International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-12, Issue-3; May-Jun, 2026
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.123.36

Quantum Computing and AI in Cybersecurity

Muhammad Ateeq Anjum

weecoode@gmail.com

Received: 16 May 2026; Received in revised form: 10 Jun 2026; Accepted: 13 Jun 2026; Available online: 17 Jun 2026

Abstract *— Rapid advances in quantum computing and artificial intelligence (AI) are reshaping cybersecurity by enhancing defensive capabilities while simultaneously introducing unprecedented threats to existing cryptographic systems. This paper examines the convergence of quantum computing and AI within the context of Pakistan's emerging digital economy and its distinct geopolitical and environmental security challenges. As Pakistan continues to rely on classical cryptographic standards such as RSA and ECC, it faces growing risks from quantum-enabled attacks and increasingly sophisticated AI-driven cyber threats. Drawing on local literature, recent state-level cyber incidents in 2026, and emerging defense strategies, this study highlights the need for quantum-safe security frameworks, stronger data protection standards, and AI-driven cyber resilience in developing economies.*

Keywords *— **Quantum computing, artificial intelligence, cybersecurity, Pakistan business market, cryptography, PECA, 5th-generation warfare, critical infrastructure, climate-induced digital vulnerability.***

I. BACKGROUND

The convergence of quantum computing and artificial intelligence (AI) is fundamentally transforming the global cybersecurity landscape, creating both unprecedented opportunities and emerging security challenges. For developing digital economies such as Pakistan, this technological evolution represents a significant paradigm shift that demands urgent strategic attention. Quantum computing, powered by quantum bits (qubits) and the principles of superposition and entanglement, has the potential to perform complex computations exponentially faster than classical computing systems.

While this capability promises breakthroughs across various sectors, it simultaneously threatens the cryptographic foundations that secure modern digital infrastructures. Widely deployed encryption standards such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), which currently protect Pakistan's financial technology (FinTech) platforms, e-governance services, telecommunications networks, and military communication systems, could become vulnerable to future quantum-enabled attacks.

At the same time, artificial intelligence is increasingly being leveraged by both defenders and adversaries in cyberspace. Advanced machine learning algorithms enable cybercriminals and state-sponsored threat actors to automate reconnaissance, identify system vulnerabilities, evade traditional signature-based detection mechanisms, and execute highly personalized phishing and social engineering campaigns at scale. The growing sophistication of AI-powered cyberattacks presents a substantial challenge to organizations that continue to rely on conventional security architectures. Conversely, AI-driven cybersecurity solutions offer enhanced capabilities in threat intelligence, anomaly detection, incident response, and predictive risk assessment, creating a dynamic environment where offensive and defensive technologies are evolving simultaneously.

Pakistan's rapid digital transformation further amplifies these challenges. With more than 120 million internet users and increasing adoption of

digital banking, cloud computing, e-commerce platforms, and smart governance initiatives, the country is becoming increasingly dependent on secure digital ecosystems. However, this transition is complicated by aging technological infrastructure, uneven cybersecurity maturity across sectors, shortages of specialized cybersecurity professionals, and the delayed implementation of a comprehensive Personal Data Protection framework. These factors collectively increase the country's exposure to sophisticated cyber threats and potential data breaches.

Moreover, cybersecurity in Pakistan cannot be examined in isolation from the broader context of environmental security concerns and regional geopolitical tensions. The country's strategic position, cross-border digital dependencies, and exposure to information warfare have elevated cybersecurity into a critical component of national security. These challenges are often discussed within the framework of fifth-generation warfare (5GW), where cyber operations, information manipulation, economic disruption, and psychological influence campaigns are employed alongside traditional military strategies. The integration of AI into such operations further increases their scale, precision, and effectiveness, while future quantum capabilities may significantly alter the balance of cyber power among state and non-state actors.

