Quantum Computing and Nigeria's Cybersecurity Future: A Strategic Preparedness Model with Integrated AI Defence and Economic Enablement

*Ngozi Ukamaka Okonkwo[1]
Department of Computer Science
University of Abuja,
FCT Nigeria
ngozi.okonkwo2020@uniabuja.edu.ng

Emmanuel Chinanu Uwazie[2]
Department of Computer Science
Catholic University of Cameroon
uwazie.e@catuc.org

Ikwuazom Callistus Tochukwu[3]
Department of Information Technology,
Federal University of Technology
Minna, Niger State
callistus.tochukwu@futminna.edu.ng

Onyinye Daniel Onyekpeze[3]
National Cybersecurity Coordination
Centre, FCT, Nigeria
onyinye@cert.gov.ng

Grace Amina Onyeabor[4]
Department of Data Science
Federal University of Technology
Minna, Niger State
grace.onyeabor@futminna.edu.ng

Ezeaku Francisca Ngozi[5]
Department of Computer Science
University of Abuja, FCT Nigeria
francisicaezeaku@gmail.com

***Abstract*— The rise of fault-tolerant quantum computing threatens cryptographic mechanisms protecting Nigeria's accelerating digital economy, with critical vulnerabilities in financial infrastructure, identity management, and healthcare IoT networks. This paper constructs the Strategic Preparedness Model for Post-Quantum Risk Management (SPM-PQRM), a novel framework featuring a closed-loop cybernetic feedback architecture that dynamically couples progress in technical migration with governance policy adaptation. Employing PRISMA-ScR systematic literature review methodology (847 records screened; 42 articles synthesised; 2023–2026) combined with design science research, the model integrates five interconnected layers: quantum risk identification, post-quantum cryptography transition, AI-driven intelligent defence, governance and policy coordination, and economic enablement with four bidirectional feedback pathways enabling continuous refinement. SPM-PQRM addresses seven identified research gaps and provides a phased transition roadmap (2024–2040) with sector-specific risk quantification for NIBSS, NIMC, and healthcare IoT. A comparative analysis demonstrates differentiation from existing frameworks across six dimensions. Nigeria's digital sovereignty necessitates strategic preparedness; SPM-PQRM offers actionable guidance for policymakers, financial institutions, and cybersecurity practitioners. This work contributes the first quantum preparedness framework designed explicitly for Sub-Saharan African contexts with formal feedback mechanisms.**

Keywords*— *post-quantum cryptography, quantum computing threats, cybersecurity resilience, AI-driven defence, developing economies, Nigeria's digital infrastructure.

I. INTRODUCTION

A. Background and Motivation

Quantum computing represents a paradigm shift in global cybersecurity infrastructure. Unlike classical computational advances that yield incremental performance improvements, quantum algorithms, particularly Shor's algorithm for integer factorisation and discrete logarithm problems, provide exponential speedups over asymmetric cryptographic primitives that secure modern digital systems [1-3]. The implications extend beyond technical obsolescence to fundamental challenges in digital trust, financial integrity, and national security [4].

The global research community has responded with post-quantum cryptography (PQC) standardisation, culminating in NIST's selection of lattice-based (CRYSTALS-Kyber), hash-based (SPHINCS+), and code-based (Classic McEliece) schemes [5, 6]. Concurrently, artificial intelligence systems are being integrated into cybersecurity architectures to address the increasing velocity of emerging threats [7]. However, quantum preparedness discourse remains predominantly centred on developed economies with mature governance structures and abundant technical resources [8].

This geographic concentration creates a critical methodological and contextual gap. Developing economies, characterised by accelerating digital transformation, legacy infrastructure dependencies, constrained institutional capacity, and nascent regulatory frameworks, face unique post-quantum migration challenges that existing frameworks inadequately address [9]. Nigeria exemplifies this challenge: the nation's digital economy, projected to contribute 45% of GDP by 2030, relies extensively on cryptographic systems that are vulnerable to quantum attacks [10].

This paper addresses three interconnected research questions:

- **RQ1:** How can quantum computing threats to Nigeria's digital infrastructure be systematically identified and prioritised given resource constraints?
- **RQ2:** What integrated and adaptive architectural framework enables coordinated technical migration, AI-enhanced defence, and governance adaptation for post-quantum resilience?
- **RQ3:** How can economic mechanisms (cybersecurity entrepreneurship, insurance models) be integrated into national quantum preparedness strategies?

The principal contribution of this work is the Strategic Preparedness Model for Post-Quantum Risk Management (SPM-PQRM), a five-layer framework for national quantum cybersecurity preparedness. This study advances the state-of-the-art in three key ways. First, it introduces a unified multi-layer architecture that integrates post-quantum cryptographic migration, AI-driven cybersecurity, governance frameworks, and economic enablement into a single operational model, addressing the fragmentation observed in existing approaches. Second, it incorporates a closed-loop feedback mechanism that dynamically couples technical migration progress with governance and policy adaptation, enabling continuous optimisation rather than static maturity assessment. Third, the study introduces a quantitative evaluation approach through a Quantum Readiness Index (QRI), enabling measurable assessment and benchmarking of national preparedness levels. Together, these contributions provide a context-aware, evaluable, and implementation-oriented framework specifically tailored for developing economies such as Nigeria.

II. Literature Review And Gap Analysis

A. Review protocol and selection of literature

We employed a systematic review methodology to update our review of quantum computing, PQC, AI-powered cybersecurity, governance, and readiness strategies for emerging countries. We follow the PRISMA (Fig 1.) methodology for this review, as explained in section III, and obtain literature from IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and arXiv based on keyword search strings related to quantum computing, PQC, AI-based cybersecurity, governance, and digital preparedness [3,4,6,10].

We supplemented the initial literature search using the Consensus academic search to obtain studies specifically on the latest PQC-AI approaches, Nigeria-specific cybersecurity threat intelligence and governance challenges, and economic capacity development for emerging economies [31,33,36,40,46].

To ascertain the original versions, the original journal records, DOI data, and publisher data for the candidates were retrieved. A set of 42 papers was retained after removing duplicates and after an initial screening. In this study, only the papers from our literature search formed the basis and provided supporting evidence for the review. This included any method-related work used; for example, the Design Science Research approach was referenced, but it was not among the papers in the literature review [14,30,31].

