International Journal of Social Science Archives

ISSN: 2707-8892

Available at *www.ijssa.com*

International Journal of Social Science Archives, October - December, 2025, 8(4), 28-36

Artificial Intelligence in Cybersecurity: Policy Readiness and Institutional Challenges in Pakistan

Nisar Azhar[1]*

[1]Nisar Azhar National University of Computer and Emerging Sciences (FAST-NUCES)

[*]**Email:** nisar_azhar_nisar@gmail.com

***Abstract*:** The rapid expansion of digital technologies in Pakistan has significantly increased exposure to cyber threats, particularly as government services, financial systems, and private sector operations become increasingly digitized. Artificial intelligence (AI) has emerged as a transformative tool for enhancing cybersecurity through real-time threat detection, predictive analytics, and automated response mechanisms. However, the effective deployment of AI-driven cybersecurity systems requires robust institutional frameworks, regulatory oversight, and technical capacity. This study examines Pakistan's policy readiness for integrating AI into cybersecurity, focusing on institutional challenges, governance gaps, and implementation barriers. Using a policy analysis approach supported by secondary data and institutional assessment, the study evaluates national cybersecurity strategies, technological capabilities, and capacity constraints. The findings highlight the need for coordinated governance, workforce development, regulatory strengthening, and strategic investment to build resilient cyber defense systems. The study provides policy recommendations for enhancing national cybersecurity readiness and offers insights relevant to other developing countries undergoing digital transformation.

Keywords: Artificial intelligence; Cybersecurity; Pakistan; Cyber resilience; Digital policy; Institutional Capacity; Cyber Governance.

Introduction

Digital transformation is reshaping economic and governance landscapes across the world, enabling new forms of connectivity, innovation, and service delivery. In Pakistan, the expansion of digital infrastructure, mobile connectivity, and online services has accelerated economic activity and improved access to information. Initiatives such as digital banking platforms, e-government portals, and online service systems have enhanced convenience and efficiency. However, these developments have also increased vulnerabilities to cyber threats, creating new challenges for national security and institutional resilience.

Cybersecurity has become a critical policy concern as cyber-attacks grow in sophistication and frequency. Financial fraud, data breaches, ransomware attacks, and cyber espionage pose risks to both public and private sector institutions. As digital ecosystems expand, traditional security mechanisms based on manual monitoring and static defenses are increasingly inadequate. Artificial intelligence offers new possibilities for enhancing cybersecurity through automated threat detection, anomaly analysis, and predictive risk management.

AI-driven cybersecurity systems can analyze vast amounts of network data to identify patterns indicative of

malicious activity. Machine learning algorithms enable proactive defense strategies by detecting threats before they escalate. These capabilities are particularly valuable in environments characterized by rapidly evolving threat landscapes. Yet adopting AI for cybersecurity also introduces challenges, including technical complexity, governance concerns, and resource requirements.

In developing countries such as Pakistan, the adoption of advanced cybersecurity technologies is influenced by institutional capacity, regulatory environments, and human capital availability. While national policies recognize the importance of cybersecurity, implementation remains uneven due to coordination challenges and resource constraints. The integration of AI into cybersecurity frameworks requires not only technological investment but also institutional reforms that support effective governance.

This study explores the role of AI in strengthening cybersecurity in Pakistan by examining policy frameworks, institutional readiness, and governance challenges. It seeks to understand how emerging technologies can enhance national cyber resilience while identifying barriers that may hinder adoption. By focusing on policy readiness, the research contributes to debates on digital security in developing economies and offers recommendations for strengthening cybersecurity strategies.

Cybersecurity Landscape in Pakistan

Pakistan's digital ecosystem has expanded rapidly, driven by growth in telecommunications, digital payments, and online services. Mobile penetration has increased significantly, enabling widespread adoption of digital platforms. Government initiatives promoting digital services have improved access to public administration, while financial institutions have expanded online banking capabilities.

However, the growth of digital systems has been accompanied by rising cyber risks. Financial institutions have faced phishing attacks and fraud attempts, while public sector systems have encountered vulnerabilities related to data security. The increasing reliance on digital platforms underscores the need for robust cybersecurity measures capable of addressing evolving threats.

National policy frameworks such as cybersecurity strategies and digital transformation plans recognize these challenges and emphasize the importance of strengthening cyber defenses. Yet implementation gaps persist, reflecting institutional constraints and limited technical capacity.

Literature Review

Evolution of Cyber Threats

Cyber threats have evolved from isolated incidents to complex, coordinated attacks involving advanced techniques. The rise of ransomware, distributed denial-of-service attacks, and sophisticated malware has increased the potential impact of cyber incidents on economic stability and national security.

AI Applications in Cybersecurity

AI technologies are increasingly used to enhance cybersecurity through automated monitoring, intrusion detection, and threat intelligence. Research shows that machine learning improves detection accuracy by identifying anomalies that traditional systems may overlook. AI systems enable continuous monitoring of networks, allowing organizations to respond more effectively to emerging threats.

Institutional and Governance Dimensions

Cybersecurity is not solely a technical issue but involves governance structures, regulatory frameworks, and coordination among stakeholders. Effective cyber defense requires collaboration between government agencies, private sector organizations, and international partners.

Challenges in Developing Countries

Developing countries face unique challenges in adopting advanced cybersecurity technologies, including limited technical expertise, resource constraints, and regulatory gaps. These factors can hinder the implementation of comprehensive cybersecurity strategies.

