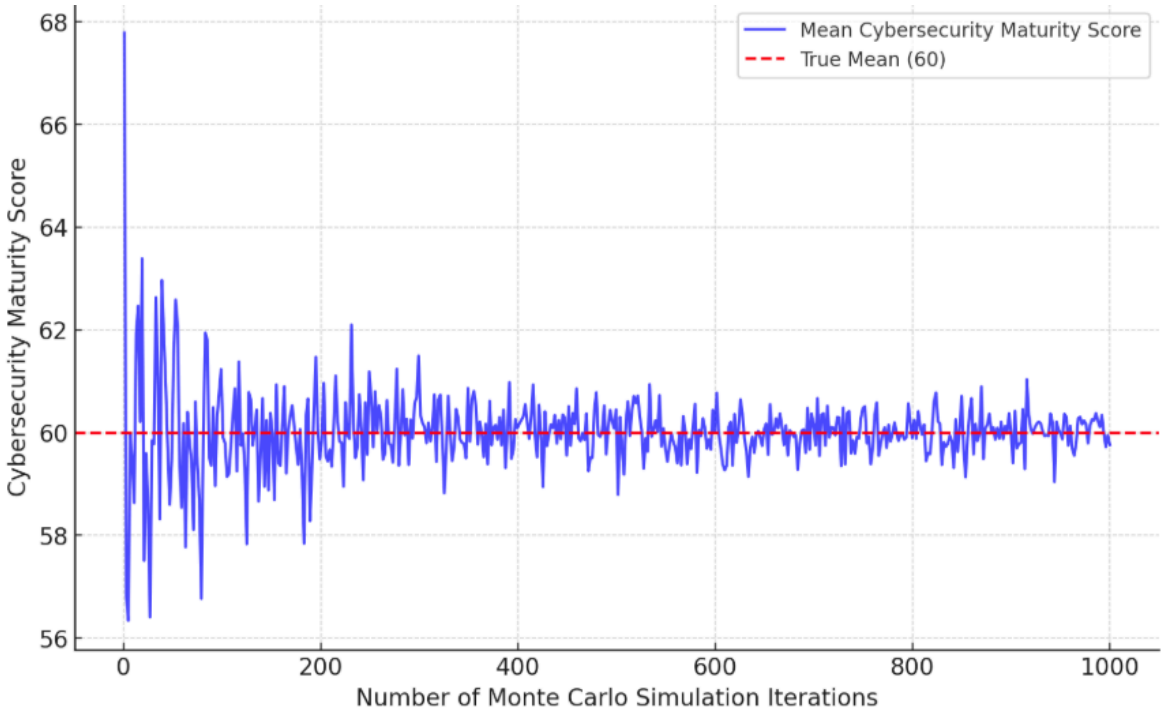
1. Determining the Baseline Score for Maturity Progression
    - The mean cybersecurity maturity score (60) derived from the graph establishes the expected starting point for organizations in the Intermediate Implementation stage.

- This baseline score ensures consistency in maturity scoring when evaluating the impact of cybersecurity policies and technological adoption on progression.

2. Validating Maturity Score Variability
    - The graph demonstrates that maturity scores exhibit a normal distribution, with organizations clustering around mid-range maturity levels (40-80).
    - The dispersion of scores confirms that some organizations remain at low maturity levels, while others achieve advanced cybersecurity resilience, reinforcing the QCMF model's structured progression.
3. Enhancing the Accuracy of Risk and Policy Simulations
    - By establishing a mean score, the Monte Carlo simulations could model how different cybersecurity policies and technological investments shift maturity scores over time.
    - Organizations that implement quantum-resistant encryption and policy enforcement are projected to increase their maturity scores above the mean (toward 80-100), while those with weak regulatory structures remain below the baseline (40-60).
4. Supporting Risk Reduction and Attack Success Probability Calculations
    - The probability of quantum cyberattack success is inversely correlated with maturity scores, meaning that as an organization’s or nation’s cybersecurity maturity increases, the likelihood of a successful quantum cyberattack decreases.
    - This graph's distribution helps determine cybersecurity thresholds, where organizations above the mean (60+) show significantly lower risk exposure, aligning with Figure A3 in Appendix A (Probability of Quantum Threat Success).

Figure A2

Monte Carlo Simulation Convergence Over Iterations



Note: This figure demonstrates how cybersecurity maturity scores stabilize as the number of Monte Carlo simulation runs increases, validating the model's statistical reliability. Running a sufficiently large number of simulations yields trustworthy and reproducible cybersecurity maturity scores, making the model a reliable tool for decision-making and risk assessment.

Description:

The X-axis represents the number of iterations, while the Y-axis represents the average cybersecurity maturity score. The graph illustrates that initial iterations show high variance, but as simulations increase, the results stabilize, confirming the predictive reliability of QCMF in cybersecurity risk assessment.