Against this backdrop, this paper explores the dual impact of quantum computing and artificial intelligence on Pakistan's cybersecurity ecosystem. It examines the vulnerabilities of existing cryptographic infrastructures, evaluates the risks posed by AI-enabled cyber threats, and assesses the readiness of Pakistan's public and private sectors for the transition toward post-quantum cryptography. Furthermore, the study investigates how organizations can leverage AI-driven defense mechanisms, strengthen data protection standards, and develop resilient cybersecurity frameworks capable of addressing both emerging technological threats and the unique geopolitical challenges facing developing nations.

II. LITERATURE REVIEW

The emergence of quantum computing has fundamentally altered contemporary cybersecurity discourse, particularly regarding the long-term viability of existing cryptographic systems. The theoretical foundation for this concern was established by Shor (1994), who demonstrated that a sufficiently powerful quantum computer could efficiently solve integer factorization and discrete logarithm problems, thereby compromising widely used public-key cryptographic schemes such as RSA and Elliptic Curve Cryptography (ECC).

Subsequent studies have reinforced the significance of this threat, warning that quantum-enabled adversaries could eventually decrypt sensitive information protected by current encryption standards (Mosca, 2018; Chhetri et al., 2025). As a result, organizations worldwide are increasingly concerned about "harvest now, decrypt later" attacks, whereby encrypted data collected today may be decrypted in the future once large-scale quantum computers become operational (Gidney & Ekerå, 2021).

In response to these developments, the National Institute of Standards and Technology (NIST) launched a global initiative to identify and standardize quantum-resistant cryptographic algorithms. Following several rounds of evaluation, NIST formally selected lattice-based and hash-based cryptographic algorithms, including ML-KEM (formerly CRYSTALS-Kyber), ML-DSA (formerly CRYSTALS-Dilithium), and SLH-DSA (formerly SPHINCS+), as foundational components of future post-quantum security architectures (NIST, 2024). Researchers argue that the adoption of post-quantum cryptography (PQC) is essential for maintaining confidentiality, integrity, and authenticity in the quantum era (Chen et al., 2016; Ahmed et al., 2025). Furthermore, crypto-agility—the ability to rapidly replace cryptographic algorithms in response to emerging threats—has been identified as a critical capability for organizations transitioning toward quantum-safe infrastructures (Mosca, 2018).

While developed nations have initiated comprehensive post-quantum migration strategies, existing literature suggests that developing economies remain significantly underprepared. In Pakistan, cybersecurity readiness is constrained by regulatory fragmentation, limited technical expertise, inadequate cybersecurity investment, and inconsistent

implementation of security policies (Khan & Malik, 2023).

Although legislative instruments such as the Prevention of Electronic Crimes Act (PECA) 2016 and the National Cyber Security Policy 2021 provide a regulatory framework, researchers consistently highlight deficiencies in enforcement, institutional coordination, and organizational compliance (Ali et al., 2024). As Pakistan continues to expand its digital economy through online banking, e-commerce, cloud computing, and e-governance initiatives, these implementation gaps create substantial vulnerabilities within critical information infrastructures.

The financial sector represents one of the most exposed components of Pakistan's digital ecosystem. According to the State Bank of Pakistan (SBP, 2024), the rapid expansion of digital banking and fintech services has increased the sector's susceptibility to cyber threats, including phishing attacks, ransomware campaigns, identity theft, and financial fraud. Financial stability reports published by the SBP emphasize that cyber incidents within a single institution can generate systemic consequences due to the interconnected nature of modern financial networks (SBP, 2024).

Similar concerns have been raised by cybersecurity researchers, who argue that financial institutions in developing countries often lack the technological maturity necessary to counter increasingly sophisticated cyberattacks (Iqbal & Ahmed, 2024). These vulnerabilities become even more significant when viewed through the lens of future quantum-enabled threats capable of undermining the cryptographic foundations of financial transactions and digital identity systems.

