The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 6, December 2025
https://doi.org/10.33022/ijcs.v14i6.5040

The Rise of Quantum Computing and its Impact on Cybersecurity

Passmore Vareta[1], Hillary Muzenda[2], Tanyaradzwa Nyamupaguma[3], Yangekile Dube[4], Belinda Ndlovu[5]
n02421251v@students.nust.ac.zw[1], n02427211x@students.nust.ac.zw[2], n02425205g@students.nust.ac.zw[3], n02315689j@students.nust.ac.zw[4], belinda.ndlovu@nust.ac.zw[5]
[1,2,3,4,5]National University of Science and Technology, Bulawayo, Zimbabwe

Article Information

Received : 4 Nov 2025
Revised : 18 Nov 2025
Accepted : 3 Dec 2025

Keywords

Quantum computing, Cybersecurity, Quantum Security, Quantum Mechanics, Quantum Threats

Abstract

Quantum computing's rapidly advancing capabilities threaten classical cryptographic systems, as algorithms such as Shor's and Grover's can break or weaken widely used encryption schemes. However, existing research remains fragmented, with limited integration of quantum threat analysis, mitigation strategies, and policy considerations. This study conducts a Systematic Literature Review (SLR) of 24 peer-reviewed articles (2021–2025) from IEEE Xplore, SpringerLink, ACM, and Google Scholar to synthesize current knowledge on quantum cybersecurity developments. Findings show that 80% of threat-focused studies confirm Shor's algorithm critically undermines RSA and ECC, while 65% highlight Post-Quantum Cryptography (PQC) as the most viable near-term defence. In contrast, only 25% of Quantum Key Distribution (QKD) studies demonstrate readiness for deployment due to challenges related to distance, cost, and standardization. Results further indicate that 40% of recent work promotes hybrid PQC–QKD models, with Europe leading the global research output at 46%. The study offers practical recommendations to guide the adoption of quantum-resilient cybersecurity.

A. Introduction

Quantum computing is based on the principles of superposition and entanglement. It allows quantum bits to handle information differently from classical binary bits of classical computers do [1];[2]. Quantum computers store information in objects called quantum bits (qubits) and transform them by exploiting particular properties of quantum mechanics. Quantum computing is an emerging domain that adopts the concepts of quantum mechanics and intersects with other domains that include computer science, mathematics, and physics to provide solutions for complex problems at a faster rate than traditional computing methods [3];[4]. Quantum computing is a technology that has the potential to revolutionise many industries. However, it also carries a significant threat of cybersecurity risks [5]. The threats posed by quantum computing to cybersecurity are of a greater magnitude. As such, precautions need to be taken when using quantum computing [6]. Quantum computers are computational devices that use the principles of quantum mechanics to tackle complex mathematical challenges that are difficult or computationally infeasible for classical computers to solve [2]. In general, quantum computers are a phenomenon that breaks the classical computations and applications of classical computers, leveraging the use of quantum physics/ mechanics [7]. Quantum computing represents an innovative approach to computation, utilising the principles of quantum mechanics to process information in new ways. Quantum computing uses quantum bits or qubits, totally distinct from the classical bits that exist as either a 0 or a 1; qubits can represent both 0 and 1 simultaneously through a process known as superposition [8]. Quantum computing offers the computing world the ability to perform tasks previously considered difficult with relative ease and at a faster rate.

Cybersecurity involves protecting computer systems, networks, and digital data from unauthorised access, attacks, damage and theft, which involves implementing measures and techniques to ensure the confidentiality, integrity and availability of information and computing resources [8];[9]. It is a set of technologies, processes, and practices to prevent attacks, damage, and illegal access to networks, computers, programs, and data [10]. Cybersecurity is defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [11]. Cybersecurity involves preserving the confidentiality, integrity, and availability of information in cyberspace [12];[13]. It is also defined as how individuals and organisations reduce the risk of being victims of cyberattacks [14]. Cybersecurity provides techniques, standards, policies, and recommendations to protect classical system assets, which are vulnerable and have been repeatedly breached in the past 10 years due to the classical weaknesses of the classical systems [15]. It helps in preserving the privacy of an individual's personal information, which should not be divulged or made public unless required by law [16]. To ensure that computer systems are protected from threats and possible attacks from the outside and inside environments[17], cybersecurity leverages the use of cryptography [18]. Quantum computing has been cited as the possible solution to addressing the threats and vulnerabilities that are affecting cybersecurity [15].

Cryptography is defined as the science of securing communication against an adversary, with its main goal being that of hiding the meaning of a message. Cryptography has three branches, namely:-
(i) Symmetric algorithms in which two parties have an encryption and decryption method for which they share a secret key,
(ii) Asymmetric (or public key) algorithms where two keys exist, a secret key and a public key,
(iii) Cryptographic protocols that realise more complex security functions through the use of cryptographic algorithms [18]

Of primary concern in today's cybersecurity is the vulnerability of the existing cryptographic systems to quantum attacks [4]. Traditional cybersecurity methods depend on cryptographic algorithms that are not easy for classical computers to break, algorithms such as Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA), which encrypt data in a way that is currently secure but potentially vulnerable to the processing power of quantum computers [19]. Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA) rely on the difficulty of factoring large numbers. However, the factoring of large numbers is efficiently solved by Quantum computing algorithms like Shor [20].

Quantum computers are a great danger to modern cryptography, as they threaten the confidentiality and integrity of communication with networks, as they can easily break the security provided by conventional cryptographic algorithms [2]. Peter Shor invented Shor's algorithm in 1994 to factor big integer numbers effectively using quantum computers [21]. Later, Shor's algorithm was demonstrated to break classical cryptographic systems, such as RSA, which classical computers used for encryption. The ever-rising quantum computing technology challenges classical cryptographic systems and requires quantum-resistant cryptography to protect sensitive data [22]. The power of quantum computers to solve complex problems threatens modern-day cybersecurity frameworks [1]. Quantum computing has brought breakthroughs in optimisation, material science, artificial intelligence, and cryptography [23]. The emergence of quantum technology presents significant benefits but poses new challenges, particularly in cybersecurity [23]. The rapid progress in quantum computing technology necessitates proactive measures to develop and adopt quantum-resistant cryptographic solutions, ensuring the long-term confidentiality, integrity, and availability of sensitive information [24].

Although quantum computers pose a threat to the cybersecurity environment, post-quantum cryptography (PQC) is an alternative cryptosystem that is designed to resist attacks using large-scale quantum computers [25]. While quantum computers pose a threat to our cybersecurity, the same technology can be leveraged to counter those threats and resist attacks posed by other quantum computers, such as quantum cryptography [26]. The PQC era aims to establish the role that quantum computers can play in addressing potential threats arising from quantum computing. It also establishes how we can utilise quantum computers in various other aspects without fear of the escalating threats posed by them [25]. An example of the PQC is the Quantum Key Distribution (QKD), which is a secure protocol by which private key bits can be created between two parties (Bob and Alice); the two private key bits form a private key cryptosystem which is regarded as secure [27]. QKD

uses quantum mechanics to exchange the secret key and detect network eavesdroppers [28]. Although existing studies extensively document the cryptographic vulnerabilities introduced by Shor's and Grover's algorithms, there remains limited consolidation of how quantum threats collectively interact with regulatory, infrastructural, and operational realities. Current literature treats PQC, QKD, policy, and governance issues in isolation rather than as interconnected components of a quantum-secure ecosystem. This fragmentation creates uncertainty for organisations attempting to operationalise quantum-safe migration. The present study addresses this gap by synthesising 24 empirical and conceptual works into an integrative quantum–cybersecurity model that connects technological, organisational, and regulatory dimensions.

This paper contributes a unified analytical lens for understanding quantum cybersecurity by mapping how threat vectors, resilience techniques (QKD, PQC, hybrid models), and governance mechanisms co-evolve. Unlike prior reviews that focus on one dimension (cryptographic algorithms or QKD performance), this study integrates technical, ethical, infrastructural, and regulatory domains to offer actionable migration guidance for practitioners

Background of the study

Modern society relies on Information and Communication Technology (ICT) [29]. Because ICT systems are interdependent, if one is compromised, all connected devices are too. Cybersecurity problems have grown as ICT systems have grown [30]. Due to escalating security concerns, policymakers should prioritise ICT infrastructure protection to mitigate the effects of evolving threats[31]. Today, governments, financial institutions, hospitals, corporations, and billions of people depend on ICT systems [32]. Over the past 20 years, organisations, consumers, and governments worldwide have driven cyberspace and cloud adoption [33]. Criminals utilise cyberspace to commit fraud and other crimes, increasing cyber risks for these stakeholders' online activities [10]. Google's 2019 quantum supremacy demonstration was among numerous quantum computing advances [34]. Quantum computers could tackle difficult problems faster than classical computers [35].

Since its founding, quantum computing—based on quantum mechanics—has changed significantly. Paul Benioff proposed the quantum computer model in the early 1980s [3]. Further quantum computing research led to the development of qubits, the building blocks of quantum computers [36]. Google's 2019 quantum supremacy demonstration was among many recent quantum computing advances [34]. Quantum computers can tackle difficult problems faster than traditional computers [35].

Quantum computing is still in its experimental stage; therefore, security is a major concern. RSA and ECC are both public-key algorithms that offer encryption and digital signatures. However, Shor's algorithm poses a threat to these classical algorithms by effectively solving complex tasks [37]. One of the positives of quantum computing is that it can improve cybersecurity. The two common cryptography approaches that offer quantum-resistant encryption are Quantum Key Distributor (QKD) and Post-Quantum Cryptography (PQC) [38]. Quantum computing embedded with Artificial intelligence can increase detection and response times [39]. The evolution of quantum computing has a

significant impact on cybersecurity, underscoring the urgent need for ongoing research and adaptation to protect sensitive data [40].

Quantum bits, known as qubits, allow exponentially faster information processing [36]. As much as this technology offers numerous positives in cybersecurity, it is also of great concern since it threatens classical cryptographic systems or algorithms. The efficiencies of Shor's algorithm threaten RSA and ECC, leaving these classical systems susceptible to quantum threats.. This vulnerability impacts data confidentiality, integrity, and availability in banking, healthcare, and national security [41].

Most financial institutions globally have cybersecurity frameworks vulnerable to quantum threats [42]. Adversaries capitalize on this gap to intercept and store encrypted sensitive data, with the intention of decrypting it later as quantum technology continues to evolve. This scenario can be best phrased as the "Harvest Now, Decrypt Later" case [43]. Factors such as interoperability issues, high infrastructure costs, and lack of standard protocols allied to Quantum Key Distributor and Post-Quantum Cryptography derail the adaptation to quantum-resistant systems [44].