This figure validates the statistical reliability of the cybersecurity maturity assessment model by demonstrating how Monte Carlo simulations converge to a stable mean as the number

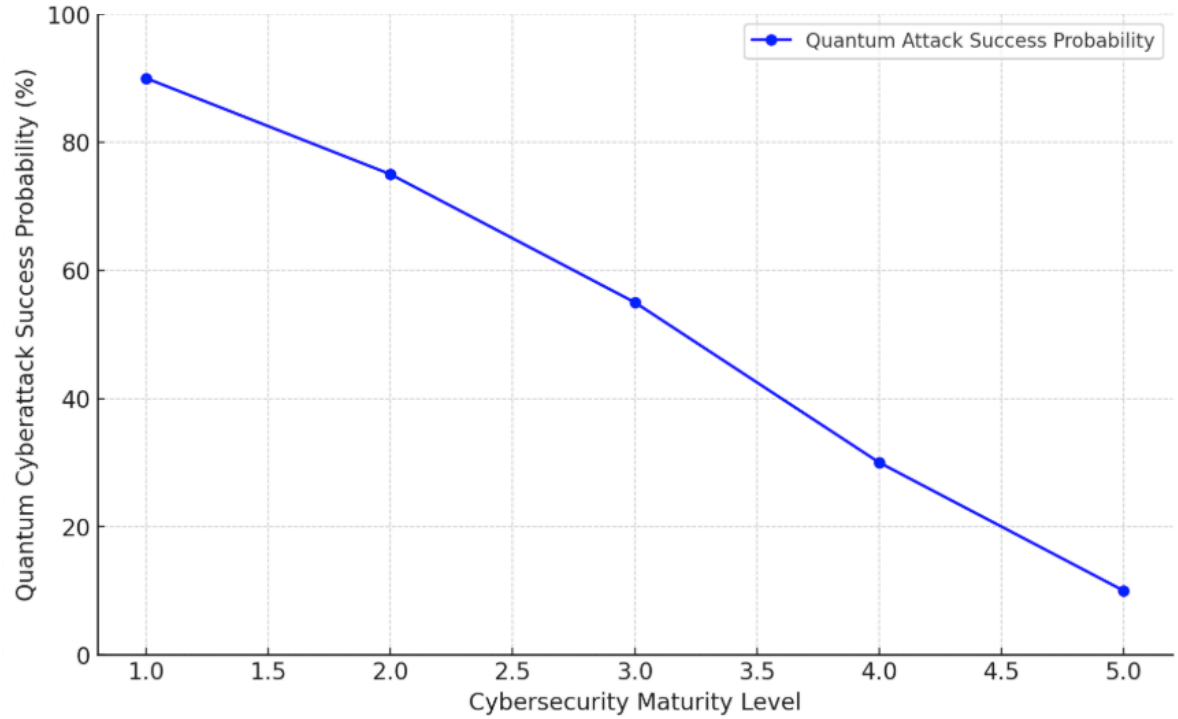
of iterations increases. The true mean cybersecurity maturity score (60), represented by the red dashed line, serves as a benchmark for evaluating organizations' cybersecurity maturity levels.

Key Insights from the Graph

1. Early Variability in Cybersecurity Maturity Scores
    - In the first 200 iterations, cybersecurity maturity scores fluctuate significantly, ranging from 56 to 68.
    - This initial variance is expected due to the random nature of early simulation trials, where limited iterations result in unstable predictions.
2. Convergence to a Stable Mean (60) as Iterations Increase
    - Around 300+ iterations, the fluctuations begin to stabilize, indicating that additional runs refine the accuracy of maturity scores.
    - 300+ iterations ensures that cybersecurity maturity scores are not influenced by randomness.
    - By 800–1000 iterations, the simulation reaches a near-consistent maturity score of 60, demonstrating that the QCMF-based maturity assessment remains statistically reliable across different conditions.
3. Confirmation of Model Predictability
    - The gradual reduction in variance validates the Monte Carlo simulation framework as a robust methodology for assessing cybersecurity preparedness.
    - The results suggest that organizations adopting QCMF-based cybersecurity enhancements will experience predictable improvements in maturity levels, reinforcing the framework’s reliability for cybersecurity risk assessment.

Figure A3

Probability of Quantum Threat Success vs. Cybersecurity Maturity Level



Note: This graph visually represents the inverse correlation between cybersecurity maturity and the likelihood of a successful quantum cyberattack. As cybersecurity maturity increases, the probability of a successful quantum cyberattacks decreases, reinforcing the critical role of proactive security measures. Nations with higher cybersecurity maturity scores indicate quantum-resistant encryption, and strong incident response strategies and those with low maturity scores lack quantum-resilient security measures and are more susceptible to quantum-enabled threats.

Description

The X-axis represents cybersecurity maturity levels, while the Y-axis denotes the probability of a successful quantum-enabled cyberattack. The results indicate that

- Lower maturity levels (Initial Awareness, Basic Preparation) have a high attack success rate (75-90%), while

- Adaptive Quantum Security (Level 5) reduces quantum attack success probability below 10%.

The following figures illustrate the relationship between cybersecurity maturity progression and regulatory enforcement. The following figures demonstrate the impact of policy enforcement and governance frameworks on cybersecurity maturity development.

The figure quantifies the relationship between cybersecurity maturity levels and the probability of a successful quantum-enabled cyberattack. It serves as empirical validation for the effectiveness of QCMF in reducing risk exposure as organizations progress through maturity stages.