Alongside quantum risks, artificial intelligence has emerged as a transformative force in cybersecurity. Contemporary studies demonstrate that machine learning and generative AI technologies are increasingly utilized by threat actors to automate reconnaissance activities, identify exploitable vulnerabilities, evade traditional detection mechanisms, and conduct highly personalized phishing and social engineering campaigns (Brundage et al., 2018; ENISA, 2025). AI-powered malware can adapt dynamically to defensive measures, making it substantially more difficult to detect than conventional malicious software. Conversely, AI has also become an essential component of modern cybersecurity defense, supporting threat intelligence, anomaly detection, behavioral analytics, and automated incident response (IBM Security, 2025). Consequently, cybersecurity scholars characterize AI as a dual-use technology that simultaneously strengthens defensive capabilities while amplifying offensive cyber operations (Buchanan et al., 2022).

Recent literature has increasingly recognized the relationship between environmental security and cybersecurity, particularly in climate-vulnerable developing nations such as Pakistan. The catastrophic floods of 2022 and subsequent climate-induced disasters exposed significant weaknesses within emergency communication systems, humanitarian databases, and digital relief distribution platforms (UNDP, 2023).

Research indicates that emergency technological deployments frequently prioritize operational continuity over cybersecurity safeguards, resulting in inadequate encryption, weak authentication mechanisms, and insufficient endpoint protection (World Bank, 2023). Consequently, sensitive citizen information, including biometric records and digital identities, becomes vulnerable to unauthorized access and exploitation during humanitarian crises. Scholars argue that climate-related disruptions should therefore be considered a growing cybersecurity concern rather than merely an environmental challenge (Kshetri, 2023).

Critical infrastructure security represents another major concern identified in the literature. Pakistan's persistent energy shortages, aging power infrastructure, and increasing reliance on cloud computing and hybrid work environments have significantly expanded the attack surface available to cyber adversaries (Asian Development Bank, 2024). Studies indicate that disruptions affecting telecommunications networks, energy systems, transportation infrastructure, and digital service providers can generate cascading cybersecurity risks across multiple sectors (CISA, 2024). Furthermore, AI-enabled attack automation allows adversaries to exploit infrastructure vulnerabilities at unprecedented speed and scale, increasing the likelihood of large-scale cyber incidents (ENISA,

2025). Researchers therefore advocate for integrated security strategies that combine cyber resilience, infrastructure modernization, and risk management frameworks to address emerging technological threats.

Finally, cybersecurity research increasingly situates Pakistan's digital security challenges within the broader framework of geopolitical competition and fifth-generation warfare (5GW). Modern conflicts are no longer confined to conventional military engagements but increasingly involve cyber espionage, information warfare, economic disruption, and digital influence operations (Hoffman, 2021).

Artificial intelligence has enhanced the effectiveness of these operations by enabling automated disinformation campaigns, deepfake generation, and large-scale psychological influence activities (Buchanan et al., 2022). Future advances in quantum computing may further reshape the strategic balance of cyber power by undermining existing encryption systems and enabling unprecedented intelligence-gathering capabilities. Despite growing international attention to quantum-safe security and AI-driven cyber defense, a significant research gap remains regarding Pakistan's preparedness for the convergence of quantum computing, artificial intelligence, environmental security challenges, and geopolitical cyber threats. Addressing this gap is essential for developing resilient cybersecurity frameworks capable of supporting Pakistan's rapidly expanding digital economy.

III. RESEARCH METHODOLOGY

This study adopts a qualitative, exploratory, and data-driven research methodology to examine the emerging cybersecurity implications of quantum computing and artificial intelligence (AI) within Pakistan's evolving digital economy. Given the relatively nascent nature of quantum technologies and the limited availability of localized empirical studies, a qualitative approach was deemed most appropriate for analyzing the intersection of technological, regulatory, environmental, and geopolitical factors influencing cybersecurity resilience in Pakistan.