As quantum computing technology evolves, legal, ethical, and policy issues must be addressed. Implications of quantum technologies on privacy and security require constant and regular updates on the regulations, such as the HIPAA (Health Insurance Portability and Accountability Act) and the GDPR (General Data Protection Regulation) [45]. It is currently unclear in the cybersecurity frameworks about quantum computing and its impact on cybersecurity, leaving a gap that malicious adversaries will capitalize on [46].

Although quantum computing is sometimes perceived as a threat to existing classical systems, it offers secure, quantum-safe protocols that can reshape the cybersecurity landscape. This scenario prompts the need for accelerating research on policy formulation and deployment of quantum-resistant systems [47];[48];[49].

This study's research problem is the urgent need to understand the impact of quantum computing, its vulnerabilities, and the necessity of exploring secure transition corridors. The study combines current research and provides insights to close gaps in quantum-enhanced cybersecurity landscapes. The goal is to gain an understanding of the impact of quantum computing on cybersecurity by addressing the following research questions.

1. What are the differences between classical computing and quantum computing?
2. What quantum threats pose challenges in existing encryption methods?
3. How can cybersecurity be enhanced by a quantum key distributor (QKD)?
4. How can data privacy and policy compliance be affected by quantum computing?
5. What quantum computing measures can be used to improve cybersecurity?

Thus, this study is guided by Cryptographic Resilience theory and the NIST Post-Quantum Migration Framework, which together explain how digital systems evolve in response to increasing computational threats. Cryptographic Resilience Theory emphasises system adaptability under adversarial conditions, while NIST's PQC migration principles highlight operational readiness, algorithm agility, and phased deployment. These frameworks provide the conceptual anchor for interpreting the themes emerging from the SLR.

B. Methodology

A systematic literature review (SLR) was conducted to eliminate bias, allowing the research objectives to be addressed in this study. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) was used to improve the reporting of systematic reviews by allowing researchers to examine and combine high-quality research-related information critically [50]. Electronic databases, including IEEE Xplore, SpringerLink, ACM Digital Library, and Google Scholar, were searched rigorously to ensure relevance.

Search Strategy

The following search queries were used to extract relevant papers from the electronic databases;

("Quantum computing" OR "Quantum technology" OR "Quantum mechanics") AND ("Cybersecurity" OR "Information security" OR "IT security")

In addition, papers searched were not older than 5 years since publication. Forty papers were extracted from the IEEE Xplore database, Google Scholar (20), SpringerLink (3), and ACM (2).

Inclusion and Exclusion Criteria

Only peer-reviewed English journal publications and conference proceedings from 2021 to 2025 were evaluated, with a focus on the most recent and relevant research in quantum cybersecurity. Articles irrelevant to quantum computing and cybersecurity were omitted, and duplicates were removed.

Table 1. Article selection criteria.

ID	Criteria
EC	Exclusion Criteria
EC1	Articles not written in English
EC2	Articles published before 2021 to ensure topical relevance
EC3	Duplicate articles identified during screening
EC4	Articles without full-text access
IC	Inclusion Criteria
IC1	Articles published in English for interpretability
IC2	Articles published between 2021 and 2025
IC3	Articles aligned with the research focus on quantum computing and cybersecurity
IC4	Peer-reviewed conference and journal articles
IC5	Articles with accessible full texts

Quality Appraisal

A quality assessment checklist adapted from the Critical Appraisal Skills Programme (CASP) [51] and the Joanna Briggs Institute (JBI)[52] SLR tool was applied. Each article was evaluated against criteria such as clarity of research aim, methodological transparency, robustness of evidence, and contribution to quantum cybersecurity. Studies scoring below 60% were excluded.

Screening and Eligibility

Sixty-five papers were screened, and 31 articles were excluded for the following reasons: Some articles were in languages other than English, some were older than 5 years, and others generalized quantum/cybersecurity without integrating the two. Thirty-four full-text articles were assessed for eligibility, and 10 full-text articles were excluded because they do not address the impact of quantum computing on cybersecurity. The articles that met the final review and were included are 24.

C. Results and Discussion

Figure 1 illustrates the flow diagram of this study, as outlined using PRISMA, and Table 2 presents the papers that met the inclusion criteria.

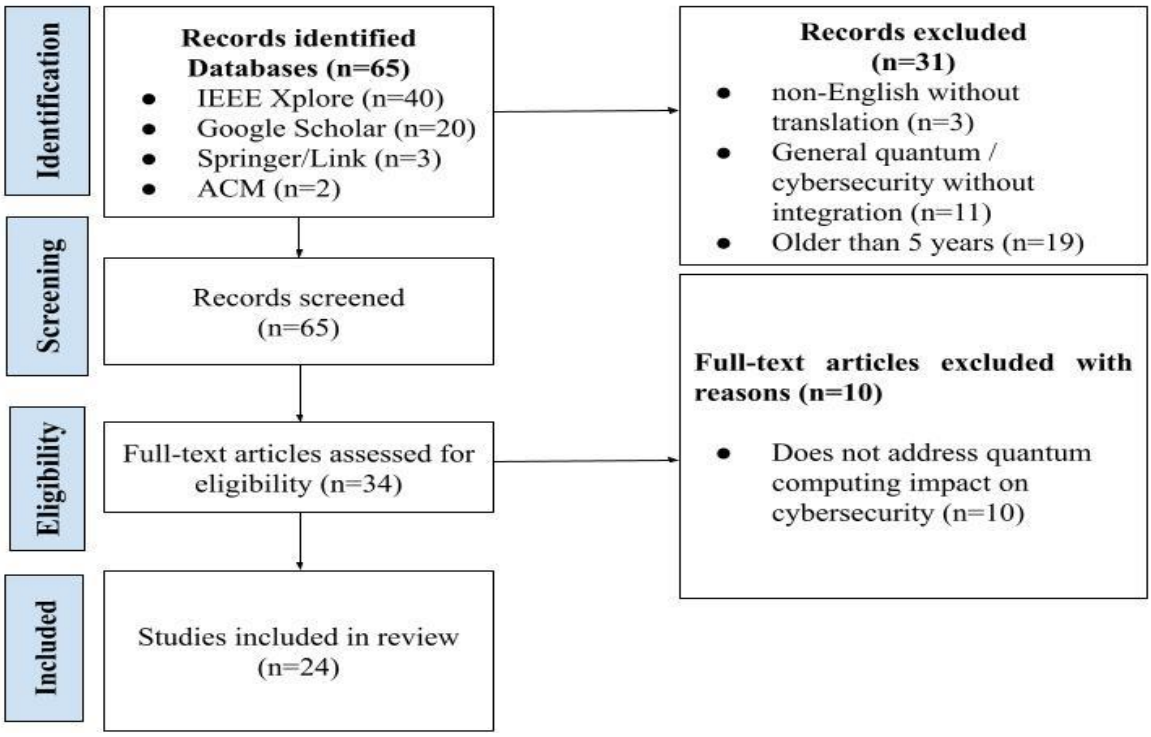

Figure 1. PRISMA Flow Diagram

A table was created to explore research questions and summarise article findings. This study analysed 24 papers. Data extraction followed an inductive thematic coding process. Codes were first generated at the sentence level (open coding), grouped into conceptual clusters (axial coding), and refined into three higher-order themes (selective coding): quantum vulnerabilities, quantum-resilient technologies, and governance/ethical considerations. Table 2 presents the comprehensive list of publications and their corresponding factors.

Table 2. Papers that met the inclusion criteria

Author(s) & Year	Country	Quantum vs Classical Computing	Threats to Existing Encryption	Quantum Key Distribution (QKD) Impact	Data Privacy & Compliance Considerations
[53]	UK	• Cryptographically Relevant Quantum Computers (CRQC) threaten Central Bank Digital Currencies • Classical: Less vulnerable	• RSA/ECC threats • "Harvest Now, Decrypt Later" (HNDL)	• QKD has financial security limitations; hybrid QKD+PQC is better	• Sensitive data at risk from HNDL
[54]	Germany	• Grover/Shor outperforms classical IDS • Classical: Not specified	• RSA/AES threats	• QKD for long-term security in communication systems	• Quantum-enhanced AI against eavesdropping
[55]	South Korea	• Quantum: Quantum mechanics principles • Classical: Binary states	• RSA/ECC threats	• QKD integrated with classical communication	• Compliance with privacy laws (e.g., HIPAA)
[56]	Japan	• Quantum: Secure state transmission • Classical: Wiretapping risks	• Classical network wiretapping	• QKD enhances security via one-way transmission	• Need for secure quantum networks
[43]	Canada	• Quantum: Solves factorization/logarithms • Classical: Relies on computational hardness	• Shor's algorithm threat	• Unconditional security for data/communication	• Quantum-safe solutions for IoT/IoD
[57]	Italy	• Quantum: Solves classically intractable problems - Classical: Not specified	• Threats to classical algorithms	• QKD for secure key exchange	• Quantum-resistant crypto for cloud security
[47]	USA	• Quantum: Physics-based security • Classical: Unproven math assumptions	• Shor's algorithm threat	• Hybrid QKD-PQC to address distance limitations	• Not explicitly stated
[45]	Spain	• Quantum: Exponential speedups • Classical: Polynomial-time algorithms	• Shor's algorithm threatens RSA/ECC	• QKD secures key distribution via quantum principles	• Urgency of PQC for critical infrastructure

[58]	China	• Quantum: Security via quantum mechanics principles • Classical: Relies on computational hardness assumptions	• Quantum attacks (CGI)	• Secures data transmission (quantum-generated keys)	• Ensures data privacy in remote imaging (quantum-safe transmission)
[59]	Australia	• Migration to quantum-resistant crypto • Classical: Not specified	• Threats to widely used crypto algorithms	• Focus on PQC migration	• Regulatory compliance during transition
[60]	USA	• Quantum: Uses superposition/entanglement • Classical: Binary bits, deterministic processing	• RSA/ECC vulnerabilities to quantum attacks	• QKD + quantum-resistant algorithms for future Cybersecurity	• Evolving regulatory/ethical concerns
[61]	South Korea	• Quantum: Multi-user QKD network • Classical: 1:1 key distribution	• Shor's algorithm breaks RSA/ECC	• QKD enables long-range key distribution in research networks	• Regulatory/policy barriers; calls for hybrid QKD framework
[62]	USA	• PQC secures against classical/quantum • Classical: Not specified	• RSA/ECC threats	• Not specified	• Migration to Quantum-Resistant Cryptography (QRC)
[4]	USA	• Quantum: Computational gains for specific problems • Classical: Sequential processing limits	• Traditional encryption weaknesses	• QKD as defense against quantum attacks	• Regulatory/privacy considerations
[63]	Australia	• Post-quantum cryptography (PQC) focus • Classical: Not addressed	• Shor's algorithm breaks RSA/ECC	• BIKE (PQC) as low-cost alternative to QKD	• Compliance with NIST PQC standards
[24]	India	• Transition from PKA to PQC • Classical: Not specified	• RSA/ECC threats	• QKD's distance limitations addressed via hybrid PQC+AI	• Not explicitly stated
[64]	Denmark	• Quantum: Qubits outperform classical • Classical: Not specified	• Breaks traditional crypto	• QKD generates robust keys for secure communication	• Robust quantum encryption to prevent cyberattacks
[65]	Slovenia	• Quantum: Near-unconditional security	• QKD implementation challenges	• Trust establishment critical due to	• Regulatory frameworks must evolve