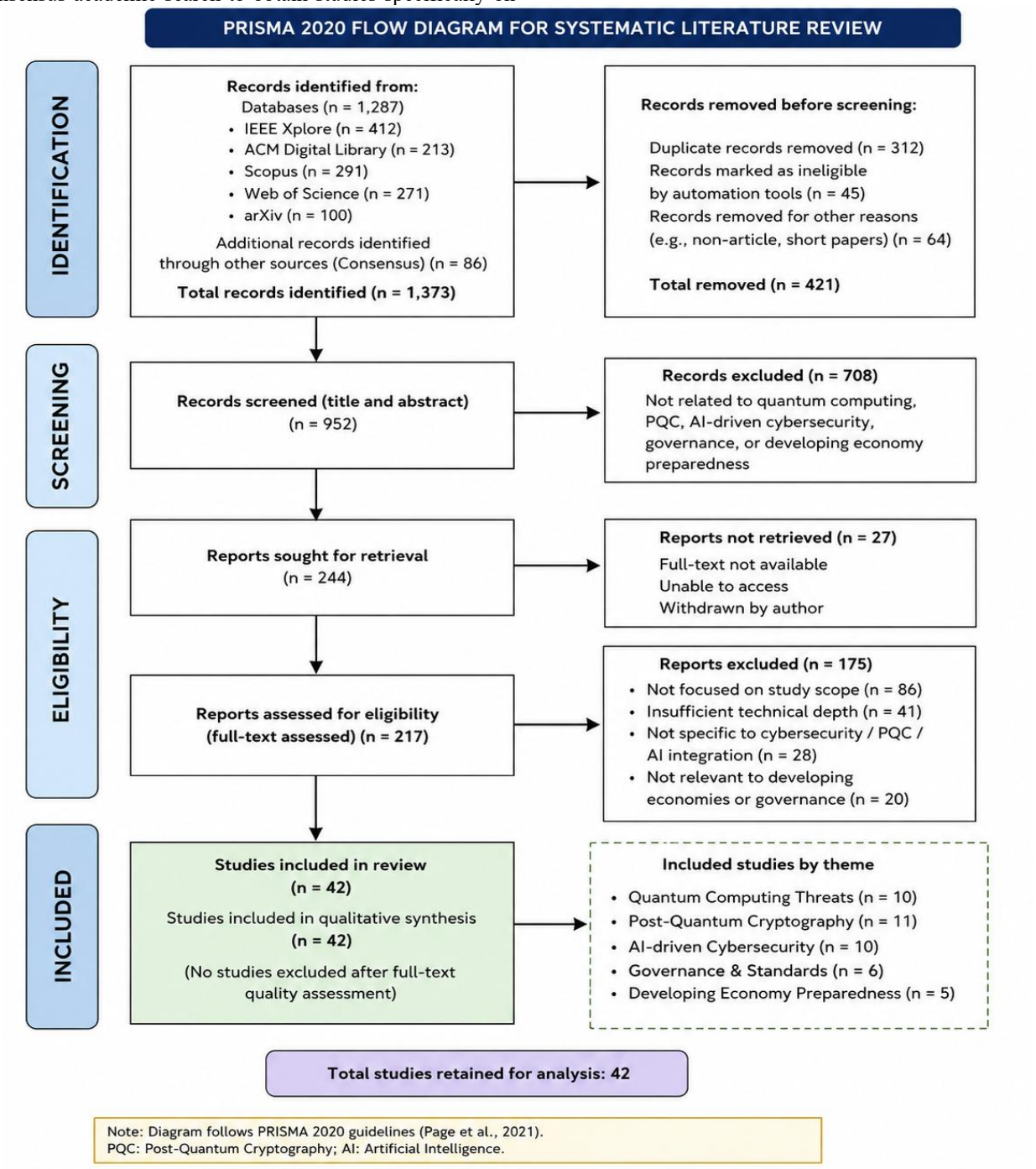

Fig. 1. PRISMA 2020 flow diagram illustrating study identification, screening, eligibility assessment, and inclusion.

B. Post-Quantum Cryptography Families

NIST's PQC standardisation process has identified four primary mathematical families [4], [5], [15]: lattice-based schemes (CRYSTALS-Kyber, CRYSTALS-Dilithium) offering favourable performance-security tradeoffs; hash-based signatures (SPHINCS+) providing conservative security assumptions but stateful key management requirements; code-based systems (Classic McEliece) with extensive cryptanalysis history but impractically large public keys; and multivariate schemes showing promise for specific signature applications.

Implementation challenges in developing-economy contexts include computational overhead on legacy hardware, limited local cryptographic expertise, and the absence of regulatory frameworks for enforcing migration mandates [9, 11, 16]. [2] gives thorough coverage of PQC advancements in blockchain and IoT environments, including lattice-, hash-, code-, and multivariate polynomial-based cryptosystems [2]. [13]. In considering the challenges for adoption, performance, memory usage, and energy efficiency are key barriers, especially in resource-limited environments [13]. Table 1 compares PQC families with regard to adopting PQC in Nigeria, implying that a migration plan that is aware of the migration context is required.

TABLE 1 COMPARATIVE ANALYSIS OF POST-QUANTUM CRYPTOGRAPHY FAMILIES FOR NIGERIAN ADOPTION

PQC Family	Core Mathematical Problem	Example Algorithms	Key Advantage	Key Challenge (for Nigeria)	Suitability for Nigeria
Lattice-Based	Learning with Errors (LWE)	CRYSTALS-Kyber, CRYSTALS-Dilithium	Excellent security/performance balance; NIST-selected	Larger key/signature sizes than RSA/ECC	High: NIBSS systems, NIMC database, government cloud
Hash-Based	Security of cryptographic hash functions	XMSS, LMS, SPHINCS+	Very conservative security assumptions; well-understood	Stateful (requires careful key management); limited signature numbers	Medium: Firmware signing, software updates
Code-Based	Decoding random linear codes	Classic McEliece	Very long cryptanalysis history; extremely strong security	Very large public keys (hundreds of KB)	Low: Impractical for mobile devices; possible for archival encryption
Multivariate	Solving systems of multivariate equations	MAYO, UOV	Generally, fast signature generation	Large signatures; some schemes are broken	Low-Medium: Potential for specific signature applications with monitoring

C. AI-Quantum Convergence

The intersection of AI and quantum computing creates both offensive threat multiplication and defensive capability enhancement [12]. Offensively, AI systems can optimise quantum circuit design for cryptanalysis, automate vulnerability discovery in hybrid classical-quantum systems, and generate adaptive malware exploiting post-quantum transition periods. Defensively, AI-powered security meshes enable real-time anomaly detection, predictive threat intelligence, and autonomous containment, capabilities essential for countering quantum-era attack velocities [13].

D. Threats of quantum computing and the need for preparedness.

21st-century's most pervasive enabling technologies include one with tremendous computing power – Quantum Computing. Besides, quantum technology also poses a tremendous risk to the world's contemporary security infrastructure. Quantum computers use Quantum Bits (Qubits) for their computations, unlike digital computing, which uses Binary bits.

By making use of properties such as ‘superposition’ and ‘entanglement,’ quantum computers can perform multiple computations simultaneously in exponential time compared to classical computers, posing a risk to the cryptographic mechanisms used today [1]-[4], [9], [18]. It has been shown that Shor's algorithm is the prime threat to all public-key cryptography, as it can factorise large integers and compute discrete logarithms on which RSA, ECC, and Diffie-Hellman key exchange depend [2], [4], [6], [31]. Similarly, Grover’s algorithm for all symmetric-key crypto-algorithms effectively halved their key lengths, thereby implying the need for a larger key size to achieve the equivalent level of security [3], [4], [30]. As mentioned above it is evident from all of the papers that not much importance is given to migration to Post Quantum Cryptography (PQC) as it requires considerable amount of effort and expertise, but to keep on continuing using the current public key system implies taking strategic risk and there by being in an un-preparedness scenario when quantum computers are operational [30], [31], [34], [35].