The research is primarily based on a comprehensive review of secondary data sources, including peer-reviewed academic literature, industry reports, cybersecurity threat assessments, government publications, legislative frameworks, and policy documents published between 2020 and 2026. Key sources include reports issued by the National Institute of Standards and Technology (NIST), the State Bank of Pakistan (SBP), the National Cyber Emergency Response Team (PKCERT), the Prevention of Electronic Crimes Act (PECA), the National Cyber Security Policy, and international cybersecurity organizations such as ENISA, IBM Security, and the World Economic Forum. These sources provide insights into global developments in post-quantum cryptography, AI-enabled cyber threats, and cybersecurity governance while allowing for contextual analysis within Pakistan's business environment.

The study employs a comparative analytical framework to assess the theoretical capabilities of quantum algorithms, particularly Shor's Algorithm (Shor, 1994) and Grover's Algorithm (Grover, 1996), against the current cybersecurity posture of Pakistan's commercial and public sectors. The analysis examines how future quantum computing capabilities may affect existing cryptographic infrastructures, including RSA and ECC-based systems that secure financial services, telecommunications, e-governance platforms, and critical national infrastructure. Simultaneously, the research evaluates the growing role of AI in both cyber offense and cyber defense, considering its implications for threat detection, automated attacks, fraud prevention, and cybersecurity resilience.

The conceptual framework guiding this study is illustrated as follows:

Global Quantum and AI Threat Landscape → Geopolitical and Environmental Security Factors → Cybersecurity Impact on Pakistan's Digital Economy

This framework facilitates an integrated examination of how emerging technological threats interact with Pakistan's unique geopolitical realities, environmental security challenges, and digital transformation initiatives. Particular attention is given to the influence of climate-related disruptions, critical infrastructure vulnerabilities, and fifth-generation warfare (5GW) dynamics on the country's cybersecurity preparedness.

To strengthen the practical relevance of the analysis, the study synthesizes quantitative indicators and threat intelligence data obtained from publicly available reports presented before the Senate Standing Committee on Information Technology and Telecommunication, cybersecurity assessments published by the State Bank of Pakistan, and industry surveys focusing on financial institutions, fintech organizations, and digital service providers. These datasets are analyzed to identify trends in cyber incidents, financial fraud, ransomware attacks, data breaches, and organizational cybersecurity maturity across Pakistan's commercial sector.

Furthermore, the research evaluates the feasibility of transitioning toward post-quantum cryptographic standards by examining the technical, financial, and organizational constraints faced by Small and Medium Enterprises (SMEs), which constitute a significant portion of Pakistan's economy. Factors such as implementation costs, workforce readiness, infrastructure limitations, regulatory support, and cybersecurity awareness are considered when assessing the practicality of adopting quantum-safe security frameworks. This assessment enables the identification of potential barriers and strategic pathways for enhancing cyber resilience within resource-constrained business environments.

While the study draws upon the most recent data and policy developments available up to 2026, it acknowledges certain limitations. The rapidly evolving nature of quantum computing and AI technologies means that future technological breakthroughs may alter current risk assessments. Additionally, the scarcity of Pakistan-specific empirical research on post-quantum cybersecurity necessitates reliance on international studies and comparative analyses. Nevertheless, the integration of global cybersecurity trends with localized economic, environmental, and geopolitical considerations provides a comprehensive foundation for understanding Pakistan's preparedness for the emerging quantum and AI-driven cybersecurity landscape.

IV. FINDINGS AND DISCUSSION

Emerging Quantum Threats to Pakistan's Financial Ecosystem

The rapid advancement of quantum computing presents a significant long-term challenge to Pakistan's financial sector, which increasingly relies on digital banking platforms, mobile payment systems, cloud-based financial services, and electronic transaction networks. Existing cryptographic infrastructures deployed across banking applications, fintech platforms such as Easypaisa and JazzCash, and interbank communication systems predominantly depend on RSA and ECC encryption standards. However, research originating from Shor's (1994) groundbreaking quantum algorithm demonstrates that a sufficiently powerful quantum computer could efficiently solve the mathematical problems underlying these cryptographic mechanisms, rendering them ineffective against future attacks.