		• Classical: Cryptographic limitations	(noise, distance)	verification risks	
[44]	Czech Republic	• Hybrid classical-quantum crypto • Classical: Not specified	• RSA/ECDSA threats	• Long-term security via secure key distribution	• Regulatory alignment during PQC transition
[66]	Spain	• Quantum: Operates via quantum principles • Classical: Deterministic binary logic	• Vulnerabilities in factorization/discrete-logarithm-based crypto	• Secure key exchange mitigates quantum risks	• Need for new regulatory frameworks
[67]	USA	• Not specified	• RSA/ECC threats	• Not specified	• Not specified
[68]	Japan	• Quantum: Internet via entanglement/repeaters • Classical: Classical encryption/routers	• Quantum repeater threats • New quantum network attack vectors	• Hybrid quantum-classical network integration	• Need for quantum internet architecture (confidentiality/integrity)
[69]	Japan	• Quantum: Speedups for optimization • Classical: Integer factorization reliance	• Integer factorization threats	• Quantum algorithms enhance physical-layer security	• Need for quantum-resistant wireless systems
[70]	USA	• Quantum: Superposition/entanglement • Classical: Binary states/logic gates	• Grover's/Shor's algorithms threaten RSA/ECC	• Secure key exchange with eavesdropping detection	• New regulatory frameworks; privacy law compliance

Publications per year

Quantum computing has witnessed a rise in awareness due to collaborative efforts to strengthen cybersecurity and better prepare for emerging threats in an increasingly digitally interconnected world. The result in Figure 2 shows that 2024 there was a growing interest in quantum computing, cryptography, and cybersecurity.

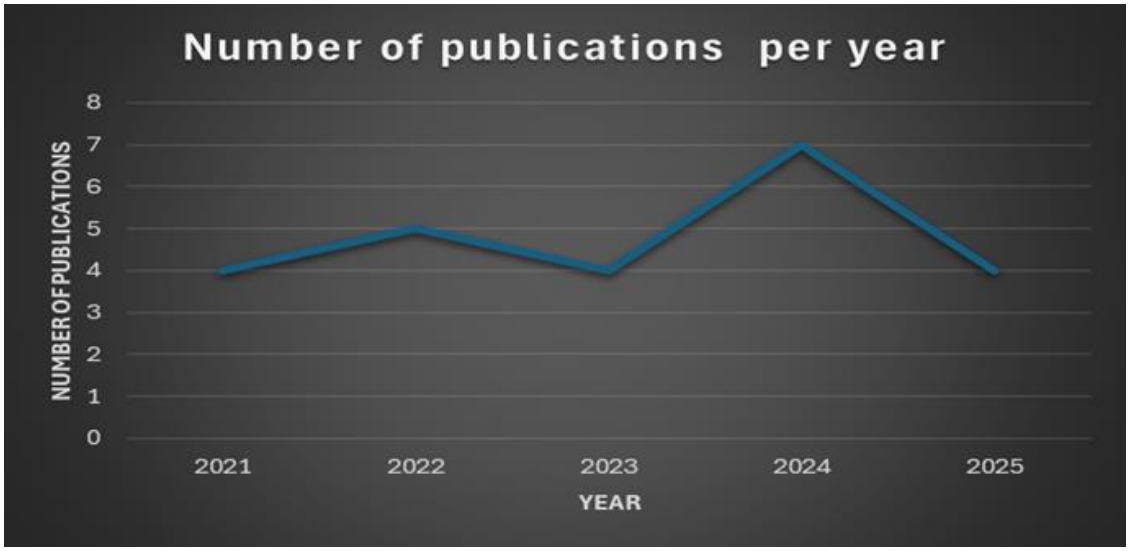

Figure 2. Number of publications

The data shows that there has been a rise in research interest for quantum computing in 2024, with a total of 7 publications. This spike aligns with the growing global developments in quantum computing and the increasing need to secure digital platforms across various sectors. This field is entering a maturity stage, as it is now shifting from theoretical work to more practical applications of quantum security frameworks, particularly PQC and QKD.

Country Representations

There are 13 countries represented in the literature, and these are the leading contributors as depicted in Table 3.

Table 3. Country Representations

Country	Frequency
USA	7 papers
Japan	3 papers
South Korea	2 papers
Australia	2 papers
Spain	2 papers

China, India, Germany, Slovenia, the Czech Republic, Italy, and Denmark	1 paper for each

Results show that the USA dominates with seven papers, indicating its strong investment in private and public sector quantum initiatives, such as the National Quantum Initiative. This is a US federal law passed in 2018 to accelerate quantum research and development. Countries such as Japan, South Korea, and Australia contribute significantly to the number of publications, accounting for 30%, which demonstrates their highly developed technological sectors and collaboration-driven research. Countries such as Italy and Denmark only hold 4% of overall publications because they lack adequate policies, innovation and funding. Countries that have adopted early strategies and strong research and development practices for quantum computing are thriving.

Research Publication by Continent

Results from Figure 3 indicate a significant academic focus on quantum Cybersecurity in Europe (46%), largely due to collaborative efforts, government support, a strong research infrastructure, and a strong emphasis on emerging technologies. Additionally, it has robust EU research frameworks, such as Horizon Europe, a key funding program for research and innovation.

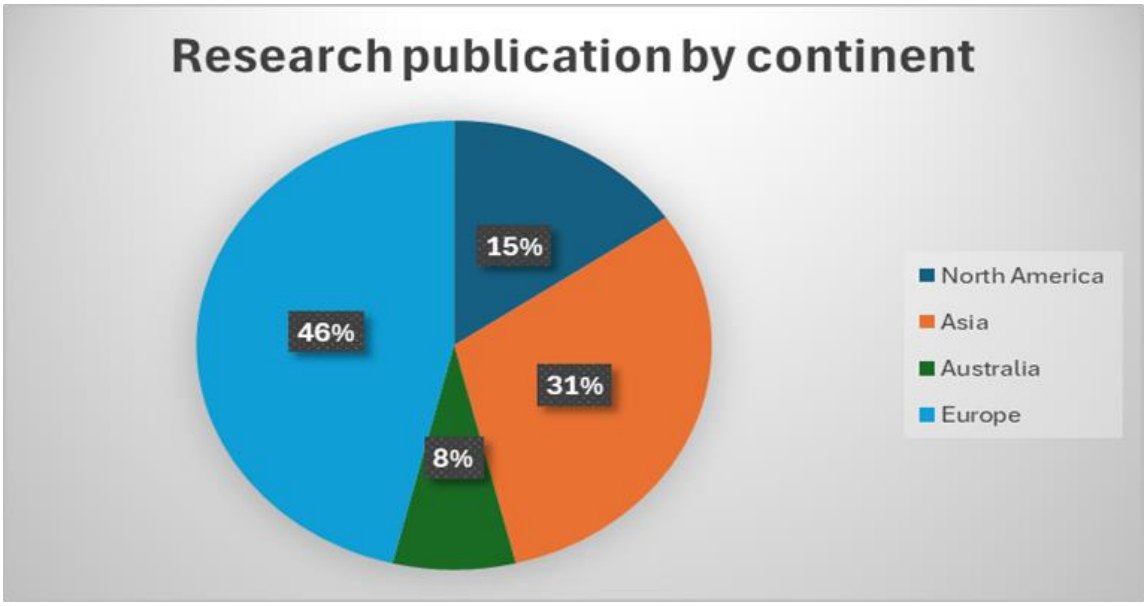

Figure 3. Research Publication by Continent

Asia's growing share (31%), particularly in China and South Korea, suggests that there may be increasing competition in quantum computing. Research publications in Australia and North America appear to be low, with percentages of 8% and 15%, respectively. In Australia, research tends to be concentrated in a few top institutions and a smaller number of elite centers, resulting in lower publication output. Some academic research may be published through consortia and not always under Australian affiliations. For North America, companies invest more in in-house research and development, not academic journals. The US

government does not openly publish articles on quantum research due to significant security concerns and implications for national security. Despite fewer published papers, North America and Australia remain leaders in quantum research. The apparent low publication rate reflects strategic, institutional, and commercial choices, not a lack of innovation or expertise.

Technological benefits and capabilities of Quantum computing

Results from Figure 4 show that superior computational power is the most frequently cited benefit, accounting for 79% overall. This is because quantum algorithms, such as Grover's and Shor's, allow exponential problems to be processed more efficiently than classical ones.

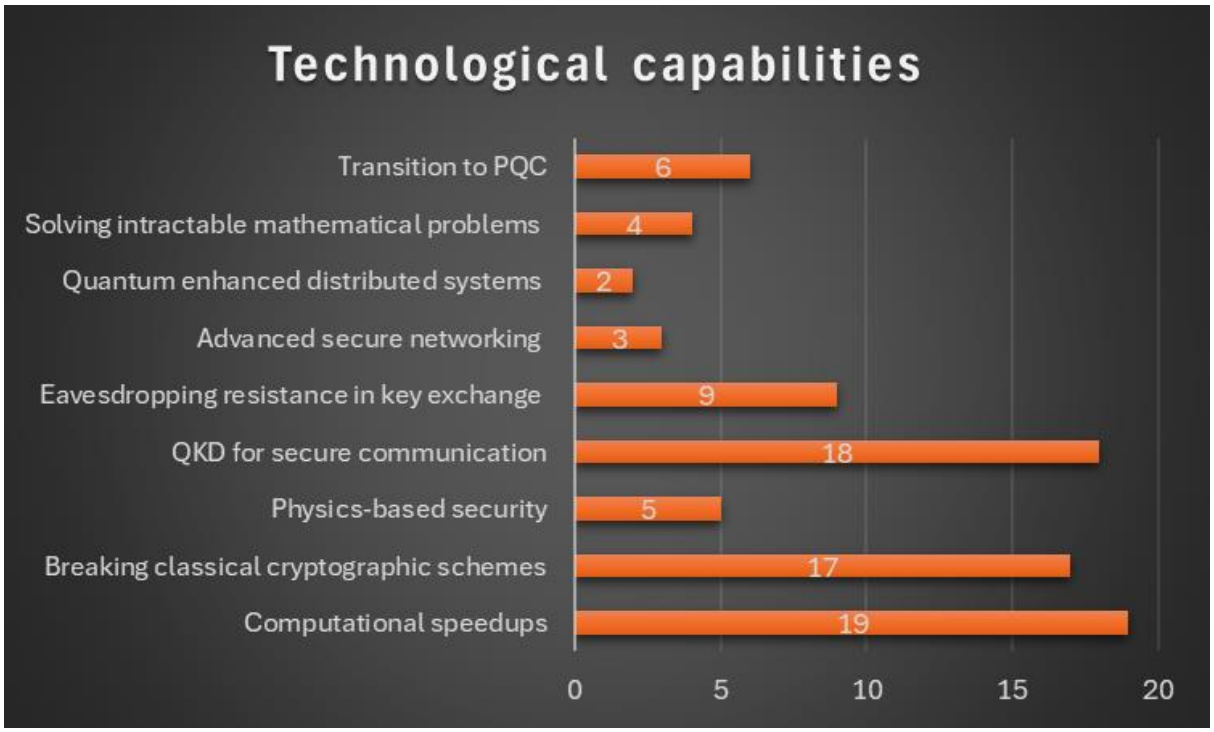

Figure 4. Technological Benefits and Capabilities

QKD for secure communication has a 75% success rate because it allows for secure communication through encryption keys, a dominant feature in quantum research. Eavesdropping resistance in key exchange is another leading benefit in quantum computing, with 37% because eavesdropping detection lessens the impact of cloning and disturbances within systems. Other technological benefits, such as advanced quantum networking, solving mathematical problems, and quantum-enhanced distributed systems, are significant but have less impact in quantum computing. This is likely because these ideas are still theoretical or in an early stage; hence, it explains their low visibility in the current literature.