Key Insights from the Graph

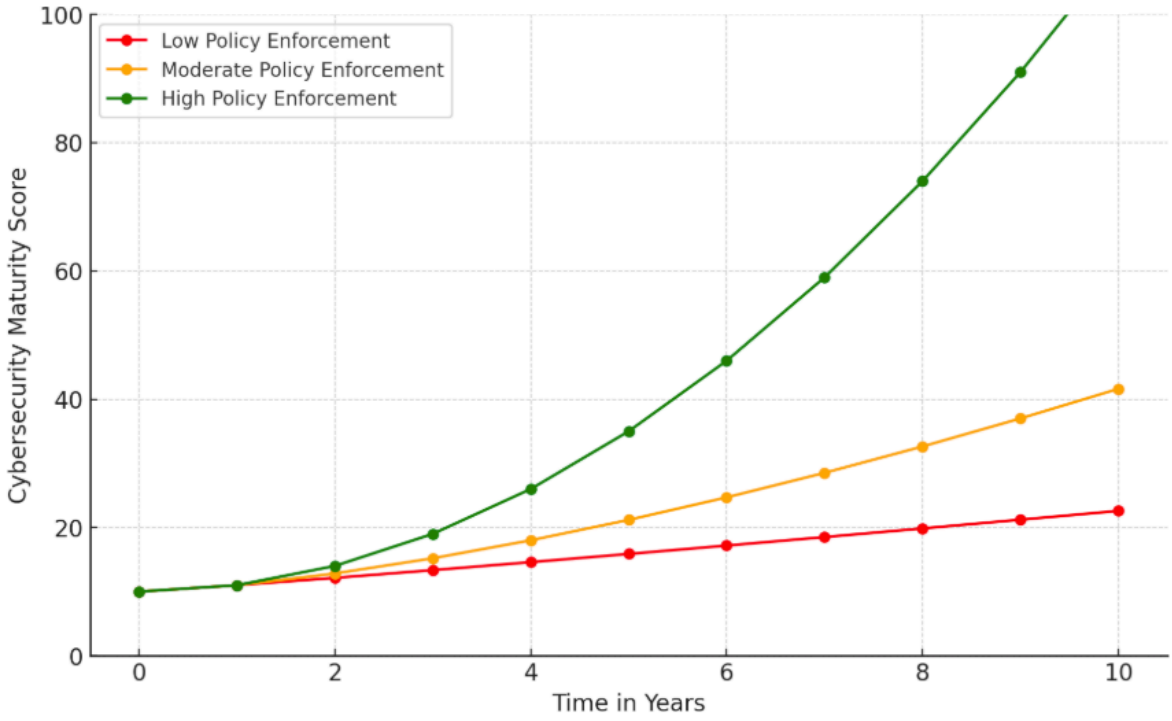
1. Higher Cybersecurity Maturity Reduces Quantum Threat Success Rates
    - The X-axis represents cybersecurity maturity levels (1 to 5), aligning with the QCMF maturity progression model.
    - The Y-axis represents the probability of a successful quantum cyberattack in percentage terms.
    - At lower maturity levels (Initial Awareness, Basic Preparation), quantum attacks have a high probability of success (75-90%), due to lack of cryptographic defenses and reactive security postures.
2. Diminishing Attack Probability with Maturity Progression
    - At Initial and Basic levels of maturity, the probability of a successful quantum-enabled attack decreases exponentially; incremental advancements in security can lead to significant risk reductions and may reduce the probability of a successful quantum attack by 30-50%.

- At Intermediate Implementation and Advanced Integration (Levels 3-4), success rates drop below 40%, indicating that stronger encryption and proactive security policies reduce vulnerabilities.
- At Adaptive Quantum Security (Level 5), the probability of attack success falls below 10%, confirming that organizations with comprehensive cybersecurity strategies can nearly eliminate major quantum cyber risks.

3. Supports Policy Enforcement & Governance Models
    - These results align with policy compliance findings, where organizations in high-enforcement jurisdictions were able to reach maturity levels 4-5 faster, significantly lowering cyberattack exposure.
    - The inverse correlation between maturity scores and quantum cyberattack success provides critical insights for decision-makers, enabling them to strategically allocate funding and resources toward security initiatives that yield the greatest risk reduction.
    - Appendix A (Figures A4 and A5) indicate that regulatory-driven cybersecurity policies accelerate risk reduction and validates the role of cybersecurity regulations in driving faster adoption of maturity improvements, ensuring that organizations progress beyond vulnerable states more effectively.

Figure A4

Impact of Policy Enforcement on Cybersecurity Maturity Progression



Note: Cybersecurity Maturity Progression Under Different Policy Enforcement Models. This figure compares the rate of cybersecurity maturity growth under different policy enforcement strategies, demonstrating how regulatory compliance accelerates cybersecurity resilience.

Description

The X-axis represents cybersecurity maturity levels, while the Y-axis represents cybersecurity maturity progression speed. The results show that:

- Low Policy Enforcement results in slow progression, keeping organizations vulnerable.
- Moderate Policy Enforcement leads to steady but delayed adoption.
- High Policy Enforcement rapidly accelerates maturity progression, ensuring faster adoption of quantum-resistant security.