Although large-scale cryptographically relevant quantum computers are not yet commercially available, cybersecurity researchers warn that organizations must prepare for future "harvest now, decrypt later" scenarios, where adversaries collect encrypted data today with the intention of decrypting it once quantum capabilities mature (Mosca, 2018; NIST, 2024). For Pakistan's rapidly expanding digital economy, such a development would have serious implications for financial confidentiality, transaction integrity, customer privacy, and institutional trust. A successful compromise of financial cryptographic systems could undermine confidence in digital banking services and disrupt critical economic activities.

The literature review identified post-quantum cryptography (PQC) as the primary defense against quantum-enabled attacks. However, Pakistan faces substantial barriers to PQC adoption. These include a shortage of specialized cybersecurity professionals with expertise in quantum-safe cryptography, limited awareness among corporate leadership regarding quantum risks, and constrained cybersecurity investment budgets, particularly among small and medium-sized enterprises (SMEs). Consequently, many organizations continue to prioritize short-term operational requirements over long-term cryptographic modernization. This implementation gap increases the likelihood that Pakistan's financial institutions will face significant migration challenges

as global cybersecurity standards transition toward NIST-approved post-quantum algorithms.

AI-Enabled Cyber Threats and the Evolution of Attack Methodologies

The findings indicate that artificial intelligence has transformed the cyber threat landscape from isolated attacks to highly automated and adaptive threat campaigns. Unlike conventional cyberattacks that require significant human intervention, AI-powered attacks leverage machine learning algorithms to automate reconnaissance, vulnerability identification, phishing campaigns, malware deployment, and lateral network movement. These developments have substantially reduced the cost and technical barriers associated with conducting sophisticated cyber operations.

Cybersecurity reports and threat intelligence assessments from 2026 indicate a notable increase in cyber incidents targeting both public and private organizations in Pakistan. Recorded attacks involved web application exploitation, distributed denial-of-service (DDoS) attacks, ransomware campaigns, and supply-chain compromises affecting critical government and commercial systems. The analysis suggests that supply-chain attacks have become particularly effective because threat actors increasingly target smaller third-party vendors with weaker security controls as entry points into larger organizations. This trend reflects global observations that cybercriminals frequently exploit interconnected digital ecosystems rather than attacking primary targets directly.

Furthermore, the emergence of Generative Artificial Intelligence (GenAI) has significantly enhanced the effectiveness of social engineering operations. Advanced language models enable attackers to create highly convincing phishing emails, fraudulent business communications, and multilingual scams tailored to local linguistic and cultural contexts. In Pakistan, where business communication commonly occurs in both Urdu and English, AI-generated content can closely mimic authentic organizational communication patterns, making detection considerably more difficult. Similarly, the growing use of deepfake technologies presents additional risks by enabling attackers to impersonate executives, government officials, and financial authorities to facilitate unauthorized transactions, manipulate public opinion, or conduct corporate fraud.

These findings support existing research that characterizes AI as a dual-use technology capable of strengthening both cyber defense and cyber offense (Buchanan et al., 2022). While AI-powered security systems improve threat detection and incident response capabilities, malicious actors are simultaneously leveraging the same technologies to increase the scale, speed, and sophistication of cyberattacks.

Environmental Security Challenges and Geopolitical Cyber Risks

A key finding of this study is that Pakistan's cybersecurity environment cannot be analyzed independently of its environmental vulnerabilities and geopolitical realities. Existing literature increasingly highlights the convergence of environmental security and cybersecurity, particularly in developing nations vulnerable to climate-related disruptions. Pakistan's recurring floods, energy shortages, and infrastructure challenges frequently necessitate emergency technological adaptations, including temporary communication networks, backup data systems, and rapid cloud migrations. While these measures enhance operational continuity, they often introduce unintended cybersecurity vulnerabilities. Emergency network reconfigurations, auxiliary power transitions, and temporary cloud deployments may result in configuration drift, inconsistent security policies, and unpatched systems. Such conditions create exploitable weaknesses that can be rapidly identified by automated AI-driven scanning tools. Consequently, environmental disruptions may indirectly increase organizational exposure to cyber threats by expanding the attack surface available to malicious actors.