Encryption vulnerabilities and threats

Results illustrated in Figure 5 show that Shor's algorithm is the most identified threat to classical computing, with 36%, due to several reasons, including

efficiency in factoring large numbers, quantum computing power, robust algorithms, and the necessity for post-quantum cryptography

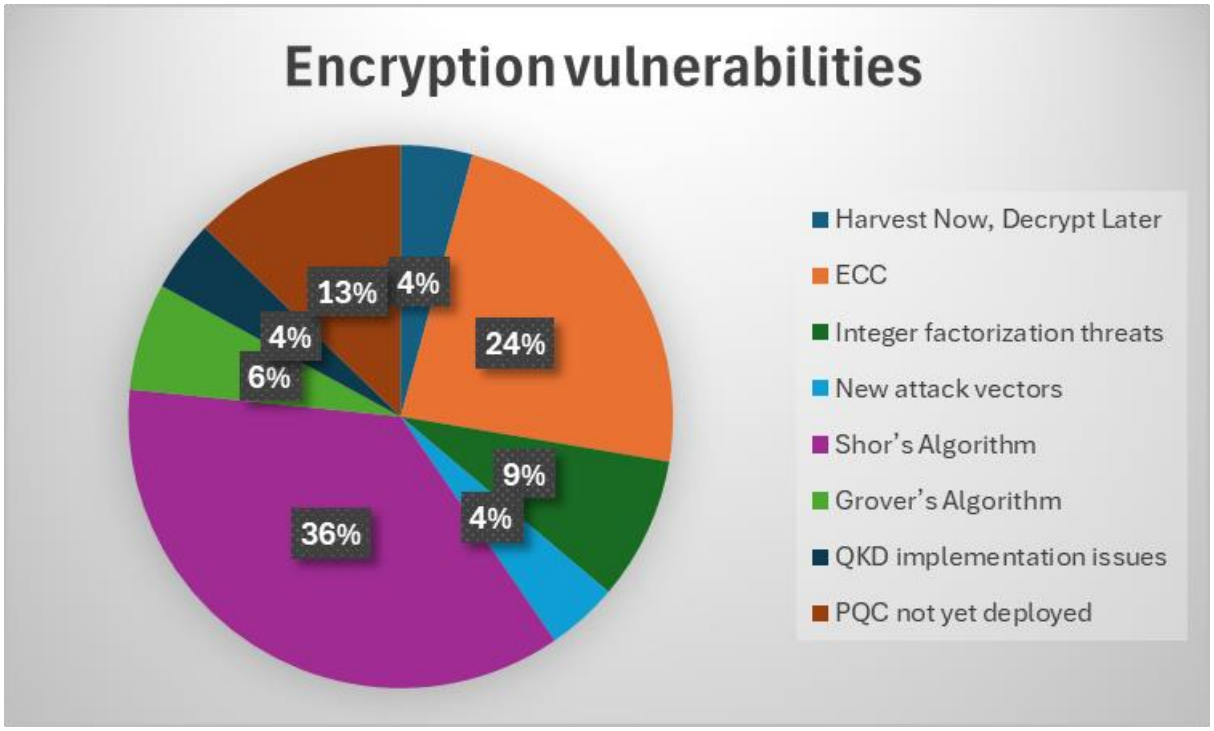

Figure 5. Encryption vulnerabilities

ECC comes second, with 24%, because most secure digital communications rely on cryptographic algorithms. Other vulnerabilities, such as new attack vectors and HNDL, have a low rate of 4% because they are usually patchable and can be detected earlier. They also pose as short-term threats that become obsolete once they are fixed. The reviewed studies show that quantum computing introduces four main categories of encryption threats, as summarised in the Quantum Threat Taxonomy in Figure 6

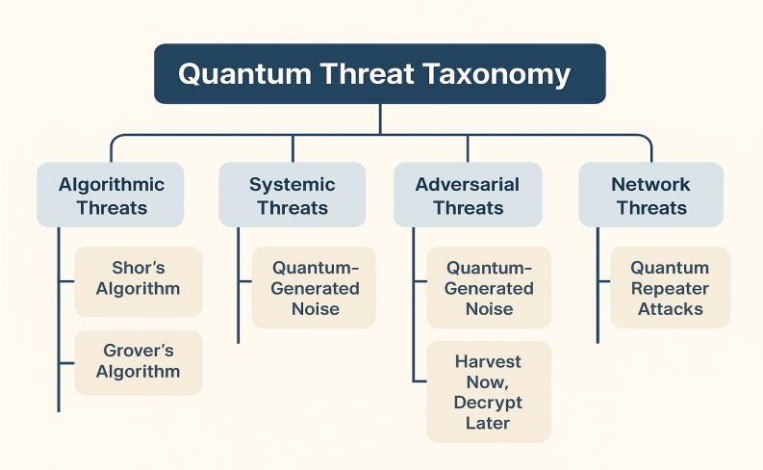

Figure 6. Quantum Threat Taxonomy

The Quantum Threat Taxonomy organises the major quantum-related vulnerabilities identified in the reviewed literature into four coherent threat classes. Algorithmic threats represent direct cryptographic risks arising from quantum algorithms, such as Shor's and Grover's, which undermine the assumptions of integer factorization and symmetric key search. Systemic threats include quantum-generated noise and hardware-induced instabilities that compromise qubit coherence, leading to unintended security failures in quantum or hybrid systems. Adversarial threats encompass strategic exploitation approaches such as "Harvest Now, Decrypt Later," where attackers store encrypted classical data for future decryption once cryptographically relevant quantum computers emerge. Finally, network threats include vulnerabilities introduced by quantum repeaters, quantum routers, and entanglement distribution systems, creating new attack surfaces in emerging quantum communication networks. Collectively, this taxonomy provides a structured lens for understanding how quantum advancements reshape the cybersecurity threat landscape and informs the need for PQC- and QKD-based defences.

While the Quantum Threat Taxonomy classifies the types of quantum-enabled risks: algorithmic, systemic, adversarial, and network-based, understanding their full impact requires examining where these threats actually penetrate digital infrastructures. These threat classes do not occur in isolation; rather, they map onto distinct layers of computing systems ranging from cryptographic algorithms and hardware components to communication protocols, network architectures, and application environments. To illustrate how these vulnerabilities cascade across technological layers, the Quantum Attack Surface Model (Figure 7) provides a structural view of the system domains exposed to quantum-driven compromise.

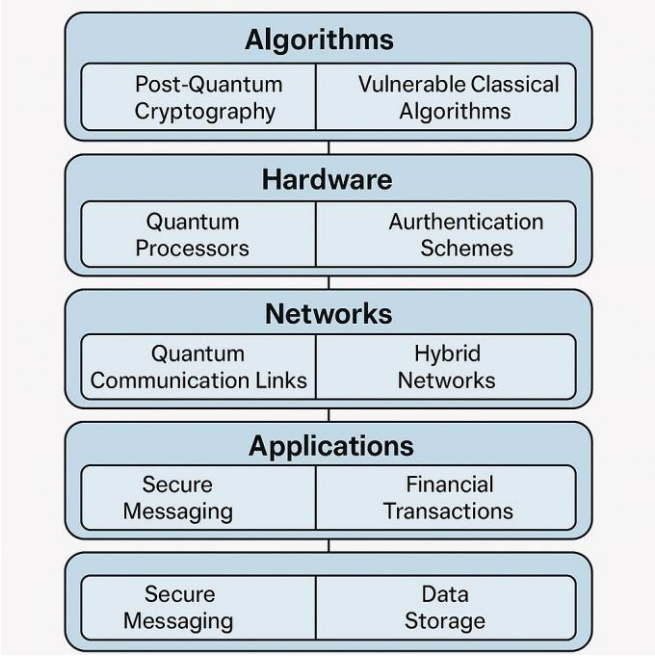

Figure 7. Quantum Attack Surface Model.

The Quantum Attack Surface Model expands the analysis of quantum threats by mapping them onto the specific system layers where compromise is most likely to

occur. At the algorithmic level, quantum attacks exploit weaknesses in vulnerable classical algorithms, thereby challenging the robustness of emerging post-quantum cryptographic schemes. The hardware layer encompasses risks associated with quantum processors, authentication devices, and physical key-generation components that may be susceptible to noise, tampering, or side-channel attacks. At the protocol layer, quantum and hybrid communication protocols introduce new points of failure that adversaries can manipulate to disrupt key exchanges or eavesdrop on secure sessions. The network layer includes quantum communication links, repeater chains, and hybrid infrastructures that expand the attack surface through entanglement distribution and long-distance key relay mechanisms. Finally, the application layer captures risks that impact secure messaging, financial transactions, data storage, and other mission-critical services, which depend on underlying cryptographic and network systems for confidentiality and integrity. This layered view complements the Quantum Threat Taxonomy by showing where and how identified threats propagate within real-world systems, guiding the placement of PQC, QKD, and hybrid defences.

The impact of QKD

According to Figure 8, enhanced communication security is the most frequently cited impact, with 83%, reflecting the major benefit of quantum computing.