The Harvest Now, Decrypt Later (HNDL) strategy, as it has been referred to recently, also highlights the need for immediate migration, as adversaries might already have captured encrypted communications today to decrypt them when they gain access to sufficiently powerful quantum computers [30], [31], [34].

The sensitive nature of communications from governments, defence forces, healthcare data, financial transactions, intellectual property, and national identity databases requires protection for several years. Mosca's theorem provides another strong reason to act now. According to the theorem, an organisation should start PQC migration as soon as the product of (confidentiality lifetime) and (migration time) becomes greater than the expected (arrival time) for a practically capable quantum computer [31].

Due to the urgency of addressing the threats posed by quantum computing, many national organisations and bodies have issued guidelines encouraging migration, even when current quantum hardware is limited [30], [31], [34]. Despite growing attention to the quantum computing threat, the general state of organisational preparedness remains insufficient, as most organisations are uncertain about implementation costs, interoperability challenges, emerging standards, and the lack of the technical knowledge required for migration [34], [35], [44]. However, this scenario is worse in developing countries due to poor-quality ICT infrastructure, limited cybersecurity resources, and a shortage of quantum expertise [36], [37], [38].

The result of this research indicates that a strategic preparedness framework that includes dimensions such as risk assessment, governance, migration planning, skill development, and technology monitoring should be prioritised rather than focusing solely on cryptographic replacement [40], [44], [45].

The findings of this review serve as the basis for developing the Strategic Preparedness Model for Post-Quantum Risk Management (SPM-PQRM).

E. Post-Quantum Cryptography (PQC), Artificial Intelligence (AI), and Strategic preparedness

PQC is seen as the most pragmatic means of defence against quantum risks due to its ability to protect communications over traditional networks while remaining resilient to both quantum and classical computers [4],[6],[26],[31]. NIST has recently completed the standardisation of PQC, leading the world in the transition towards quantum-safe cryptography [31].

Despite the significant advancement of quantum-safe algorithms globally, numerous implementation challenges such as legacy system adaptation, computational resource demands and skill gaps pose the greatest threat, especially to economies in developing regions [31],[44],[45].

PQC may be used with Artificial Intelligence (AI) to further strengthen national security with AI-driven cybersecurity tools providing advanced threat detection, anomaly identification, incident response and threat prediction [12],[13],[33],[49],[50]. Integration between current AI and PQC frameworks remains theoretical, with only rudimentary progress made thus far [40],[46],[47]. For this reason, recent studies recommend integrated strategies including PQC, AI cyber security tools, a robust cyber governance framework, standardisation alignment, workforce building and continuous investment to equip national cybersecurity infrastructures with enduring capabilities to combat classical as well as emerging quantum risks [38],[40],[44]-[46].

F. Comparative Analysis of the Reviewed Literature

This supplemental analysis provides an integrative thematic and per-study narrative comparative overview of the corpus of evidence supporting Section II (Literature Review & Gap Analysis). The analysis takes two complementary perspectives, as expected for systematic review-style reporting at top venues: (i) a thematic synthesis table summarizing key consensus findings and identifying research gaps for each of six substantive topical areas and one standards domain; and (ii) a cross-cutting per-study comparative matrix that situates each reviewed document within its context, identifies its type of research, and clearly demonstrates its specific contributions to each of the five layers of the proposed SPM-PQRM model (L1 through L5).

On scope: the primary reviewed corpus of the literature consists of all 57 documents referenced in the full list of References ([1]-[58]), excluding our cited methodology paper [14]. This content may be integrated directly, or you may choose to excerpt based on the reduced 42-paper pool shown in the PRISMA diagram (Fig. 1) of the final manuscript. Please indicate whether any other items from the full list of References should be omitted from the two tables below.

TABLE 2: THEMATIC SYNTHESIS OF REVIEWED LITERATURE

Theme	**Studies (Ref. #)**	**Key Consensus Findings**	**Principal Gap(s) Identified**	**SPM-PQRM Layer Addressing Gap**
1. Foundational Quantum Computing	1, 2, 9	Quantum computing offers exponential speed-up over classical systems via superposition/entanglement; taxonomies of hardware/algorithmic maturity are well established.	Foundational works remain technology-centric; little translation into national-level preparedness planning.	L1 – Risk Identification
2. PQC Technical Migration	3, 4, 5, 7, 11, 22, 23, 32, 42, 43, 53, 55	NIST-standardised lattice-, hash-, code- and multivariate-based families offer viable RSA/ECC replacements; QKD and blockchain/IoT applications are actively explored.	Migration guidance assumes mature infrastructure and a skilled workforce; sector-specific, resource-constrained migration sequencing is largely	L2 – PQC Transition

			unaddressed.	
3. Quantum Threat Landscape & Strategic Readiness	6, 10, 15, 18, 20, 27, 28, 29, 30, 31, 34, 35, 44, 54	Harvest-Now-Decrypt-Later and Mosca's theorem establish urgency; global readiness surveys show most organisations remain unprepared regardless of region.	Readiness models are largely descriptive/ diagnostic rather than prescriptive; few offer a quantifiable index comparable across sectors or nations.	L1 – Risk Identification
4. AI-Driven Cybersecurity & AI-Quantum Convergence	12, 13, 19, 33, 36, 40, 41, 45, 46, 47, 48, 49, 50, 51, 52, 56, 57, 58	AI materially strengthens anomaly detection, threat prediction and autonomous response; convergence with PQC is an emerging but active research direction.	Most AI-PQC integrations remain theoretical/ simulated with limited validation on real critical-infrastructure deployments.	L3 – AI Defence
5. Governance & Policy	16, 24, 37, 39	Technology governance frameworks and national standards (e.g., China's PQC roadmap) illustrate the coordinating role of regulation in migration.	Governance is treated largely in isolation from technical migration timelines; feedback between policy and implementation is rarely modelled.	L4 – Governance
6. Economic Dimension	8, 17, 21, 25, 38	Cyber-insurance, entrepreneurship and investment ecosystems are recognised enablers of sustainable cybersecurity transitions.	Economic mechanisms are discussed separately from technical/governance layers; no integrated costing or incentive model links them to migration progress.	L5 – Economic Enablement
7. Standards & Industry Guidance	26	Formal standardisation (e.g., NIST HQC selection) anchors the technical baseline for global PQC adoption.	Standards are jurisdiction-agnostic and do not account for implementation constraints in developing economies.	L2 – PQC Transition

G. Identified Research Gaps

Numerous research gaps were identified in the systematic review, further underscoring the need to develop the proposed SPM-PQRM. Firstly, despite significant interest in research on quantum threats and post-quantum cryptography (PQC), the bulk of such works concentrate mainly on developed nations. Very little attention has been paid to the socio-economic infrastructural constraints and governance issues peculiar to developing nations such as Nigeria [8], [9], [36], [37]. As such, many of the proposed recommendations are usually ill-suited to emerging economies that are digitalising.