The figure quantifies the role of policy enforcement in accelerating cybersecurity maturity progression, demonstrating that stronger regulatory mandates lead to faster adoption of quantum-resistant security measures.

Key Insights from the Graph

1. Direct Correlation Between Policy Enforcement and Cybersecurity Maturity Growth
    - The X-axis represents time in years (0–10), while the Y-axis represents cybersecurity maturity scores based on QCMF progression.
    - Three distinct policy enforcement scenarios are modeled:
        - Low Policy Enforcement (Red Line): Minimal government intervention and voluntary compliance.
        - Moderate Policy Enforcement (Orange Line): Industry-recommended cybersecurity compliance audits.
        - High Policy Enforcement (Green Line): Mandatory security mandates, government audits, and strict enforcement.
2. Low Enforcement Leads to Slow Cybersecurity Progression
    - Organizations under low-enforcement policies show only marginal improvements over 10 years.
    - Without strict regulatory requirements, cybersecurity maturity scores remain below 30, keeping organizations vulnerable to quantum threats.
3. Moderate Enforcement Improves Maturity but Lags in Adoption
    - The orange line (moderate enforcement) shows steady, but slower cybersecurity growth.

- Organizations improve over time but reach only ~50% of the cybersecurity maturity scale by year 10, suggesting that voluntary compliance alone is insufficient.

4. High Policy Enforcement Leads to Exponential Cybersecurity Growth
    - The green line (high enforcement) shows rapid cybersecurity maturity growth, with scores reaching above 90 within 10 years.
    - This confirms that stronger regulatory compliance mechanisms accelerate the adoption of post-quantum security measures, making organizations more resilient against emerging quantum threats.

How This Supports Findings from the Study

Aligns with QCMF Maturity Model:

- Organizations in high policy enforcement jurisdictions reach advanced cybersecurity maturity (Levels 4–5) faster, confirming policy mandates as a key driver of resilience.

Supports Policy Recommendations in Chapter 5:

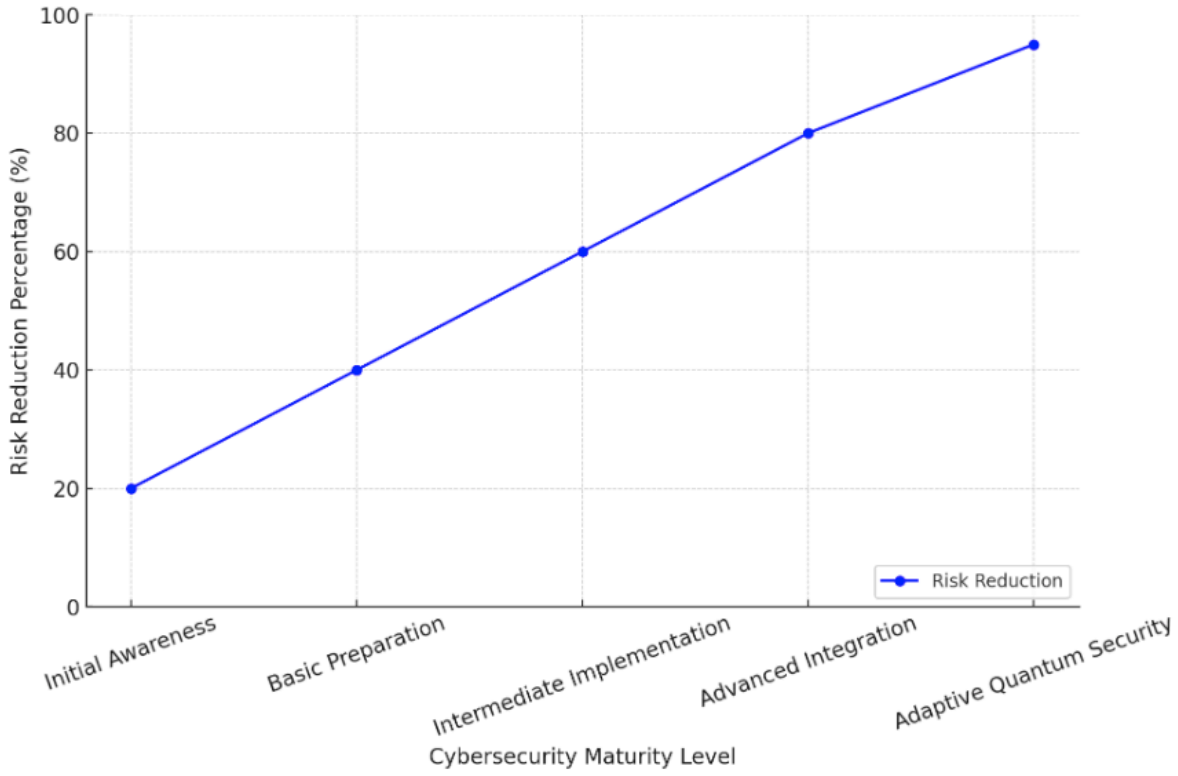
- Simulation results align with findings that government-backed cybersecurity enforcement significantly reduces quantum cyber risks over time.
- This figure reinforces the argument that nations adopting stricter security policies achieve faster quantum security integration.