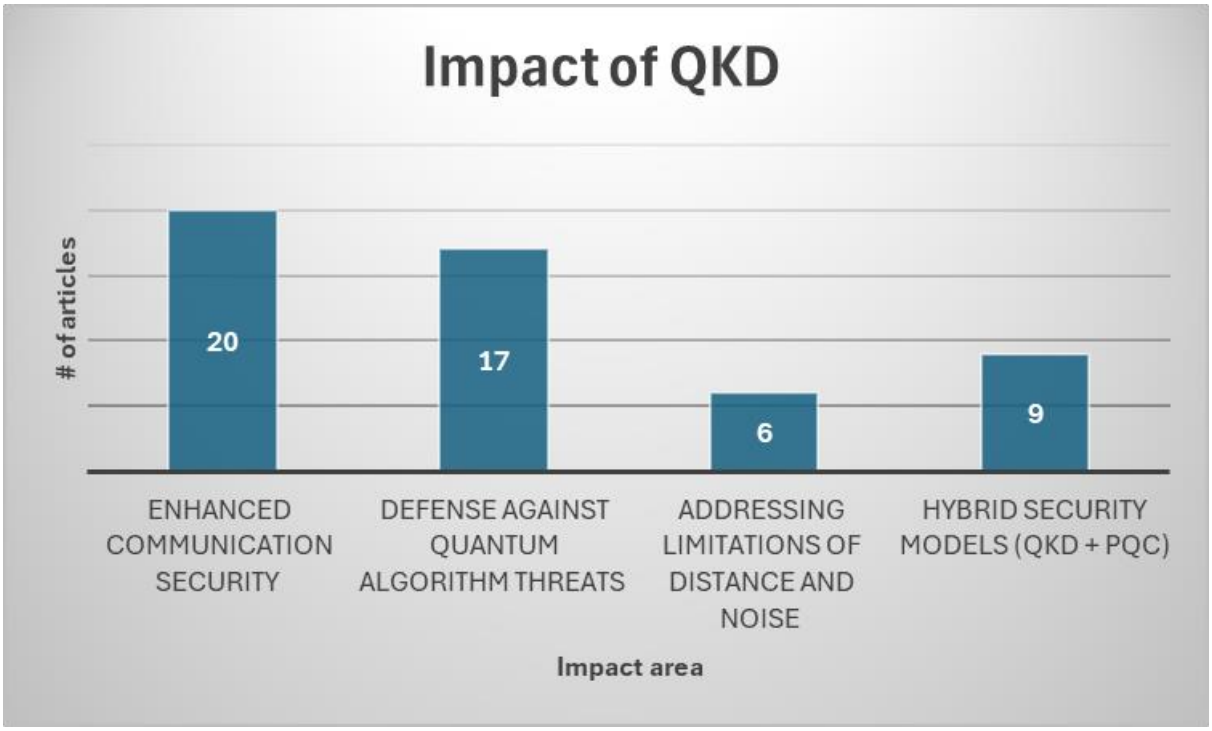

Figure 8. Impact of QKD

QKD ensures that any eavesdropping and interception attempts are detected before damage occurs. Frequency is very high because secure communication is crucial, and quantum computing offers it at its highest level. Defense against quantum algorithm threats also has a high frequency of 70% because it addresses the need to protect current cryptographic systems, such as

RSA and ECC, from quantum algorithms. This is a priority issue for cybersecurity because quantum computing poses a direct threat to current cryptographic infrastructure. Hybrid security models have a moderate frequency of 38% because they are gaining popularity in networks, although they are still in the development stage. Hybrid models combine QKD and PQC to provide high-level security. Lastly, addressing the limitations of distance and noise has a lower frequency of 25% because it is a subfield of quantum communication. These limitations must be addressed, as quantum systems are highly sensitive to both distance and speed.

Legal, Ethical, and Privacy Considerations

Ten out of 24 (43%) articles emphasized on the need to align migration of classical computing to quantum computing with the regulatory frameworks e.g HIPPA, GDPR, NIST .7/24 (21%) articles highlight the need for updated policies to address quantum threats .4/24 (16%) articles briefly address the ethical concerns of quantum computing .5/24 (20%) articles focused on the need to enhance data privacy using quantum computing and showing how HNDL is a major threat to sensitive data. This is especially true in sectors such as healthcare and finance.

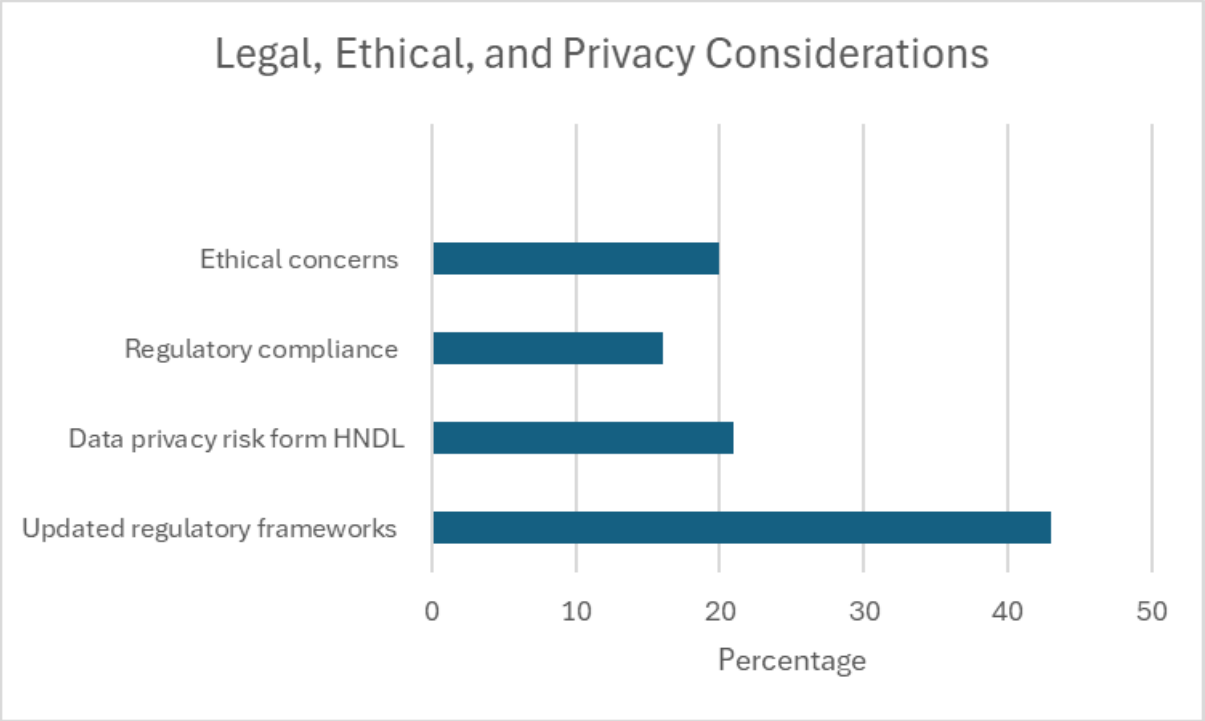

Figure 9. Legal, Ethical, and Privacy Considerations

The counts in Figure 9 reflect the frequency with which each consideration is discussed across the articles. Most studies consider updating regulatory frameworks to ensure quantum practices comply with regulations because of emerging threats, sector-specific impacts, data privacy and compliance, future-proofing security, ethical considerations and technological advancements.

This section presents the discussion of the study. It addresses the research questions of the study and provides implications for this study.

Fundamental Differences Between Quantum and Classical Computing

Quantum principles of superposition and entanglement vs. classical binary logic. Quantum computing uses superposition and entanglement, distinguishing it from classical computing. Superposition allows quantum bits (qubits) to represent 0 and 1 simultaneously [3]. Entanglement allows qubits to demonstrate correlations that classical bits cannot, allowing instantaneous state determination independent of distance, exponentially increasing computational capabilities [28]. This computational power gap enables innovative problem-solving [8]. In classical systems, parallelism is limited since it can exist in only 0 or 1 state, whereas in quantum computing, superposition allows parallel or simultaneous calculations [64].

Even though quantum computing has the potential to revolutionize technology, the implementation of qubits can face problems due to their interactions with the environment, which can cause them to lose the quantum property of interference [43]. Quantum computing can transform and reshape the cybersecurity landscape positively and adversely, since it threatens classical encryption standards [4].

How the qubit functions

Qubits execute complex calculations using quantum computing properties, entanglement, and interference [71]. Qubits perform operations that classical bits cannot by doing integer factorization and database search faster [25]; [72]. Shor's and Grover's algorithms can be executed faster by quantum circuits than their classical counterparts. This exponential speed of quantum computing affects cybersecurity defense [59].

Qubit systems can process information in parallel via quantum correlation [56]. This ensures that no eavesdropping occurs during the encoding, processing, and transmission of information. Quantum Key Distribution (QKD) enables this secure quantum communication [57]. However, qubits have limitations in that qubit coherence times and quantum error correction are resource-intensive [65]. However, this differs from classical bits, which utilize scalable hardware that is well-understood in terms of error prevention.

Quantum vs Classical computing in terms of computational speedup and parallelism

Quantum systems can analyse and perform complex tasks concurrently [20]. In quantum computing, the superposition property allows and promotes parallelism, outperforming classical computers that rely on computational hardness assumptions [69];[37].

Threats of Quantum Computing to Existing Encryption Methods

RSA and ECC Susceptibility to Shor's algorithm

Both RSA and ECC are public-key cryptographic algorithms that use integer factorisation to support current classical systems [59]. Although these classical algorithms provide and support current classical systems, Shor's algorithm factors huge numbers in polynomial time. It breaks classical cryptographic methods [72].

Sensitive data in key sectors, including finance, health, and government, will be susceptible to Shor's algorithm [41]. Cryptographic resilience to withstand the computational power of quantum computers [6].
The pace at which quantum hardware progresses increases the probability of cryptographic failures and indicates a substantial disruption of over 75% of global encrypted communication [2];[73]. The major concern is that safe quantum algorithms must be implemented before quantum computing comes into full force to prevent vulnerabilities [43].

"Harvest Now, Decrypt Later" (HNDL) Quantum Attack

This approach is used by malicious adversaries who intercept and archive encrypted communications in anticipation of quantum computers to decrypt them later [41]. Data secrecy in key sectors like health, finance, and the government is affected in the long run [74]. Quantum Key Distribution can be used to prevent the problem of "Harvest Now, Decrypt Later". There is a need to have robust threat intelligence security procedures to identify HNDL [8].

Current Cybersecurity Shortfalls Against Quantum-Enabled Threats

Quantum threats capitalise on their computational power to outsmart classical cybersecurity encryption techniques [49]. These current cybersecurity practices are ineffective against the power of quantum computers [20]. Very few industries have a clear practical plan to move to post-quantum cryptography [59]. The major blow for faster adoption of post-quantum cryptographic techniques is the issue of interoperability and standardisation delays [63]. Several factors must be considered when developing defences against quantum threats [44].