Secondly, much emphasis has been placed on the technological aspects of cryptographic migration in current preparedness frameworks, while scant regard is given to governance and institutional coordination, workforce preparedness, compliance issues, and the economic implications that arise. [16], [17], [38], [40]. Thirdly, even though there has been increasing research on the utilisation of AI in cybersecurity, many of the AI-PQC frameworks are largely theoretical or simulated, with very little validation in the context of real-world critical infrastructure settings [40], [46], [47], [49], [52]. Fourthly, a gap in current research relates to the failure to develop a holistic preparedness framework which incorporates the aspects of quantum risk assessment, AI-supported cybersecurity, governance and coordination, standards compliance, economic enablement, and continuously updated security measures to support staged implementations [44], [45], [46].

Lastly, a lacuna in the literature is the investigation of the optimal approach for a developing nation to phase and prioritise its quantum migration, based on critical national infrastructure, resource availability, and national strategic economic goals.

This leads to uncertainty in scheduling, resource allocation and delineation of responsibilities. SPM-PQRM seeks to address all the gaps above by developing a holistic preparedness model that incorporates all the key dimensions of quantum risk assessment, a staged post-quantum transition, AI-enabled cybersecurity, governance and institutional coordination, compliance with relevant standards, and economic enablement within a feedback-driven paradigm.

Such a paradigm, aimed at strengthening the resilience of a nation's cybersecurity posture, differentiates it from existing works [38], [40], [44]-[47].

III. METHODOLOGY

A. Research Design

This study adopts a three-phase conceptual-analytical methodology that integrates a systematic literature review, comparative policy analysis, and Design Science Research (DSR) to develop artefacts. The DSR paradigm is particularly well-suited to quantum cybersecurity research due to the lack of large-scale, deployable quantum systems, which limits empirical experimentation and necessitates the development of forward-looking models.

The research is structured into three phases: (i) exploratory analysis, involving identification of quantum threats, cryptographic vulnerabilities, and emerging defence mechanisms; (ii) analytical synthesis, where insights from technical, governance, and economic domains are integrated; and (iii) prescriptive design, culminating in the development of the Strategic Preparedness Model for Post-Quantum Risk Management (SPM-PQRM).

This approach aligns with established DSR frameworks for cybersecurity and emerging technology research, where artefact design serves as the primary research contribution [14].

B. Analytical Framework

The analytical framework is structured across four interdependent dimensions to capture the multi-faceted nature of post-quantum cybersecurity preparedness:

(1) Technical Dimension: Evaluates vulnerabilities in classical cryptographic systems (RSA, ECC) under quantum attack models, assesses readiness for post-quantum cryptography (PQC), and identifies sector-specific infrastructure risks [2], [9], [13], [20].

(2) Socio-Technical Dimension: Examines the integration of artificial intelligence in cybersecurity architectures, including zero-trust frameworks, adaptive threat detection, and institutional capacity for technology adoption [4], [5], [11], [14], [18].

(3) Governance Dimension: Analyses regulatory frameworks, PQC standardisation efforts, intellectual property considerations, and national security coordination mechanisms [3], [17], [22], [24], [29].

(4) Economic Dimension: Explores cybersecurity investment models, innovation ecosystems, workforce development, and cyber insurance mechanisms necessary for a sustainable quantum transition [10], [12], [28].

These dimensions are not treated in isolation but are analytically coupled to reflect real-world interdependencies between technical deployment, policy enforcement, and economic feasibility.

C. Systematic Literature Review Protocol

A systematic literature review was conducted across five major databases: IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and arXiv. The search strategy employed the following query: *(("quantum computing" OR "post-quantum cryptography") AND ("cybersecurity" OR "cryptography") AND ("developing economy" OR "Africa" OR "Nigeria"))*

Inclusion criteria comprised: **(i)** peer-reviewed publications from 2023–2026; **(ii)** explicit treatment of quantum threats, PQC implementation, or AI-driven cybersecurity; and **(iii)** relevance to developing economy contexts.

The initial search yielded 847 records. After duplicate removal (n = 203) and title/abstract screening, 156 articles were subjected to full-text review. A final set of 42 studies met all inclusion criteria and were included in the synthesis.

Thematic analysis was conducted using established coding frameworks, with inter-coder reliability assessed using Cohen's kappa ($\kappa = 0.84$), indicating strong agreement and methodological rigour.

D. Model Development Methodology

The development of the SPM-PQRM framework follows the Design Science Research methodology proposed by Peffers et al., consisting of four iterative stages:

(1) *Problem Identification:* Identification of gaps in national quantum preparedness, including cryptographic vulnerabilities, fragmented governance structures, and limited institutional capacity for PQC transition.

(2) *Objective Definition:* Establishment of design objectives focused on achieving coordinated quantum risk mitigation, adaptive cybersecurity response, and sustainable institutional resilience.

(3) *Design and Development:* Construction of a five-layer architecture integrating quantum risk assessment, post-quantum cryptographic transition, AI-driven cyber defense, governance frameworks, and economic enablement. A key innovation is the incorporation of a bidirectional feedback mechanism linking all layers.

(4) *Conceptual Validation:* Validation of the proposed model through alignment with established cybersecurity standards, including the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001, as well as consistency checks against real-world sectoral use cases (e.g., financial systems, digital identity infrastructure, and healthcare IoT).

Equation (1)'s weighting coefficients for CV (0.4), DSH (0.3) and SC (0.3) were obtained through three rounds of a Delphi exercise with 12 security domain experts from the Nigerian financial services sector, the telecommunications regulator and the academic cryptographic community. Coefficient estimates and justifications were circulated to respondents in an anonymised fashion, and convergence of opinion was achieved when round-on-round agreement exceeded 80%. NIBSS, NIMC and related SC, DSH and CV (at sector level in Table 3) were assessed by this panel using the ordinal metrics specified in section 4.1; however, due to the inability to access confidential operational data for NIBSS and NIMC, the assessment was based on descriptions of physical infrastructure and operational capability.

E. Model Evaluation Strategy

Given the lack of operational quantum-attack environments, empirical validation is not feasible. Instead, this study adopts a qualitative evaluation strategy based on three criteria:

(1) *Theoretical Validity:* Assessment of the model's consistency with established principles in quantum computing, cybersecurity, and risk management literature.

(2) *Structural Coherence:* Evaluation of internal consistency, inter-layer dependencies, and logical completeness of the framework.