The findings also reveal a growing relationship between cybersecurity risks and regional geopolitical tensions. Contemporary security studies categorize many of these threats within the broader framework of fifth-generation warfare (5GW), where cyberattacks, information operations, digital espionage, and critical infrastructure disruption are employed to achieve strategic objectives. Recent incidents involving attacks on communication

networks, public-sector systems, and critical digital infrastructure demonstrate how cyber operations increasingly target societal stability rather than merely technological assets. The convergence of AI-enabled cyber capabilities with geopolitical competition further amplifies these risks by enabling faster, more targeted, and more scalable offensive operations.

Cyber Exploitation and Operational Disruption

This framework highlights the interconnected nature of environmental security, critical infrastructure resilience, and cybersecurity preparedness within Pakistan's digital ecosystem.

Strategic Cybersecurity Framework for Pakistan's Digital Economy

Given the convergence of quantum threats, AI-enabled cyberattacks, environmental vulnerabilities, and geopolitical risks, the findings suggest that Pakistan requires a multi-layered and forward-looking cybersecurity strategy. Traditional perimeter-based security models are increasingly inadequate against modern attack techniques that exploit identities, supply chains, and trusted network relationships.

First, organizations should accelerate the adoption of Zero Trust Architecture (ZTA), which operates on the principle of continuous verification rather than implicit trust. Continuous authentication, identity management, and behavioral monitoring can significantly reduce the effectiveness of credential theft and insider threats, which remain among the most common attack vectors.

Second, financial institutions, telecommunications providers, and critical infrastructure operators should begin preparing for post-quantum migration by conducting cryptographic inventories, assessing hardware compatibility, and implementing crypto-agility frameworks. Hybrid security models that combine conventional cryptography with post-quantum algorithms can facilitate a gradual transition while minimizing operational disruption. Early adoption is particularly important for institutions managing long-term sensitive data that may remain vulnerable to future quantum decryption.

Third, organizations should strengthen cyber resilience through immutable and air-gapped backup strategies capable of mitigating ransomware and double-extortion attacks. Maintaining isolated, tamper-resistant backups enables rapid recovery of critical business operations without dependence on ransom payments. This approach is particularly relevant given the increasing prevalence of ransomware campaigns targeting financial institutions, healthcare providers, and government agencies.

Finally, cybersecurity policy development should incorporate environmental and geopolitical considerations alongside technological threats. Investments in resilient digital infrastructure, cybersecurity workforce development, post-quantum research initiatives, and public-private threat intelligence sharing will be essential for enhancing national cyber resilience. By integrating these measures, Pakistan can better position itself to address the emerging challenges posed by quantum computing, artificial intelligence, climate-related disruptions, and evolving geopolitical cyber threats.

V. CONCLUSIONS

The convergence of quantum computing and artificial intelligence represents one of the most significant cybersecurity challenges of the twenty-first century. While quantum computing promises transformative advancements in computational power and innovation, it simultaneously threatens the cryptographic foundations that secure modern digital infrastructures. At the same time, artificial intelligence is accelerating the sophistication, scale, and speed of cyberattacks, enabling threat actors to conduct highly automated and adaptive operations that increasingly outpace traditional security mechanisms. Together, these technologies are reshaping the global cyber threat landscape and exposing critical vulnerabilities within developing digital economies such as Pakistan.

The findings of this study indicate that Pakistan's expanding digital ecosystem—including financial services, e-governance platforms, telecommunications networks, and critical infrastructure—remains particularly vulnerable due to its continued reliance on legacy cryptographic systems, fragmented cybersecurity implementation, limited post-quantum preparedness, and growing dependence on interconnected digital services. These vulnerabilities are further amplified by environmental security challenges, critical infrastructure constraints,

and evolving geopolitical threats that increasingly manifest through cyber and information warfare domains.