Quantum Key Distribution (QKD) and Its Role in Enhancing Cybersecurity

Quantum Key Distribution (QKD) Overview

QKD can be described as a mechanism that uses properties of quantum mechanics to generate and allocate secure keys between two parties [47]. This mechanism ensures that eavesdropping is detectable, thereby promoting secure communication. Despite all the strong positives of QKD, constructing perfect quantum hardware and a noiseless channel is difficult [57]. The most common QKD algorithms are the BB84 and E91, which offer unconditional security with optimal components [2]. This edges classical cryptographic systems; hence, QKD leads the next generation of cybersecurity. Its implementation encompasses protocol standardisation and compatibility [58]. Regardless of all the challenges to come up with QKD, it stands out as a strong solution against future quantum-related threats [61].

Eavesdropping Detection and Prevention

Eavesdropping can be detected in real time by comparing a subset of bits. If a deviation exceeds threshold levels, they throw away the key and restart [75]. However, the channel can be subject to false attacks due to its circumstances. These circumstances can be system noise within the channel itself [65]. These

flaws necessitate continuous improvement and the development of robust QKD systems [2].

Quantum Key Distribution (QKD) Challenges

Several challenges affect the deployment of QKD, including high costs, short transmission distances, network integration, and a lack of standardization and interoperability. Light particles carrying quantum keys can only travel for a few hundred kilometres at their best, an obstacle to developing QKD [65]. To overcome this, there is a need to build and come up with a quantum internet with quantum repeaters to enable long-distance quantum communications [67]. High implementation costs of QKD lead to commercialisation and operational complexities [57];[2]. QKD requires skilled human resources to deploy and maintain sufficient quantum communication systems [8].

Quantum Computing's Impact on Data Privacy and Policy Compliance

Quantum Computing Data Protection Regulations (HIPAA and GDPR)

Regulations such as the General Data Protection and Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) need to be consistently updated in order to keep pace with ever-evolving emerging quantum threats [4]. Most classical encryption protocols do not address quantum computing and this requires urgent frameworks so that data is not compromised [59]. This process needs industry, government and academia collaboration to keep updating data privacy policies [45]. When developing frameworks, long-term future needs need to be considered, as shown by HNDL [41];[59].

Ethical Concerns

Quantum computing demands physical and human resources available to a few nations [41]. In addition, quantum computing's power can potentially break existing encryption schemes, leading to data breaches [8]. The complexity of quantum computing algorithms may lead to a lack of accountability and transparency, making it difficult to understand the reason behind some of the mistakes [55]. More so, many jobs can be lost since quantum computing can automate most jobs in the future [76]. Sound ethical governance and international cooperation are essential to ensure that quantum-enabled technologies benefit society rather than endanger it.

Regulatory Gaps

Existing regulatory laws lack frameworks that address the threats posed by quantum computers [59]. There are also missing ethical guidelines on how to safely use quantum computers, resulting in a need for key stakeholders to seek new regulatory approaches [44]; [74]. Organisations such as the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI) are developing post-quantum cryptographic standards. However, global adoption is slow [58]. This prompts the global community to adopt and implement post-quantum cryptographic measures to mitigate and

combat quantum threats [45]. Equal participation is needed internationally to ensure that disparities do not exist through capacity training.

Leveraging Quantum Computing to Improve Cybersecurity

Post-Quantum Cryptography (PQC) Development and Implementation

Lattice-based, code-based, hash-based, and multivariate are the most common PQC algorithms that can tackle quantum computers' power [59]. NIST and other international agencies are standardising PQC algorithms to accelerate deployment [63].

Migrating from existing classical algorithms to PQC algorithms is complicated and requires the necessary skills [44]. Despite all these issues required to migrate to the PQC algorithm, PQC remains the basis for future-proofing cybersecurity against quantum threats [49].

Integration of hybrid cryptographic models combining QKD and PQC for robust security

Considering the pros and cons of quantum security technologies, hybrid cryptographic models may improve cybersecurity. QKD unconditional security and PQC computational resilience complement security guarantees in these models [44]. QKD for quantum-secure key exchange and PQC algorithms for data encryption and authentication give hybrid systems defence in depth [65]. PQC's software-based flexibility reduces QKD's distance and infrastructure restrictions, making this fusion feasible [57].

Hybrid cryptographic systems improve security without losing performance, making them suitable for critical infrastructures and sensitive communication channels [47]. Key management, protocol coordination, and regulatory compliance frameworks are needed to harmonise hybrid models [49]. Synchronizing QKD and PQC enhances cryptographic defenses against various attacks and underscores the need for integrated quantum cybersecurity infrastructures. Figure 10 illustrates the Hybrid PQC–QKD Architecture, demonstrating how post-quantum algorithms and quantum key distribution can be integrated to provide layered quantum-resilient security

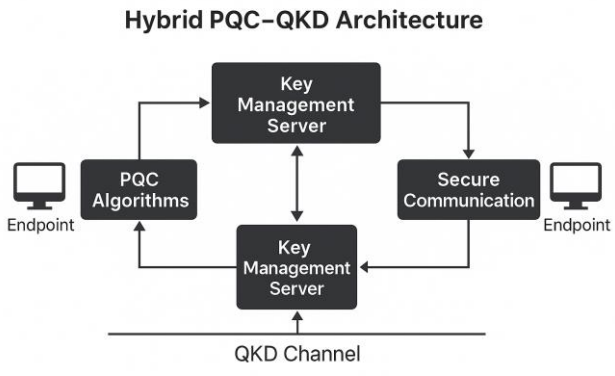

Figure 10. Hybrid PQC–QKD Architecture

The Hybrid PQC–QKD Architecture illustrates how organisations can integrate post-quantum algorithms with quantum-enhanced key distribution to establish resilient communication systems. In this model, endpoints encrypt and decrypt messages using PQC algorithms while relying on a QKD channel to generate and exchange quantum-secure keys. A centralised key management server coordinates both cryptographic layers: it receives keys generated through QKD, distributes them securely to endpoints, and ensures compatibility with PQC-based encryption processes. The combination of PQC for data confidentiality and QKD for key integrity provides layered protection against quantum adversaries, mitigating algorithmic, adversarial, and network threats identified in the study. This hybrid architecture demonstrates a practical pathway for transitioning from classical cryptographic infrastructures to quantum-resilient communication environments.

Quantum-Aware Cybersecurity Capacity Building

Capacity building is needed to professionally train and equip human resources with quantum skills [8]. This is due to the transformative power of quantum computing in cybersecurity. Execution of quantum-safe systems requires expert skill in quantum computing [59].

This entails that key stakeholders, including the government, academia, and the industry, must foster partnerships to exchange knowledge on quantum computing and its quantum-safe solutions. [55]. Collaboration is key to coming up with flexible frameworks that consider the rise of quantum computing [77].

Research Gaps

The findings collectively suggest that quantum threats progress faster than organisational readiness, widening a 'quantum preparedness gap'. Although QKD offers theoretical security, practical deployment remains limited by distance, cost, and standardisation barriers. PQC appears more deployable, yet migration complexity and backward compatibility hinder adoption. A hybrid model, therefore, emerges as the most viable path, aligning with 40% of analysed studies. However, regulatory and ethical frameworks lag behind technological advancements, exposing systemic governance vulnerabilities

Implications

This SLR is among the first SLRs (2021–2025) to empirically map global quantum–cybersecurity research trends across continents and quantify thematic frequencies. Thus, in order to protect sensitive data in key sectors, PQC and QKD must be

incorporated faster due to quantum threats. The absence of quantum-safe solutions can have serious economic and national security consequences, hence the need for urgent adaptation of quantum-safe practices. A combination of powerful cryptographic models that incorporate both classical and quantum-resistant algorithms is essential to curb these threats while maintaining compatibility across both systems.

Collaboration from the international community is necessary to formulate policies that consider and respect individual rights and innovation. Cybersecurity professionals require professional training to acquire quantum literacy. A

multidisciplinary response and holistic approach are needed in quantum computing to protect future digital ecosystems.

This study advances quantum cybersecurity scholarship by integrating fragmented literature into a multi-layered resilience framework that explains how quantum threats interact with technological and regulatory systems. The proposed framework and migration roadmap provide actionable guidance for governments, critical infrastructure operators, and cybersecurity practitioners navigating PQC and QKD adoption

D. Quantum–Cybersecurity Integration Framework

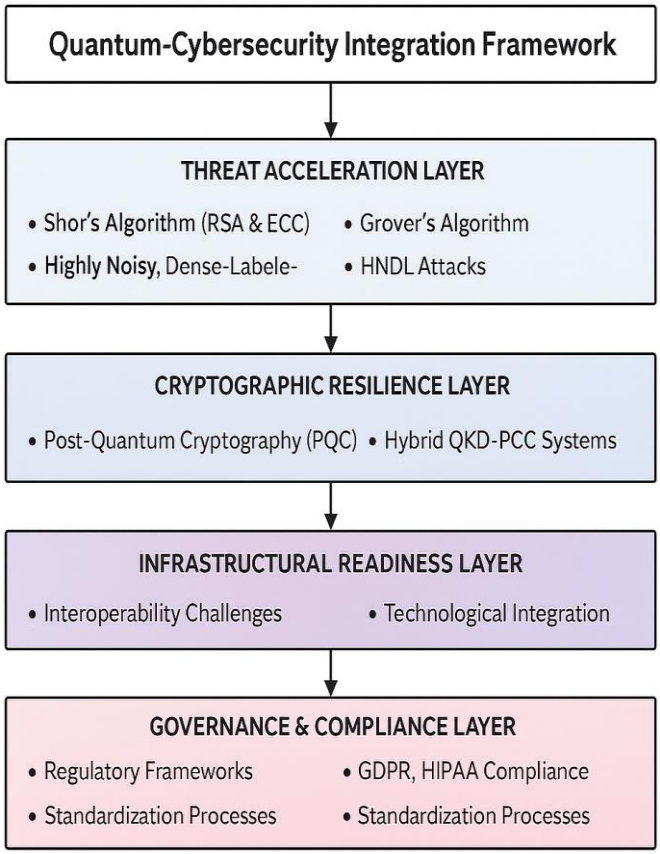

Figure 11. Quantum-Cybersecurity Integration Framework

Based on synthesised findings, we propose a Quantum–Cybersecurity Integration Framework Figure 11, comprising four interlinked pillars: (1) Threat Acceleration Layer, capturing quantum-enabled attacks (Shor/Grover/HNDL); (2) Cryptographic Resilience Layer including PQC and hybrid QKD–PQC systems; (3) Infrastructural Readiness Layer addressing interoperability, scalability, and integration challenges; (4) Governance & Compliance Layer mapping GDPR/HIPAA/NIST readiness. This framework provides practitioners with a structured pathway for quantum-secure transformation.