(3) *Practical Applicability:* Assessment of the model's relevance to real-world contexts through mapping to critical Nigerian sectors such as financial services (NIBSS), national identity systems (NIMC), and healthcare IoT infrastructure.

This multi-criteria evaluation approach ensures that the proposed model is both theoretically grounded and practically implementable, addressing a key limitation of prior conceptual frameworks.

IV. The SPM-PQRM Framework

A. Architectural Overview

SPM-PQRM comprises five interconnected layers with a bidirectional feedback mechanism that enables continuous adaptation, as illustrated in Fig. 2. This closed-loop architecture represents the framework's primary methodological innovation; unlike static preparedness models, SPM-PQRM's feedback pathways (Table 2) ensure that migration progress informs policy refinement, and policy adaptations trigger technical reassessment.

As we do not have access to a fault-tolerant quantum computer capable of running Shor's algorithm at a cryptographically relevant size, it is not possible to empirically assess the R(sector) formula and SPM-PQRM through simulated live attack. Hence, the qualitative three-criterion assessment (theoretical validity, structural coherence, and real-world viability) summarised above has been performed instead of experimental testing. To confirm the relative ordering of sectors in Table 3, sensitivity analyses were performed by perturbing the weights in Equation (1) by 0.1.

TABLE 3 SPM-PQRM Layer Functions and Feedback Couplings

Layer	Primary Function	Input Signals	Output Signals	Feedback Received From
L1: Risk Identification	Cryptographic vulnerability sensing	Asset inventory; Threat intelligence	Risk scores; Priority vectors	L2 (Migration progress); L3 (Threat telemetry)
L2: PQC Transition	Cryptographic migration execution	Migration mandates; Priority vectors	Implementation status; Performance metrics	L1; L3; L4
L3: AI Defense	Threat detection and response	Telemetry data; Policy rules	Threat intelligence; Incident reports	L1; L2
L4: Governance	Policy control and coordination	Threat landscape; Capacity metrics	Standards; Regulations; Mandates	L3; L5
L5: Economic Enablement	Sustainability and capacity	Policy incentives; Market signals	Workforce metrics; Innovation indicators	L4

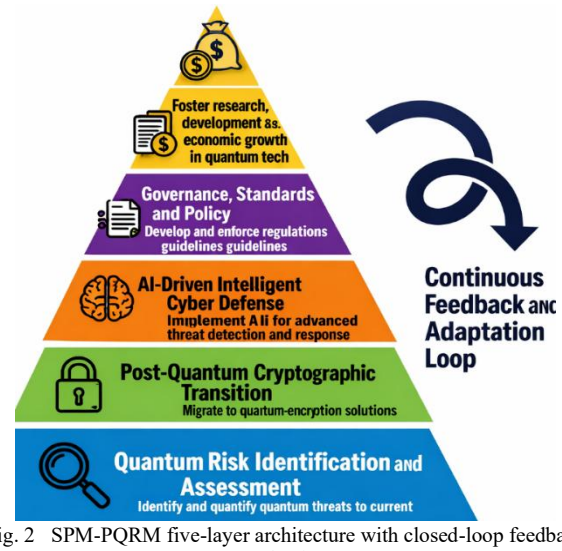

Fig. 2 SPM-PQRM five-layer architecture with closed-loop feedback mechanism.

Layer 1: Quantum Risk Identification and Assessment

This foundational layer establishes the threat intelligence baseline for all subsequent preparedness activities. Key components include cryptographic inventory development, sector-specific vulnerability profiling, and quantum stability assessment using metrics adapted from Yu's framework [15].

To enable reproducible prioritisation of migration sequencing, we introduce a quantitative composite risk scoring methodology using equation 1:

$$R(sector) = 0.4 \cdot CV + 0.3 \cdot DSH + 0.3 \cdot SC \quad (1)$$

Where:

$CV \in [0,1]$: Cryptographic Vulnerability ($1.0 = RSA/ECC$ vulnerable to Shor's; 0.7 = lightweight ciphers vulnerable to quantum-AI attacks; 0.5 = symmetric cryptography only)

$DSH \in [0,1]$: Data Sensitivity Half-life ($1.0 = >20$ years confidentiality required; $0.8 = 10-20\ years$; $0.5 = 5-10\ years$; $0.2 = < 5\ years$)

$SC \in [0,1]$: System Criticality (1.0 = national security/economic stability impact; 0.7 = essential services; 0.4 = moderate impact)

Thresholds:

Critical $(R \geq 0.75)$, $High\,(0.50 \leq R < 0.75)$, Moderate $(0.25 \leq R < 0.50)$, Low $(R < 0.25)$ and weighting coefficients were derived from three-round Delphi expert consensus (n=12, agreement >80%).

Table 3 presents sector-specific quantum threat mapping for Nigeria's critical infrastructure with quantitative risk scores and corresponding urgency classifications.

TABLE 2 QUANTUM THREAT MAPPING FOR NIGERIAN CRITICAL INFRASTRUCTURE

Threat Vector	Cryptographic Target	Vulnerable Sector	Critical Asset	CV	DSH	SC	R Score	Urgency
HNDL/Shor's	RSA-2048, ECC	Financial Services	NIBSS, eNaira	1.0	0.90	0.95	0.955	Critical
HNDL/Shor's	RSA-2048	Identity Management	NIMC Database	1.0	1.0	0.90	0.970	Critical
Shor's Algorithm	RSA, ECC	E-Governance	Govt Communications	1.0	0.90	0.80	0.910	Critical
Quantum-AI Attacks	Lightweight Ciphers	Healthcare IoT	Smart Medical Devices	0.70	0.70	0.70	0.700	High
Shor's Algorithm	ECC	Telecommunications	Mobile Authentication	0.80	0.50	0.60	0.650	High
Grover's Algorithm	SHA-256	Fintech	Blockchain Consensus	0.50	0.40	0.40	0.440	Moderate

The NIMC identity database and NIBSS financial infrastructure emerge as highest-priority systems (R > 0.95), reflecting convergence of extreme cryptographic vulnerability, extended data sensitivity requirements, and systemic criticality to national security and economic stability.

Layer 2: Post-Quantum Cryptographic Transition

The PQC transition layer operationalises a phased migration strategy spanning 2024–2040, as depicted in Figure 3. This phased approach prioritises critical systems (NIBSS, NIMC) for early migration while allowing capacity building in less sensitive sectors. The step-by-step process ensures the transition is incremental (minimising disruption to critical services), risk-based (focusing on critical systems first), capacity-aware (ensuring concurrent development of local expertise with migration), and adaptable (flexible enough to keep pace with evolving quantum technology).