Validates Need for Policy-Driven Cybersecurity Funding:

- Countries that fund cybersecurity resilience programs experience faster progression through maturity levels.
- This graph supports Appendix A, Figure A5, which shows that increased cybersecurity investments further accelerate risk reduction.

Figure A5

Comparative Risk Reduction Across Cybersecurity Maturity Levels



Note: Risk Reduction Across Cybersecurity Maturity Levels. This bar chart illustrates the correlation between cybersecurity maturity and risk reduction, highlighting the effectiveness of higher cybersecurity maturity in mitigating quantum threats.

Description

The X-axis represents the five maturity levels, while the Y-axis represents percentage reduction in cybersecurity risk exposure. The results demonstrate that:

- Lower maturity levels (Initial Awareness, Basic Preparation) exhibit limited risk reduction due to weak security measures.
- Intermediate Implementation and Advanced Integration significantly reduce cyber risk due to enhanced cryptographic resilience.

- At the Adaptive Quantum Security stage, risk exposure is minimized, demonstrating that high-maturity organizations are substantially more resistant to quantum-enabled threats.

The figure quantifies the direct correlation between cybersecurity maturity progression and risk reduction, reinforcing the effectiveness of structured cybersecurity enhancements in mitigating quantum-enabled threats. It provides empirical validation for QCMF by illustrating that higher maturity levels correspond to greater risk reduction.

Key Insights from the Graph

1. Higher Cybersecurity Maturity Directly Reduces Risk Exposure
    - The X-axis represents cybersecurity maturity levels, from Initial Awareness (Level 1) to Adaptive Quantum Security (Level 5).
    - The Y-axis represents the percentage reduction in cybersecurity risk exposure, showing how risk diminishes as organizations adopt quantum-resistant security measures.
    - A consistent upward trend confirms that as cybersecurity maturity improves, overall risk exposure declines.
2. Low Maturity Levels (Initial Awareness, Basic Preparation) Provide Minimal Protection
    - Organizations at Level 1 (Initial Awareness) experience less than 20% risk reduction, meaning most security threats remain unmitigated.
    - At Level 2 (Basic Preparation), risk reduction improves slightly (~40%), but security measures are still largely reactive rather than proactive.
    - These findings align with Figure A3 (Quantum Threat Success Probability), which shows that organizations at low maturity levels face higher cyberattack success rates.

3. Mid-Level Maturity (Intermediate Implementation, Advanced Integration) Significantly Reduces Risk
    - Level 3 (Intermediate Implementation) marks a turning point, where risk reduction surpasses 50% due to the implementation of cryptographic resilience strategies.
    - Level 4 (Advanced Integration) further enhances cybersecurity readiness, reducing risk exposure by nearly 80% through proactive encryption measures and real-time threat monitoring.
4. Adaptive Quantum Security (Level 5) Nearly Eliminates Quantum Cyber Threats
    - Organizations that achieve Level 5 (Adaptive Quantum Security) experience the highest level of resilience, with risk exposure falling below 10%.
    - These results align with policy enforcement data (Figure A4), which demonstrates that strong regulatory mandates accelerate cybersecurity maturity and risk reduction.

Cost-Benefit Advantage of Cybersecurity Investments

- Findings confirm that investing in cybersecurity maturity progression leads to substantial risk reduction, justifying quantum-resistant security funding initiatives.
- These results align with the cost-benefit analysis in Chapter 5, which argues that higher cybersecurity investments yield greater security returns.

Supports QCMF as a Predictive Cybersecurity Maturity Model

- The gradual but steady decline in risk exposure confirms that QCMF can be used to predict cybersecurity outcomes based on maturity progression.

- This finding validates the structured transition between QCMF levels, reinforcing its use for cybersecurity policy development.

Justifies Need for Mandatory Cybersecurity Governance Models

- Governments and organizations that enforce stronger cybersecurity mandates (Figure A4) reach higher maturity levels faster, experiencing greater risk reduction benefits.
- This figure strengthens policy-driven cybersecurity recommendations in Chapter 5, reinforcing the necessity of strict regulatory enforcement for cybersecurity progression.

Appendix B: Maturity Model Scoring and Selection

Overview

The QCMF was calculated by evaluating the contribution of each assessment criterion to the overall score. Decomposing the score according to key criteria, the framework not only highlights the areas where each nation excels but also identifies specific gaps that need to be addressed. This ensures that the framework offers actionable insights tailored to each nation's unique cybersecurity landscape. Each level of the maturity model is associated with a specific range of total scores on the 0 – 100 scale. These ranges reflect the level of preparedness and maturity in managing quantum cybersecurity threats.

Mapping Scores to Maturity Stages

Level 1 Initial Awareness

Score Range: *0–20*

Description: Organizations or nations at this level have minimal awareness of quantum cybersecurity risks and have not taken significant steps to address these threats. A low score indicates that they are just beginning to understand the implications of quantum technologies for cybersecurity and have not yet implemented any quantum-resistant measures.

Level 2 Basic Preparation

Score Range: 21–40

Description: This level represents a basic level of preparedness, where organizations have begun to implement quantum-resistant technologies and strategies, but these efforts are still in the early stages and may be inconsistent or ad-hoc. The score range reflects some initial efforts to address quantum threats, but there is significant room for improvement.