The Quantum–Cybersecurity Integration Framework provides a structured representation of how emerging quantum threats intersect with technological, infrastructural, and regulatory readiness. At the top, the Threat Acceleration Layer captures the rapidly evolving quantum attack vectors such as Shor's and Grover's algorithms and "Harvest Now, Decrypt Later" strategies that undermine classical encryption. The Cryptographic Resilience Layer highlights the shift toward quantum-safe security mechanisms, particularly Post-Quantum Cryptography (PQC) and hybrid QKD–PQC solutions that combine algorithmic robustness with quantum-enhanced key exchange. The Infrastructural Readiness Layer emphasises the practical challenges of integrating quantum-secure technologies into existing systems, including interoperability constraints, hardware dependencies, and network adaptation requirements. Finally, the Governance & Compliance Layer emphasizes the importance of regulatory frameworks, privacy requirements (e.g., GDPR, HIPAA), and emerging standards in ensuring the responsible and secure adoption of technology. Together, these layers form a holistic roadmap for organisations preparing for a post-quantum cybersecurity landscape.

To operationalise this framework, this study proposes an actionable roadmap presented in Figure 12.

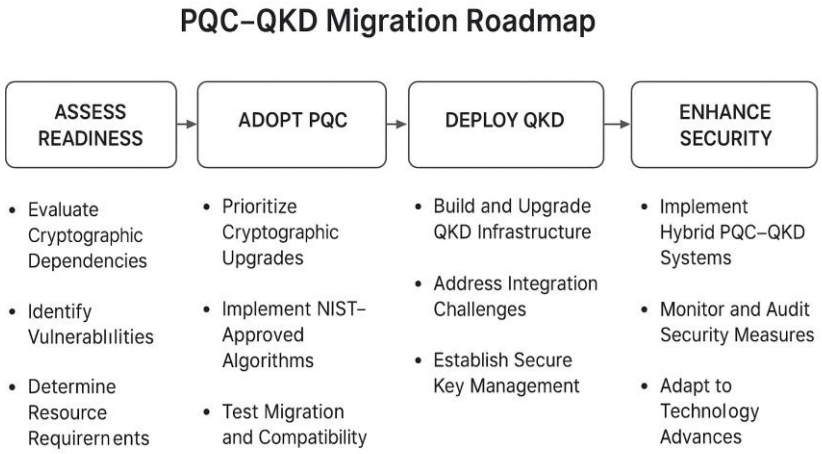

Figure 12. PQC–QKD Migration Roadmap

The PQC–QKD Migration Roadmap provides a strategic pathway for organisations preparing for quantum-resilient security. The process begins with Assess Readiness, which involves identifying cryptographic dependencies, detecting vulnerabilities, and determining organisational resource requirements. The second stage, Adopt PQC, focuses on prioritising cryptographic upgrades, implementing NIST-approved post-quantum algorithms, and conducting compatibility and migration tests. The third phase, Deploy QKD, introduces quantum-based secure key exchange, which necessitates upgrades to QKD infrastructure, the resolution of network integration challenges, and the establishment of secure key management processes. The final stage, Enhance Security, integrates PQC and QKD into hybrid architectures, promotes continuous

monitoring and auditing of cryptographic elements, and ensures adaptive updating as quantum technologies evolve. Together, these stages form a comprehensive roadmap for transitioning toward quantum-secure cyber ecosystems.

E. Limitations of the Study

Articles were extracted from only four digital libraries: IEEE Xplore, Google Scholar, SpringerLink, and ACM, thereby limiting the scope of material required to conduct robust research. The review excludes non-English and grey literature, which may omit industry-driven quantum innovations. Additionally, due to the rapidly evolving nature of quantum technologies, findings may shift as new algorithms and NIST standards mature. Understanding the basis of research by extracting articles written long ago restricts the historical context. These gaps reiterate the need for cautiousness when generalising conclusions and suggesting further studies.

F. Future Works

Future studies should focus on developing systems that can tolerate faults. It should focus on helping policymakers to address integration and performance issues. Future work must also focus on developing practical algorithms and overcoming critical hardware issues. Additionally, capacity-building research should be considered when focusing on the future of quantum computing. This will be achieved by developing cybersecurity training frameworks that encompass both cybersecurity and quantum technology. Lastly, integration of artificial intelligence and quantum computing may create a holistic technical and societal answer. Moreso, future research should empirically validate hybrid QKD-PQC deployment models, investigate sector-specific migration strategies (finance, healthcare, defence), and develop quantum-risk assessment metrics linked to organisational digital maturity

G. Conclusion

Cybersecurity transformation can be realised through the positives and risks brought about by quantum computing. Imminent threats to RSA and ECC cryptographic protocols necessitate protection by Post-Quantum Cryptographic (PQC) solutions and Quantum Key Distribution (QKD). It is also crucial to invest in quantum-awareness and professional training programs to build a workforce that is capable of managing quantum threats. Reliable security frameworks can be established through constant innovation and standardization of quantum technology. This assessment demonstrates that quantum cybersecurity methods are essential for securing digital infrastructures in the rapidly evolving technological landscape. The study concludes that quantum computing poses not merely a cryptographic threat but a systemic disruptor that spans technology, regulation, and digital sovereignty. Transitioning to quantum-secure ecosystems requires coordinated adoption of PQC, hybrid cryptographic models, updated governance frameworks, and quantum-aware workforce development.

H. References

[1] Q. A. Memon, M. Al Ahmad, and M. Pecht, “Quantum Computing: Navigating

the Future of Computation, Challenges, and Technological Breakthroughs," *Quantum Reports*, vol. 6, no. 4, pp. 627–663, 2024, doi: 10.3390/quantum6040039.

[2] Durr-E-Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum Cryptography for Future Networks Security: A Systematic Review," *IEEE Access*, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3504815.

[3] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J. M. Leimeister, "Quantum computing," *Electron. Mark.*, vol. 32, no. 4, pp. 2525–2536, 2022, doi: 10.1007/s12525-022-00570-y.

[4] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities," *2022 1st Int. Conf. AI Cybersecurity, ICAIC 2022*, pp. 1–8, 2022, doi: 10.1109/ICAIC53980.2022.9896970.

[5] Rafiul Azim Jowarder and Sawgat Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," *World J. Adv. Eng. Technol. Sci.*, vol. 13, no. 1, pp. 330–339, 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[6] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," pp. 1–25, 2024.

[7] G. S. Mamatha, N. Dimri, and R. Sinha, "Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era," doi: https://arxiv.org/abs/2403.11741.

[8] K. S. Bhosale, S. Ambre, Z. Valkova-Jarvis, A. Singh, and M. Nenova, "Quantum Technology: Unleashing the Power and Shaping the Future of Cybersecurity," 2023, doi: 10.1109/Lighting59819.2023.10299447.

[9] B. Mutunhu, S. Dube, N. Ncube, and S. Sibanda, "Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology," *Proc. Int. Conf. Ind. Eng. Oper. Manag. Nsukka, Niger.*, pp. 5–7, 2022, [Online]. Available: https://ieomsociety.org/proceedings/2022nigeria/111.pdf.

[10] P. Dixit, R. Kohli, A. Acevedo-Duque, R. R. Gonzalez-Diaz, and R. H. Jhaveri, "Comparing and Analyzing Applications of Intelligent Techniques in Cyberattack Detection," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5561816.

[11] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories," *Appl. Sci.*, vol. 13, no. 9, 2023, doi: 10.3390/app13095700.

[12] B. von Solms and R. von Solms, "Cybersecurity and information security – what goes where?," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018, doi: 10.1108/ICS-04-2017-0025.

[13] N. Ncube, B. Mutunhu, and K. Sibanda, "Land Registry Using a Distributed Ledger," in *2022 IST-Africa Conference, IST-Africa 2022*, 2022, pp. 1–7, doi: 10.23919/IST-Africa56635.2022.9845584.

[14] A. Peslak and D. S. Hunsinger, "What Is Cybersecurity and What Cybersecurity Skills Are Employers Seeking?," *Issues Inf. Syst.*, vol. 20, no. 2,

pp. 62–72, 2019, doi: 10.48009/2_iis_2019_62-72.
[15] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electron.*, vol. 11, no. 14, 2022, doi: 10.3390/electronics11142181.
[16] K. Maguraushe, A. da Veiga, and N. Martins, "A personal information privacy perceptions model for university students," *Inf. Secur. J. A Glob. Perspect.*, vol. 33, no. 4, pp. 394–424, Jul. 2024, doi: 10.1080/19393555.2024.2329554.
[17] S. Chishakwe, N. Moyo, B. M. Ndlovu, and S. Dube, "Intrusion Detection System for IoT environments using Machine Learning Techniques," *2022 1st Zimbabwe Conf. Inf. Commun. Technol. ZCICT 2022*, pp. 1–7, 2022, doi: 10.1109/ZCICT55726.2022.10045992.
[18] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157356–157381, 2020, doi: 10.1109/ACCESS.2020.3019345.
[19] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *Int. J. Sci. Res. Publ.*, vol. 8, no. 7, pp. 495–516, 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.
[20] G. Nkulenu, "Quantum computing : The impending revolution in cryptographic security," pp. 1137–1149, 2024.
[21] E. D. Dahl, "Quantum computing," *Mach. Des.*, vol. 87, no. 1, pp. 36–41, 2015, doi: 10.1145/3402127.3402131.
[22] N. Adriani, "Electronic copy available at : Electronic copy available at :," *Grou*, vol. 23529, no. 2, pp. 1–45, 2018.
[23] J. Choudrie, P. N. Mahalle, and T. Perumal, *ICT for Intelligent systems*, vol. 2. 2024.
[24] G. Nookala *et al.*, "MZ Journals Post-Quantum Cryptography : Preparing for a New Era of Data Encryption," *Post-Quantum Cryptogr.*, vol. 5, no. 2, pp. 1–19, 2024.
[25] C. Paar, J. Pelzl, and T. Güneysu, *Understanding Cryptography From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms Second Edition*. Springer, 2024.
[26] Enoch Oluwademilade Sodiya, Uchenna Joseph Umoga, Olukunle Oladipupo Amoo, and Akoh Atadoga, "Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets," *Glob. J. Eng. Technol. Adv.*, vol. 18, no. 2, pp. 049–064, 2024, doi: 10.30574/gjeta.2024.18.2.0026.
[27] D. Rusca and N. Gisin, "Quantum Cryptography: An Overview of Quantum Key Distribution," *Encycl. Math. Physics, Second Ed. Vol. 1-5*, vol. 1–5, p. V2:211-V2:223, 2024, doi: 10.1016/B978-0-323-95703-8.00103-8.
[28] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum Internet - Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2218–2247, 2021, doi: 10.1109/COMST.2021.3109944.
[29] P. S. Aithal and S. Aithal, "Information Communication and Computation Technology (ICCT) and its Contribution to Universal Technology for Societal Transformation," *… Comput. Technol. Pillar …*, pp. 1–28, 2020.