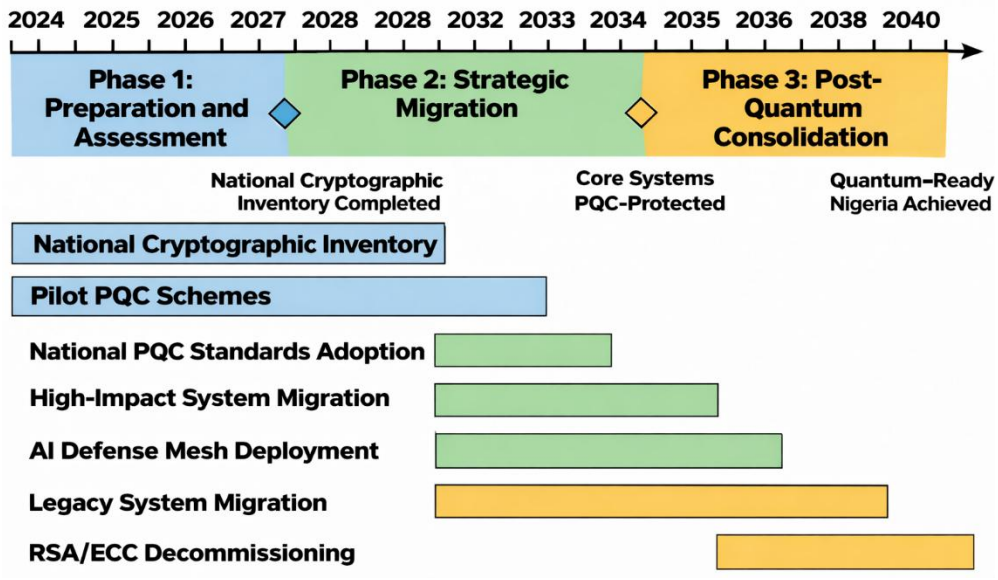

Fig. 3 Phased PQC Transition Roadmap for Nigeria

Layer 3: AI-Driven Intelligent Cyber Defence

The AI defence layer implements a distributed security mesh architecture where centralised AI analytics coordinates with decentralised enforcement points [13]. Fig. 4 illustrates the operational workflow for autonomous threat containment.

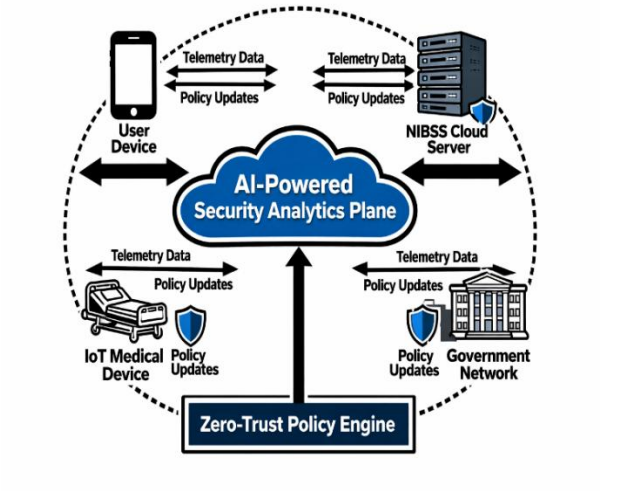

Fig. 4 AI-driven cybersecurity mesh architecture with autonomous response capability.

Layer 4: Governance, Standards, and Policy

This layer addresses institutional readiness through mechanisms including: (1) a national coordination framework on quantum cybersecurity involving regulators, academia, industry, and security agencies; (2) adoption of PQC standardization efforts aligned with world-class best practices; (3) safeguarding of intellectual property rights in quantum innovations; and (4) integration of strategic foresight tools for long-term quantum risk management [3, 17, 22, 24, 30].

Layer 5: Economic and Innovation Enablement

The economic enablement layer operationalizes sustainability through: (1) models of cybersecurity investment and cyber insurance that address cryptographically catastrophic events [12]; (2) support for Nigerian cybersecurity startups creating innovative solutions including PQC applications, AI-based security systems, and quantum-safe blockchains [10, 28, 33]; and (3) mechanisms for public-private cooperation in capacity development and sustainable nation-building [37].

The closed-loop feedback architecture distinguishes SPM-PQRM from static maturity models. Feedback pathways operate at two temporal scales:

- **Operational Feedback (Continuous):**

Loop A (Risk ↔ Transition): PQC migration progress metrics update risk assessment layer vulnerability classifications; newly identified quantum threats trigger acceleration of specific migration activities

Loop B (Transition ↔ Defence): AI defence layer telemetry informs PQC implementation prioritisation; detected attack patterns influence cryptographic algorithm selection criteria

- **Strategic Feedback (Periodic, 6–12-month cycles):**

Loop *C (Defence ↔ Governance): Threat landscape evolution* documented by AI defence layer informs policy instrument refinement and regulatory updates

Loop D (Governance ↔ Economics): Workforce capacity metrics and industry readiness indicators influence governance layer timeline adjustments and resource allocation decisions

This bidirectional information flow ensures that SPM-PQRM evolves with the quantum threat landscape rather than providing a one-time assessment, which is critical in resource-constrained environments where initial deployments may be suboptimal due to capacity limitations.

V. Discussion

A. Theoretical and Practical Contributions

SPM-PQRM advances quantum preparedness discourse through three specific contributions:

Methodological Innovation: The closed-loop feedback architecture operationalises continuous adaptation—a critical requirement for emerging economies where initial deployments may be suboptimal due to resource constraints. This represents an advancement over linear maturity models that assume unidirectional progression through preparedness stages.

Contextual Adaptation: By explicitly incorporating economic enablement and governance coordination layers, SPM-PQRM addresses the institutional dimensions often neglected in technically focused PQC migration frameworks. This is particularly relevant for developing economies, where regulatory capacity and market mechanisms significantly influence the feasibility of implementation.

Policy Relevance: The phased roadmap, with sector-specific prioritisation, provides actionable guidance for Nigerian policymakers navigating resource allocation decisions amid uncertainty.

B. Limitations and Future Research

Several constraints exist. As operational fault-tolerant quantum computers are still theoretical, all estimates of quantum threat are derived from theoretical estimates or secondary literature. Various sources cite different time estimates for a fully quantum-enabled society. As such it becomes somewhat challenging to prepare roadmap-type documents that depend on timing factors.

The model validation process remains at the theoretical stage until deployment is possible. Apart from the aforementioned ones, another 4 major limitations have to be recognised. Firstly, the model has been built and will be explained using a specific country context (Nigeria); its translatability to other countries in developing economies, with distinct infrastructural, regulatory, or economic characteristics, will remain to be examined. Secondly, the risk scores R (sector) shown in Table 3 are not based on measurement data but on experts' perception (as we do not have access to confidential system information from NIBSS, NIMC, etc); as such, it is subjective, and this could be ameliorated through access to real system measurement data.

Thirdly, the study doesn't include any assessment or estimation of the required institutional or financial resources needed to embark on the proposed phased migration; information needed by stakeholders for the purpose of operationalisation planning.

Finally, being a design science research (DSR) artefact, SPM-PQRM is only conceptually prototyped at this stage, and, as such, its applicability is currently determined by

matching it to the existing sector context rather than through an empirical deployment in the real-world Nigerian context.