Level 3 Intermediate Implementation

Score Range: *4 –60*

Description: At this stage, organizations have developed a more structured and systematic approach to quantum cybersecurity. They have implemented quantum-resistant technologies across key areas and are actively working to close gaps in their defenses. A score in this range indicates moderate maturity, with a solid foundation in place but ongoing work needed to achieve full integration.

Level 4 Advanced Integration

Score Range: *61–80*

Description: Organizations or nations at this level have achieved a high level of preparedness, with quantum-resistant technologies fully integrated into their cybersecurity frameworks. Regular assessments and updates are conducted to ensure that all systems are capable of withstanding quantum threats. A score in this range reflects a mature, well-developed approach to quantum cybersecurity, with few gaps remaining.

Level 5 Adaptive Quantum Security

Score Range: *81–100*

Description: This is the highest level of maturity, where organizations have a dynamic and adaptive cybersecurity framework that evolves with technological advancements. They continuously monitor for new quantum threats, proactively mitigate risks, and can quickly adapt to emerging challenges. A score in this range indicates full maturity, with the organization being at the forefront of quantum cybersecurity practices.

Summary of Score Ranges

0–20: Level 1 - Initial Awareness

21–40: Level 2 - Basic Preparation

41–60: Level 3 - Intermediate Implementation

61–80: Level 4 - Advanced Integration

81–100: Level 5 - Adaptive Quantum Security

These score ranges help to categorize the maturity of organizations or nations in handling quantum cybersecurity threats, guiding them on the necessary steps to advance to higher stages of maturity.

Original List of Candidate Countries

The initial list of ten candidate countries considered for this study included the United States, China, Estonia, Germany, Japan, South Korea, Canada, United Kingdom, France, and Israel. These nations were identified based on their significant involvement in quantum computing research, cybersecurity investments, and legislative initiatives supporting quantum-resistant strategies.

Screening Criteria and Evaluation

Each country was evaluated against the following criteria to ensure alignment with the study's objectives:

1. **Government Investments**: Funding allocated to quantum computing research and development, with a focus on quantum cybersecurity initiatives.
2. **Legislative and Policy Initiatives**: Presence of legislative frameworks or national strategies explicitly addressing quantum threats.
3. **Cybersecurity Maturity**: Demonstrated progress in implementing advanced cybersecurity measures, particularly quantum-resistant technologies.

4. **Global Collaboration**: History of participation in international cybersecurity initiatives, reflecting their commitment to knowledge-sharing and coordinated defenses.

Rationale for Final Selection

The United States, China, and Estonia were selected based on their exemplary performance in these areas:

- **United States**: Advanced integration of quantum-resistant technologies, supported by robust investments and coordinated federal policies, positioned the U.S. as a leading example of quantum cybersecurity readiness.
- **China**: Significant investments in quantum technologies and a strong focus on offensive quantum capabilities provided a contrasting approach, highlighting the need for balanced strategies.
- **Estonia**: As a smaller nation with advanced digital infrastructure, Estonia represented an agile, foundational approach to quantum cybersecurity, showcasing the challenges and opportunities for resource-constrained nations.

Countries not selected, such as Germany, Japan, and South Korea, demonstrated strong quantum research and development but lacked comprehensive quantum-specific cybersecurity strategies. These nations' emphasis remained on broader quantum advancements rather than targeted quantum-resistant cybersecurity measures, making them less aligned with the study's focus on cybersecurity maturity models.

Assessment Criteria and Scoring Breakdown

The overall maturity score for each nation was derived from a composite of scores across several key assessment criteria. These criteria were chosen to comprehensively evaluate each

nation's preparedness for quantum cybersecurity threats. The criteria and their respective contributions to the total score are detailed below:

Adoption of Quantum-Resistant Technologies (30% of Total Score)

Definition: This criterion assesses the extent to which quantum-resistant technologies have been adopted and integrated into the nation's cybersecurity infrastructure. It includes the use of post-quantum cryptographic algorithms, quantum-resistant hardware, and other technological innovations designed to counter quantum threats.

Scoring: Each nation was scored on a scale of 0–30 based on the level of adoption and implementation of these technologies. A score closer to 30 indicates widespread and effective adoption, while a lower score suggests minimal or nascent implementation.

Case Study Breakdown:

United States: 28/30

China: 21/30

Estonia: 15/30

Effectiveness of Threat Detection and Response Systems (25% of Total Score)

Definition: This criterion evaluates the effectiveness of systems in place to detect, respond to, and mitigate quantum cybersecurity threats. This includes the ability to recognize quantum-related anomalies, the speed of response, and the success rate in neutralizing threats.

Scoring: Scored on a scale of 0–25, with higher scores representing faster and more effective threat detection and response capabilities.

Case Study Breakdown:

United States: 22/25

China: 18/25

Estonia: 12/25

Integration of Quantum Cybersecurity in National Policies (20% of Total Score)

Definition: This criterion assesses how well quantum cybersecurity measures are integrated into national cybersecurity policies and frameworks. It includes evaluating whether quantum cybersecurity is a strategic priority and the extent of governmental support and regulation.