[30] S. Carvalho, J. V. Carvalho, J. C. Silva, G. Santos, and G. S. de Melo Bandeira, "Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies," *J. Inf. Syst. Eng. Manag.*, vol. 8, no. 2, 2023, doi: 10.55267/iadt.07.13226.
[31] B. Ndlovu and K. Maguraushe, "Balancing Ethics and Privacy in the Use of Artificial Intelligence in Institutions of Higher Learning: A Framework for Responsive AI Systems," *IJIE (Indonesian J. Informatics Educ.*, vol. 9, no. 1, p. 39, 2025, doi: 10.20961/ijie.v9i1.100723.
[32] E. A. Fischer, "Cybersecurity Issues and Challenges: In Brief," 2016.
[33] D. C. Wyld, "David C. Wyld 1 1," *Int. J.*, vol. 1, no. October 2009, pp. 1–20, 2010.
[34] Oyekunle Claudius Oyeniran, Adebunmi Okechukwu Adewusi, Adams Gbolahan Adeleke, Chidimma Francisca Azubuko, and Lucy Anthony Akwawa, "Advancements in quantum computing and their implications for software development," *Comput. Sci. IT Res. J.*, vol. 4, no. 3, pp. 577–593, 2023, doi: 10.51594/csitrj.v4i3.1558.
[35] F. Bova, A. Goldfarb, and R. G. Melko, "Commercial applications of quantum computing," *EPJ Quantum Technol.*, vol. 8, no. 1, pp. 1–13, 2021, doi: 10.1140/epjqt/s40507-021-00091-1.
[36] M. Nofer, K. Bauer, O. Hinz, W. van der Aalst, and C. Weinhardt, "Quantum Computing," *Bus. Inf. Syst. Eng.*, vol. 65, no. 4, pp. 361–367, 2023, doi: 10.1007/s12599-023-00823-w.
[37] A. Mohammed and N. Bank of UAE, "Cyber Security Implications of Quantum Computing: Shor's Algorithm and Beyond."
[38] Olakunle Abayomi Ajala, Chuka Anthony Arinze, Onyeka Chrisanctus Ofodile, Chinwe Chinazo Okoye, and Andrew Ifesinachi Daraojimba, "Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," *Magna Sci. Adv. Res. Rev.*, vol. 10, no. 1, pp. 321–329, 2024, doi: 10.30574/msarr.2024.10.1.0038.
[39] M. L. How and S. M. Cheah, "Forging the Future: Strategic Approaches to Quantum AI Integration for Industry Transformation," *AI*, vol. 5, no. 1, pp. 290–323, 2024, doi: 10.3390/ai5010015.
[40] J. P. Aumasson, "The impact of quantum computing on cryptography," *Comput. Fraud Secur.*, vol. 2017, no. 6, pp. 8–11, 2017, doi: 10.1016/S1361-3723(17)30051-9.
[41] A. M. Elmisery, M. Sertovic, A. Zayin, and P. Watson, "CYBER THREATS IN FINANCIAL TRANSACTIONS Addressing the Dual Challenge of AI and Quantum Computing," no. March, pp. 1–38, 2025.
[42] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," vol. 4, pp. 8–9, 2024.
[43] H. Abulkasim, B. Goncalves, A. Mashatan, and S. Ghose, "Authenticated Secure Quantum-Based Communication Scheme in Internet-of-Drones Deployment," *IEEE Access*, vol. 10, no. August, pp. 94963–94972, 2022, doi: 10.1109/ACCESS.2022.3204793.
[44] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography,"

IEEE Access, vol. 12, no. January, pp. 23206–23219, 2024, doi: 10.1109/ACCESS.2024.3364520.

[45] J. Oliva Del Moral, A. Demarti Iolius, G. Vidal, P. M. Crespo, and J. Etxezarreta Martinez, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 30217–30244, 2024, doi: 10.1109/JIOT.2024.3410702.

[46] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," *CEUR Workshop Proc.*, vol. 3008, pp. 20–28, 2021.

[47] I. B. Djordjevic, "QKD-Enhanced Cybersecurity Protocols," *IEEE Photonics J.*, vol. 13, no. 2, 2021, doi: 10.1109/JPHOT.2021.3069510.

[48] S. R. Hasan, M. Z. Chowdhury, M. Saiam, and Y. M. Jang, "Quantum Communication Systems: Vision, Protocols, Applications, and Challenges," *IEEE Access*, vol. 11, no. December 2022, pp. 15855–15877, 2023, doi: 10.1109/ACCESS.2023.3244395.

[49] K. S. Shim, B. Kim, and W. Lee, "Research on Quantum Key, Distribution Key and Post-quantum Cryptography Key Applied Protocols for Data Science and Web Security," *J. Web Eng.*, vol. 23, no. 6, pp. 813–830, 2024, doi: 10.13052/jwe1540-9589.2365.

[50] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *BMJ*, vol. 339, no. 7716, pp. 332–336, 2009, doi: 10.1136/bmj.b2535.

[51] H. A. Long, D. P. French, and J. M. Brooks, "Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis," 2020, doi: 10.1177/2632084320947559.

[52] W. M. dos Santos, S. R. Secoli, and V. A. de A. Püschel, "The Joanna Briggs Institute approach for systematic reviews," *Rev. Lat. Am. Enfermagem*, vol. 26, p. e3074, 2018.

[53] A. M. Elmisery, M. Sertovic, A. Zayin, and P. Watson, "Cyber Threats in Financial Transactions – Addressing the Dual Challenge of AI and Quantum Computing," *arXiv Prepr.*, no. March, pp. 1–38, 2025.

[54] C. Ai, "Enhancing Cybersecurity for Renewable Energy with Quantum Algorithms and," vol. 39, no. 11, pp. 140–151, 2024.

[55] E. A. Tuli, J. M. Lee, and D. S. Kim, "Integration of Quantum Technologies into Metaverse: Applications, Potentials, and Challenges," *IEEE Access*, vol. 12, no. January, pp. 29995–30019, 2024, doi: 10.1109/ACCESS.2024.3366527.

[56] G. Kato, M. Owari, and M. Hayashi, "Single-shot secure quantum network coding for general multiple unicast network with free one-way public communication," *IEEE Trans. Inf. Theory*, vol. 67, no. 7, pp. 4564–4587, 2021, doi: 10.1109/TIT.2021.3078812.

[57] I. Pedone, A. Atzeni, D. Canavese, and A. Lioy, "Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment," *IEEE Access*, vol. 9, pp. 115270–115291, 2021, doi: 10.1109/ACCESS.2021.3102313.

[58] J. Wu, Y. Chen, C. Zhou, Z. Chen, C. Xu, and L. Song, "A Remote Security Computational Ghost Imaging Method Based on Quantum Key Distribution Technology," *IEEE Access*, vol. 10, pp. 18899–18909, 2022, doi: 10.1109/ACCESS.2022.3144297.

[59] K. F. Hasan *et al.*, "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," *IEEE Access*, vol. 12, no. January, pp. 23427–23450, 2024, doi: 10.1109/ACCESS.2024.3360412.
[60] Y. Shukla, "Decrypting the Future: Quantum Computing's Role in Modern Cryptography," *Ijarcce*, vol. 13, no. 8, pp. 14–18, 2024, doi: 10.17148/ijarcce.2024.13837.
[61] K. S. Shim, Y. H. Kim, I. Sohn, E. Lee, K. Il Bae, and W. Lee, "Design and Validation of Quantum Key Management System for Construction of KREONET Quantum Cryptography Communication," *J. Web Eng.*, vol. 21, no. 5, pp. 1377–1418, 2022, doi: 10.13052/jwe1540-9589.2151.
[62] M. C. Wheatley, "PREMIER JOURNAL OF COMPUTER SCIENCE Quantum Shifts : The Societal Implications of Quantum Computing on Security , Privacy , and the Economy."
[63] M. R. Nosouhi, S. W. A. Shah, L. Pan, and R. Doss, "Bit Flipping Key Encapsulation for the Post-Quantum Era," *IEEE Access*, vol. 11, no. June, pp. 56181–56195, 2023, doi: 10.1109/ACCESS.2023.3282928.
[64] P. S. R. Henrique and R. Prasad, "6G Networks Orientation by Quantum Mechanics," *J. ICT Stand.*, vol. 10, no. 1, pp. 39–62, 2022, doi: 10.13052/jicts2245-800X.1013.
[65] S. Bajric, "Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions," *IEEE Access*, vol. 11, no. October, pp. 128801–128809, 2023, doi: 10.1109/ACCESS.2023.3333020.
[66] J. Binder, L. Hachmann, and S. Luber, "A KPI framework to standardize the measurement of a country's progress in bringing quantum computing into application," *EPJ Quantum Technol.*, vol. 11, no. 1, 2024, doi: 10.1140/epjqt/s40507-024-00245-x.
[67] S. Sodagari, "Integrating Quantum and Satellites: A New Era of Connectivity," *IEEE Access*, vol. 11, no. December, pp. 145101–145110, 2023, doi: 10.1109/ACCESS.2023.3344321.
[68] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. van Meter, "Attacking the Quantum Internet," *IEEE Trans. Quantum Eng.*, vol. 2, 2021, doi: 10.1109/TQE.2021.3094983.
[69] T. Matsumine, H. Ochiai, and J. Shikata, "Quantum Algorithms for the Physical Layer: Potential Applications to Physical Layer Security," *IEEE Access*, vol. 13, no. November 2024, pp. 13988–14009, 2025, doi: 10.1109/ACCESS.2025.3528443.
[70] Z. Yang, M. Zolanvari, and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 1059–1094, 2023, doi: 10.1109/COMST.2023.3254481.
[71] I. B. Djordjevic, "Hybrid CV-DV Quantum Communications and Quantum Networks," *IEEE Access*, vol. 10, pp. 23284–23292, 2022, doi: 10.1109/ACCESS.2022.3154468.
[72] D. J. J. Tom, D. N. P. Anebo, D. B. A. Onyekwelu, A. Wilfred, and R. E. Eyo, "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems," *Int. J. Eng. Adv. Technol.*, vol. 12, no. 5, pp. 25–38, 2023, doi:

10.35940/ijeat.e4153.0612523.
[73] A. A. Abushgra, “How Quantum Computing Impacts Cyber Security,” in *2023 Intelligent Methods, Systems, and Applications (IMSA)*, 2023, pp. 74–79, doi: doi: 10.1109/IMSA58542.2023.10217756.
[74] T. M. Fernandez-Carames and P. Fraga-Lamas, “Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks,” *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
[75] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, “Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement,” *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 3076–3086, 2022, doi: 10.1109/TIA.2022.3159314.
[76] P. N. Nguyen, *Quantum technology: a financial risk assessment*, vol. 7, no. 2. Springer International Publishing, 2025.
[77] T. Nguyen, T. Sipola, and J. Hautamäki, “Machine Learning Applications of Quantum Computing: A Review,” *Eur. Conf. Cyber Warf. Secur.*, vol. 23, no. 1, pp. 322–330, Jun. 2024, doi: 10.34190/eccws.23.1.2258.