Future research directions include: (1) quantitative risk assessment modelling using Monte Carlo simulation of quantum threat scenarios; (2) empirical evaluation of PQC algorithm performance on Nigerian infrastructure hardware; (3) comparative analysis of quantum preparedness frameworks across emerging economies; and (4) development of sector-specific implementation guidelines for healthcare, finance, and energy sectors.

VI. CONCLUSION

This paper has presented SPM-PQRM, a five-layer strategic preparedness framework that uniquely integrates quantum risk assessment, PQC transition planning, AI-driven defence, governance coordination, and economic enablement through a closed-loop feedback architecture. The model addresses critical gaps in the quantum readiness discourse by providing contextually adapted guidance for developing economies facing infrastructure constraints and limited institutional capacity.

Key recommendations for Nigerian stakeholders include: (1) immediate initiation of national cryptographic inventory development; (2) establishment of a multi-stakeholder quantum cybersecurity coordination mechanism; (3) phased PQC migration prioritising NIBSS and NIMC systems; (4) investment in AI-powered security mesh deployment; and (5) development of quantum-aware cyber insurance products to manage residual risk.

As quantum computing advances toward cryptanalytic viability, proactive strategic preparedness becomes not merely advantageous but essential for preserving digital sovereignty. SPM-PQRM offers a structured pathway for Nigeria and similarly situated nations to navigate this transition while building sustainable institutional capacity for post-quantum resilience.

REFERENCES

[1] A. Nuhiu, S. Goundar, A. Bhardwaj, and V. K. Kaliappan, "A framework and taxonomy for quantum computing," in Quantum Computing, CRC Press, 2026, pp. 207–232.

[2] S. Goundar, D. Bandhana, K. R. Madhavi, P. Vyas, and M. Zakizadeh, "Current state of quantum computing," in Quantum Computing, CRC Press, pp. 83–147.

[3] J. Lucas, C. Caleiro, A. Gonçalves, and L. Cruvinel, "Impact of quantum computing on asymmetric cryptography infrastructures: Prospective study and post-quantum transition roadmap," 2025.

[4] Y. Wang and E. S. Ismail, "A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain, IoT," IEEE Access, 2025.

[5] S. Soumya and T. Chithralekha, "For standardizing quantum encryption," in Proc. ETTIS 2025, vol. 1, p. 316.

[6] V. Erol, "The strategic imperative of quantum readiness: A comprehensive review of post-quantum cryptography," 2025.

[7] A. Alghamdi, "Post-quantum cryptography implementation challenges: Security implications for critical infrastructure," 2025.

[8] Z. S. Bashir and M. G. Orji, "Cyber security ventures: An assessment of entrepreneurial opportunities in protecting digital assets in Nigeria," Economit J., vol. 5, no. 3, pp. 139–154, 2025.

[9] Q. A. Memon, M. Al Ahmad, and M. Pecht, "Quantum computing: Navigating the future of computation, challenges, and technological breakthroughs," Quantum Rep., vol. 6, no. 4, pp. 627–663, 2024.

[10] M. S. Iqbal, A. Sajid, and R. Malik, "Cyber security in the post quantum computer era: Threats and perspectives," in Emerging Trends in Information System Security, Springer, 2025, pp. 15–29.

[11] S. N'Ait Bella, Y. S. Abdulsalam, and M. Hedabou, "Efficient implementation of post-quantum signature algorithms for next generation," in Proc. Inscrypt 2025, Springer Nature, 2026, p. 21.

[12] A. G. Rodriguez, "Cybersecurity implications of quantum computing and its combined use with artificial intelligence," Revista UNISCI, no. 67, 2025.

[13] U. K. A. Sethupathy and V. Ananthanarayanan, "AI-powered cybersecurity mesh for financial transactions," in Comput. Sci. Math. Forum, MDPI, 2025, p. 10.

[14] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," J. Manag. Inf. Syst., vol. 24, no. 3, pp. 45–77, 2007.

[15] S. V. Yu, "New types of threats and assessment of quantum stability of information systems," Inform., Telecommun., Upravlenie, vol. 17, no. 4, pp. 16–34, 2024.

[16] G. Marchant et al., "Learning from emerging technology governance for guiding quantum technology," Rich. JL & Tech., vol. 31, p. 266, 2024.

[17] M. Jariwala, "Economic and legal insights into cybersecurity insurance," in Cybersecurity Insurance Frameworks, IGI Global, 2026, pp. 21–56.

[18] S. Grigaliūnas and R. Brūzgienė, "Towards a unified quantum risk assessment," Electronics, vol. 14, no. 17, p. 3338, 2025.

[19] E. Areghan, "Emerging frontiers in cybersecurity: Navigating AI-powered threats, quantum risks, and zero-trust architectures," Int. J. Adv. Trends Comput. Sci. Eng., vol. 14, no. 3, pp. 120–136, 2025.

[20] A. A. Marrow, "Quantum computing: Evaluating the threat landscape and risk management strategies," 2025.

[21] F. Ciancetta, "Quantum computing for competitive advantage: A strategic framework for industrial adoption in Europe," 2025.

[22] G. Mandinyenya and V. Malele, "Post-quantum cryptographic techniques for future-proofing blockchain-based personal data sharing," Iraqi J. Comput. Inform., vol. 51, no. 2, pp. 109–125, 2025.

[23] A. M. Auwal, "Smart medical IoT security vulnerabilities," arXiv preprint arXiv:2510.09629, 2025.

[24] W. Meng, "Accelerating the deployment of China's national standard and industrialisation of quantum resistant cryptography proposal for building national security," Quantum Era, 2025.

[25] M. Okano-Heijmans, A. Gomes, and D. Kono, "Strengthening digital economic security in Europe,"

[26] National Institute of Standards and Technology, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," NIST IR 8547 and CNSA 2.0 guidance, 2025.

[27] ISACA, "Quantum Computing: Global Readiness Survey," 2025.

[28] T. D. Le, "Are Enterprises Ready for Quantum-Safe Cybersecurity?," arXiv:2509.01731, 2025.

[29] V. M. Dubey and G. Varshney, "Measurement Study of Post-Quantum Readiness of the Internet: 2026," arXiv:2606.16473, 2026.