Scoring: Scored on a scale of 0–20, where a higher score reflects comprehensive policy integration, and lower scores indicate gaps in policy or lack of strategic focus.

Case Study Breakdown:

United States: 18/20

China: 14/20

Estonia: 10/20

Workforce Readiness and Expertise (15% of Total Score)

Definition: This criterion measures the availability and expertise of the cybersecurity workforce in quantum-related areas. It includes the presence of trained professionals, ongoing education and training programs, and the nation's capacity to attract and retain quantum cybersecurity talent.

Scoring: Scored on a scale of 0–15, with higher scores indicating a more prepared and knowledgeable workforce.

Case Study Breakdown:

United States: 13/15

China: 10/15

Estonia: 8/15

Scalability and Flexibility of Cybersecurity Measures (10% of Total Score)

Definition: This criterion evaluates the ability of a nation's cybersecurity measures to scale and adapt to evolving quantum threats. It examines whether the nation can rapidly deploy quantum-resistant solutions across different sectors and adjust to new developments.

Scoring: Scored on a scale of 0–10, where a higher score indicates strong scalability and adaptability.

Case Study Breakdown:

United States: 8/10

China: 7/10

Estonia: 5/10

Calculation of Total Maturity Score

The total maturity score for each nation was calculated by summing the weighted scores from each of the assessment criteria. Each criterion's contribution was weighted according to its importance (as described above), and the scores were added to provide an overall maturity score on a scale of 0–100.

Case Study: United States

Adoption of Quantum-Resistant Technologies: 28/30

Effectiveness of Threat Detection and Response Systems: 22/25

Integration of Quantum Cybersecurity in National Policies: 18/20

Workforce Readiness and Expertise: 13/15

Scalability and Flexibility of Cybersecurity Measures: 8/10

Total Maturity Score = **89**/100

Case Study: China

Adoption of Quantum-Resistant Technologies: 21/30

Effectiveness of Threat Detection and Response Systems: 18/25

Integration of Quantum Cybersecurity in National Policies: 14/20

Workforce Readiness and Expertise: 10/15

Scalability and Flexibility of Cybersecurity Measures: 7/10

Total Maturity Score = **70**/100

Case Study: Estonia

Adoption of Quantum-Resistant Technologies: 15/30

Effectiveness of Threat Detection and Response Systems: 12/25

Integration of Quantum Cybersecurity in National Policies: 10/20

Workforce Readiness and Expertise: 8/15

Scalability and Flexibility of Cybersecurity Measures: 5/10

Total Maturity Score = **50**/100

Table A1 provides a comparative assessment of quantum cybersecurity maturity among the United States, China, and Estonia, evaluating across five key assessment criteria, each contributing a weighted percentage to the total score. Highlighting each country's strengths and weaknesses; the U.S. excels in policy, workforce readiness, and scalability, China leads in quantum adoption but lags in policy and training, and Estonia, though innovative, faces scaling challenges due to limited resources and may struggle to scale quantum-resistant technologies. This comparison provides a data-driven foundation for strategic decision-making, helping policymakers prioritize investments, enhance international collaboration, and accelerate quantum-safe cybersecurity advancements to ensure long-term resilience.

Table A1

Assessment Criteria Score Table

Assessment Criteria	United States	China	Estonia
Adoption of Quantum-Resistant Technologies (30%)	28	21	15
Effectiveness of Threat Detection and Response Systems (25%)	22	18	12
Integration of Quantum Cybersecurity in National Policies (20%)	18	14	10
Workforce Readiness and Expertise (15%)	13	10	8
Scalability and Flexibility of Cybersecurity Measures (10%)	8	7	5
Total Maturity Score	89	70	50

Note: The table represents the aggregate scores (with relative weight) of multiple countries across several key criteria, such as the adoption of quantum-resistant technologies, effectiveness in threat detection and response, integration of quantum cybersecurity into policies, workforce readiness, and scalability of cybersecurity measures.

Appendix C: Metrics for Cost-Benefit Analysis and Application

This appendix outlines the specific metrics used for the cost-benefit analysis in the QCMF. Each metric is illustrated with example values derived from the case studies of the United States, China, and Estonia, demonstrating how the framework was applied in diverse geopolitical contexts.

1. Implementation Costs

Metric: Initial Investment in Technology

- **Definition**: Total cost of implementing quantum-resistant encryption across critical systems.
- **United States Example**: $10 billion allocated over five years to quantum-resistant cryptographic upgrades in critical infrastructure (National Quantum Initiative Act, 2018).
- **China Example**: Estimated $8 billion spent on quantum research, with $2 billion directed toward upgrading national networks with quantum communication protocols (Chinese Academy of Sciences, 2021).
- **Estonia Example**: $50 million investment in transitioning national e-governance systems to quantum-resistant standards (Kõiv & Naruskov, 2024).

Metric: Training and Workforce Development Costs

- **Definition**: Financial and time investments in training cybersecurity personnel for quantum-specific challenges.
- **United States Example**: $200 million allocated for federal cybersecurity workforce training initiatives focused on quantum threats (Quantum Economic Development Consortium, 2022).

- **China Example**: Investment in training 5,000 cybersecurity professionals specializing in quantum-resistant measures, estimated at $150 million (Gariso, 2021).
- **Estonia Example**: $2 million allocated for workforce training programs, representing 10% of the total cybersecurity budget (Panwar, 2018).