The research also demonstrates that existing cybersecurity frameworks are insufficient to address the emerging realities of machine-speed attacks, AI-driven threat automation, and future quantum-enabled cryptographic disruption. Consequently, cybersecurity can no longer be treated solely as a technical or organizational issue; it must be recognized as a strategic national security and economic resilience imperative. Failure to prepare for the quantum-AI transition could undermine public trust in digital services, disrupt critical business operations, compromise sensitive national assets, and hinder Pakistan's broader digital transformation agenda.

To strengthen long-term cyber resilience, a coordinated and proactive national response is essential. Policymakers must accelerate the implementation of comprehensive data protection and cybersecurity regulations, while public and private sector organizations should prioritize the adoption of Zero Trust architectures, AI-enhanced threat detection capabilities, crypto-agile infrastructures, and post-quantum cryptographic migration strategies. Equally important are investments in cybersecurity education, workforce development, indigenous research capabilities, and public-private collaboration to address emerging technological risks.

Ultimately, Pakistan's ability to thrive in the next generation of the digital economy will depend on its readiness to anticipate and adapt to the quantum-AI paradigm shift. A comprehensive, sovereign, and future-oriented cybersecurity strategy—one that integrates technological innovation, regulatory governance, environmental resilience, and national security considerations—will be critical for protecting the country's critical infrastructure, preserving corporate and institutional trust, and ensuring sustainable economic growth in an increasingly complex cyber environment.

REFERENCES

[1] *Ahmed, N., Zhang, L., & Gangopadhyay, A. (2025).* A survey of post-quantum cryptography support in cryptographic libraries. arXiv. https://arxiv.org/

[2] Ali, A., Hussain, M., & Raza, S. (2024). Cybersecurity governance and policy implementation challenges in Pakistan. [Verify publication details before submission].

[3] Asian Development Bank. (2024). Asian development outlook 2024: Infrastructure resilience and digital transformation in Asia. Asian Development Bank. https://www.adb.org

[4] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute, University of Oxford.

[5] Buchanan, B., Lohn, A., Musser, M., & Sedova, K. (2022). Truth, lies, and automation: How language models could change disinformation. Center for Security and Emerging Technology (CSET), Georgetown University.

[6] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

[7] Cybersecurity and Infrastructure Security Agency. (2024). Cybersecurity performance goals for critical infrastructure. U.S. Department of Homeland Security. https://www.cisa.gov

[8] European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. ENISA. https://www.enisa.europa.eu

[9] Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.22331/q-2021-04-15-433

[10] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (pp. 212–219). Association for Computing Machinery. https://doi.org/10.1145/237814.237866

[11] Hoffman, F. G. (2021). The contemporary spectrum of conflict: Protracted, gray zone, ambiguous, and hybrid modes of war. The American University Press.

[12] IBM Security. (2025). IBM X-Force threat intelligence index 2025. IBM Corporation. https://www.ibm.com/security

[13] Iqbal, S., & Ahmed, R. (2024). Cybersecurity maturity challenges in developing-country financial institutions. [Verify publication details before submission].
[14] Khan, M., & Malik, A. (2023). Cybersecurity readiness and digital resilience in Pakistan. [Verify publication details before submission].
[15] Kshetri, N. (2023). Climate change and cybersecurity: Emerging risks and implications for developing economies. Telecommunications Policy, 47(6). https://doi.org/10.1016/j.telpol.2023.102596
[16] Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSEC.2018.2875369
[17] National Institute of Standards and Technology. (2024). Post-quantum cryptography standards. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography
[18] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE Computer Society. https://doi.org/10.1109/SFCS.1994.365700
[19] State Bank of Pakistan. (2024). Financial stability review 2024. State Bank of Pakistan. https://www.sbp.org.pk
[20] United Nations Development Programme. (2023). Pakistan floods recovery and resilience report. United Nations Development Programme. https://www.undp.org
[21] World Bank. (2023). Pakistan digital development and resilience assessment. World Bank Group. https://www.worldbank.org