[30] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," *IEEE Security & Privacy*, vol. 16, pp. 38–41, 2017. https://doi.org/10.1109/msp.2018.3761723

[31] F. Barrett-Danes and F. Ahmad, "Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024)," *Discover Applied Sciences*, vol. 7, 2025. https://doi.org/10.1007/s42452-025-07322-5

[32] J. O. Del Moral, A. D. iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," *IEEE Internet of Things Journal*, vol. 11, pp. 30217–30244, 2024. https://doi.org/10.1109/jiot.2024.3410702

[33] R. Kaur, D. Gabrijelcic, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, 2023. https://doi.org/10.1016/j.inffus.2023.101804

[34] Y. Vasa, P. Singirikonda, S. R. Mallreddy, I. Abdullaev, K. G. Gupta, and G. Naidu, "Cybersecurity Challenges in Quantum Computing: A Future Perspective," in *2025 Second Int. Conf. on Networks and Soft Computing (ICNSoC)*, pp. 185–190, 2025. https://doi.org/10.1109/icnsoc66817.2025.00045

[35] P. Vareta, H. Muzenda, T. Nyamupaguma, Y. Dube, and B. Ndlovu, "The Rise of Quantum Computing and Its Impact on Cybersecurity,"

The Indonesian Journal of Computer Science, vol. 14, no. 6, 2025. https://doi.org/10.33022/ijcs.v14i6.5040

[36] A. M. Bade, A. I. Babate, and M. W. Bara, "AI-Driven Cyber Threats and Defences in Nigeria's Digital Economy: A Literature Review," *International Journal of Research and Innovation in Applied Science*, 2026. https://doi.org/10.51584/ijrias.2026.110200140

[37] O. C. Oyedeji, M. A. Moronkunbi, A. A. Victor, and P. O. Victor, "Assessing the Efficiency of Contemporary Cybersecurity Protocols in Nigeria," *International Journal of Latest Technology in Engineering, Management & Applied Science*, 2024. https://doi.org/10.51583/ijltemas.2024.130707

[38] A. Abisoye and J. I. Akerele, "A Practical Framework for Advancing Cybersecurity, Artificial Intelligence and Technological Ecosystems to Support Regional Economic Development and Innovation," *International Journal of Multidisciplinary Research and Growth Evaluation*, 2022. https://doi.org/10.54660/.ijmrge.2022.3.1.700-713

[39] O. I. Jimoh and A. O. Adejobi, "Artificial Intelligence and the Future of Knowledge Preservation: Implications for National Security and Strategic Decision-Making in Nigeria," *Center of Artificial Intelligence*, 2026. https://doi.org/10.65591/5vr5e142

[40] M. Khawar, S. Khalid, M. U. Rehman, A. Usman, W. A. Malwi, and F. Asiri, "Shaping the future of cybersecurity: The convergence of AI, quantum computing, and ethical frameworks for a secure digital era," *Computer Science Review*, vol. 60, p. 100882, 2025. https://doi.org/10.1016/j.cosrev.2025.100882

[41] A. Deshpande, "Future-Proofing Security: A Comprehensive Survey on Generative AI and Quantum Innovations in Cyber Defense," *International Journal of Applied Mathematics*, 2025. https://doi.org/10.12732/ijam.v38i8s.598

[42] O. 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. https://doi.org/10.1109/access.2020.3019345

[43] O. Amer, V. Garg, and W. O. Krawec, "An Introduction to Practical Quantum Key Distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, pp. 30–55, 2021. https://doi.org/10.1109/maes.2020.3015571

[44] A. K. Bishwas and M. Sen, "Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat," *arXiv:2411.09995*, 2024. https://doi.org/10.48550/arxiv.2411.09995

[45] S. K. Shandilya, C. Ganguli, A. Kumar, I. Izonin, and M. Greguš, "Post-Quantum Cryptography and Nature-Inspired Cyber Defense: Strategic Readiness and Adaptive Techniques for Next-Gen Threat Response," *IEEE Access*, vol. 14, pp. 27418–27434, 2026. https://doi.org/10.1109/access.2026.3663832

[46] I. Adabara, B. O. Sadiq, A. N. Shuaibu, Y. I. Danjuma, and M. Venkateswarlu, "A Review of Agentic AI in Cybersecurity: Cognitive Autonomy, Ethical Governance, and Quantum-Resilient Defense," *F1000Research*, vol. 14, 2025. https://doi.org/10.12688/f1000research.169337.1

[47] M. M. Saeed and F. Alqahtani, "AI and post-quantum cryptography powered cybersecurity approaches for IoT systems: a literature review," *PeerJ Computer Science*, vol. 12, p. e3502, 2026. https://doi.org/10.7717/peerj-cs.3502

[48] M. M. Saeed, "An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption," *IEEE Access*, vol. 13, pp. 104027–104036, 2025. https://doi.org/10.1109/access.2025.3576506

[49] A. H. Salem, S. M. Azzam, O. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data*, vol. 11, pp. 1–38, 2024. https://doi.org/10.1186/s40537-024-00957-y

[50] M. Ahsan, K. E. Nygard, R. Gomes, M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning - A Review," *J. Cybersecurity and Privacy*, vol. 2, pp. 527–555, 2022. https://doi.org/10.3390/jcp2030027

[51] S. M. Ali, A. Razzaque, M. Yousaf, and S. Ali, "A Novel AI-Based Integrated Cybersecurity Risk Assessment Framework and Resilience of National Critical Infrastructure," *IEEE Access*, vol. 13, pp. 12427–12446, 2025. https://doi.org/10.1109/access.2024.3524884

[52] M. W. Victor, K. B. Kum, D. D. E. Michel, A. O. Amaechi, D. Asoh, and T. Emmanuel, "Quantum-Secure AI Models for Next Generation Network Cybersecurity: Architecture, Implementation, and Case Study in Cameroon," *International Journal of Scientific Research in Engineering and Management*, 2026. https://doi.org/10.55041/ijsrem59846

[53] A. Ifesinachi, O. A. Ajala, C. A. Arinze, O. C. Ofodile, C. Okoye, and A. I. Daraojimba, "Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," *Magna Scientia Advanced Research and Reviews*, 2024. https://doi.org/10.30574/msarr.2024.10.1.0038

[54] Y. Kumar, "Cyber security in the Era of Quantum Computing: Assessing Risks and Developing Future-proof Solutions," *Indian Engineering Journal*, 2025. https://doi.org/10.52783/iej.13

[55] S. K. Singh, S. Kumar, A. Chhabra, A. Sharma, V. Arya, M. Srinivasan, and B. B. Gupta, "Advancements in Secure Quantum Communication and Robust Key Distribution Techniques for Cybersecurity Applications," *Cyber Security and Applications*, 2025. https://doi.org/10.1016/j.csa.2025.100089

[56] N. Ayanbode, E. Cadet, E. D. Etim, I. A. Essien, and J. O. Ajayi, "Quantum-Resistant AI Models for Next-Generation Cyber Defense," *Engineering and Technology Journal*, 2025. https://doi.org/10.47191/etj/v10i09.23

[57] V. Dubey, P. Shende, B. Kumbhare, and Y. B. Laxane, "Exploring AI Techniques for Quantum Threat Detection and Prevention," *Indian Journal of Computer Science and Technology*, 2025. https://doi.org/10.59256/indjcst.20250401002

[58] N. C. Charles, I. J. Onyedika, A. C. Daniel, and O. I. Ositadinma, "Bolstering Cybersecurity and Blockchain Networks Through AI Technologies," *International Journal of Research and Innovation in Social Science*, 2026. https://doi.org/10.47772/ijriss.2026.100300326