2. Long-Term Savings

Metric: Projected Cost of a Quantum Breach

- **Definition**: Potential financial losses from a quantum-enabled cyberattack.
- **United States Example**: Projected $1 trillion impact from a successful breach of financial systems if RSA-based encryption is compromised (Vance, 2024).
- **China Example**: Estimated $300 billion in potential losses from a quantum attack targeting state-owned enterprises (Quantum Economic Development Consortium, 2022).
- **Estonia Example**: Estimated $5 billion loss due to compromised national e-governance infrastructure (Panwar, 2018).

Metric: Reduction in Recovery Costs

- **Definition**: Savings from reduced recovery times due to improved quantum defenses.
- **United States Example**: 50% reduction in recovery costs, translating to $500 million annually (National Security Agency, 2024).
- **Estonia Example**: $20 million annual savings due to faster incident response enabled by quantum-resistant measures (Kõiv & Naruskov, 2024).

3. Risk Mitigation Metrics

Metric: Probability of a Quantum Breach

- **Definition**: Likelihood of a quantum-enabled attack without mitigation efforts.

- **United States Example**: 20% probability of critical infrastructure compromise without quantum-resistant measures (Waller & McCafferty, 2022).
- **China Example**: 30% probability due to an imbalanced focus on offensive capabilities (Dohler & Althobaiti, 2020).
- **Estonia Example**: 40% probability due to foundational maturity levels and resource constraints (Alagic et al., 2020).

Metric: Risk Reduction Rate

- **Definition**: Percentage decrease in vulnerabilities achieved through quantum-resistant measures.
- **United States Example**: 75% reduction in vulnerabilities post-adoption of quantum-resistant cryptography (Grobman, 2020).
- **Estonia Example**: 50% reduction after initial deployment of quantum-resistant encryption in national databases (Panwar, 2018).

4. Opportunity Costs

Metric: Economic Impact of Delayed Adoption

- **Definition**: Financial losses from maintaining outdated cryptographic systems.
- **United States Example**: $200 billion in projected losses over 10 years if adoption of quantum-resistant technologies is delayed (Quantum Economic Development Consortium, 2022).
- **China Example**: $80 billion in delayed adoption costs due to reliance on legacy systems (Grobman, 2020).

5. Economic Growth Potential

Metric: Revenue from Quantum-Safe Products

- **Definition**: Income generated from commercializing quantum-safe technologies.
- **United States Example**: $50 billion in projected revenue from quantum-safe software solutions by 2030 (Grobman, 2020).
- **China Example**: $40 billion projected from exports of quantum communication devices (Chinese Academy of Sciences, 2021).

6. Time-to-Value Metrics

Metric: Implementation Timeline

- **Definition**: Time required to fully deploy quantum-resistant technologies.
- **United States Example**: Five-year plan for full adoption across federal agencies and critical sectors (National Quantum Initiative Act, 2018).
- **Estonia Example**: Three-year plan focusing on foundational systems within national e-governance (Kõiv & Naruskov, 2024).

Metric: Break-Even Point

- **Definition**: Duration required to recover initial investments.
- **United States Example**: Seven years due to high initial costs but significant long-term savings (Quantum Economic Development Consortium, 2022).
- **Estonia Example**: Four years due to smaller-scale investments but immediate operational improvements (Panwar, 2018).

7. Stakeholder Impact

Metric: End-User Satisfaction

- **Definition**: Level of satisfaction among stakeholders with improved cybersecurity measures.

- **United States Example**: 90% satisfaction rate among government agencies post-adoption of quantum-resistant technologies (National Security Agency, 2024).
- **Estonia Example**: 85% satisfaction rate among citizens using quantum-secured e-governance systems (Kõiv & Naruskov, 2024).

How Metrics Were Applied

The metrics in this appendix were developed based on the principles of adaptive policy evaluation outlined by Purdon et al. (2001), particularly their emphasis on iterative refinement and cost-benefit analysis as essential tools for assessing organizational readiness and strategic investments. By systematically applying these metrics, the QCMF provided actionable insights grounded in the seminal work of Purdon et al. (2001), ensuring that the findings and recommendations outlined in Chapter 4 and Chapter 5 are both theoretically sound and practically applicable.

These metrics were designed to:

1. **Evaluate the financial and operational feasibility of implementing quantum-resistant technologies**:
    - Drawing from Purdon et al.'s (2001) framework, the cost-benefit analysis assessed both immediate investments and long-term savings
    - Ensuring that resource allocation aligns with strategic priorities while addressing quantum-specific risks.
2. **Assess the readiness and vulnerabilities of the case study countries**:
    - Informed by Purdon et al.'s (2001) iterative methodology, the metrics enabled a dynamic evaluation of how readiness evolves across maturity levels
    - Accounting for geopolitical contexts and resource constraints.

3. **Guide the development of tailored recommendations for each nation based on their unique contexts and maturity levels**:
    - The framework's adaptive principles informed the development of context-sensitive strategies
    - Balancing short-term actions (e.g., foundational upgrades) with long-term goals (e.g., scalability and resilience).