Conceptual Framework

This study conceptualizes AI-enabled cybersecurity readiness as dependent on five interrelated dimensions:

1. Policy and regulatory frameworks
2. Institutional coordination
3. Technical infrastructure
4. Human capital and expertise
5. Risk management capabilities

These dimensions collectively influence the effectiveness of cybersecurity strategies and the integration of AI technologies.

Research Questions

1. What is the current state of cybersecurity policy readiness in Pakistan?
2. How can AI enhance national cyber resilience?
3. What institutional challenges affect the adoption of AI-driven cybersecurity?
4. What policy reforms are needed to strengthen cybersecurity governance?

Methodology

The study adopts a qualitative policy analysis approach supported by secondary data review. Policy documents, cybersecurity strategies, institutional reports, and digital indicators are analyzed to assess readiness and identify governance gaps. The analysis emphasizes institutional dynamics and policy frameworks rather than technical performance metrics.

Empirical Assessment of Cybersecurity Readiness in Pakistan

Overview of National Cyber Risk Environment

Pakistan's expanding digital ecosystem has created both opportunities and vulnerabilities. The rapid growth of digital banking, e-commerce, mobile payments, and e-government services has increased reliance on digital infrastructure, making cybersecurity a national priority. However, threat intelligence reports and institutional assessments indicate that cyber risks continue to evolve, driven by increased connectivity and the sophistication of malicious actors.

Cyber incidents affecting financial institutions, public databases, and private organizations highlight the need for advanced security mechanisms capable of responding to dynamic threats. Traditional security models based on reactive monitoring are increasingly insufficient, reinforcing the importance of AI-driven approaches that enable predictive and adaptive defense.

Threat Landscape Analysis

Table 1 Major Cyber Threat Categories Affecting Pakistan

Threat Type	Description	Impact Level
Phishing attacks	Fraudulent attempts targeting users	High
Ransomware	Data encryption for financial gain	High
Data breaches	Unauthorized access to sensitive data	High
Malware	Malicious software targeting systems	Medium-High
Insider threats	Misuse of internal access	Medium
Distributed denial-of-service	Service disruption attacks	Medium

The prevalence of phishing and ransomware attacks reflects vulnerabilities in both technical systems and user awareness. Financial institutions and government agencies remain key targets due to the sensitivity of their data.

Institutional Capacity Assessment

Table 2 — Institutional Readiness Dimensions

Dimension	Current Status	Assessment
Policy framework	Developing	Moderate
Regulatory enforcement	Limited capacity	Weak-Moderate
Inter-agency coordination	Fragmented	Weak
Technical capability	Improving	Moderate
Workforce expertise	Skills gap	Weak-Moderate

The analysis indicates that while policy frameworks acknowledge cybersecurity risks, implementation capacity varies significantly across institutions. Coordination challenges limit the effectiveness of national cybersecurity strategies.

AI Adoption Potential

Artificial intelligence offers opportunities to enhance cybersecurity through automated threat detection, anomaly analysis, and real-time response. In Pakistan, financial institutions have begun adopting AI-based fraud detection systems, demonstrating the potential for wider application.

However, broader adoption remains constrained by factors such as limited technical expertise, resource limitations, and concerns regarding governance. Expanding AI deployment requires investments in infrastructure, workforce training, and regulatory oversight.

Governance Challenges in AI-Driven Cybersecurity

Skills and Workforce Constraints

One of the most significant barriers to adopting AI in cybersecurity is the shortage of skilled professionals. Developing and maintaining AI systems requires expertise in data science, machine learning, and cybersecurity operations. Addressing this gap is essential for building sustainable cyber defense capabilities.

Regulatory and Legal Gaps

While cybersecurity policies exist, comprehensive frameworks addressing AI governance remain limited. Issues related to accountability, data protection, and algorithmic transparency require greater regulatory attention.

Resource Limitations

Implementing advanced cybersecurity technologies involves significant financial investment. Budget constraints may limit the ability of institutions to deploy AI solutions at scale.

Coordination Issues

Effective cybersecurity requires collaboration among government agencies, private sector actors, and international partners. Fragmented coordination can reduce responsiveness to emerging threats.

Policy Roadmap for AI-Enabled Cybersecurity

Strengthening National Cybersecurity Strategy

Updating national cybersecurity strategies to explicitly incorporate AI technologies can provide a roadmap for coordinated action. Strategic frameworks should define roles, responsibilities, and implementation timelines.

Building Technical Capacity

Investments in training programs, research initiatives, and partnerships with academic institutions can enhance workforce capabilities. Developing specialized training programs can support long-term capacity building.

Enhancing Regulatory Oversight

Developing regulations that address AI governance, data protection, and accountability can strengthen institutional frameworks and build public confidence.

Promoting Public-Private Collaboration

Collaboration with private sector organizations can facilitate knowledge sharing and technological innovation. Public-private partnerships can support resource mobilization and enhance resilience.

Improving Awareness and Preparedness

Public awareness campaigns and cybersecurity education initiatives can reduce vulnerabilities associated with human factors.

Discussion

The findings highlight the importance of adopting a holistic approach to cybersecurity that integrates technological innovation with institutional strengthening. AI technologies offer significant potential for improving threat detection and response capabilities, yet their effectiveness depends on governance structures and capacity development.

The study underscores that cybersecurity should be viewed as a national resilience issue rather than solely a technical concern. Strengthening institutional frameworks and promoting collaboration can enhance preparedness for emerging threats.

Policy Implications

Policymakers should prioritize investments in cybersecurity infrastructure and workforce development. Strengthening regulatory frameworks can support responsible adoption of AI technologies while ensuring accountability.

Developing integrated governance strategies can enhance coordination and improve response capabilities. These measures can contribute to building a resilient digital ecosystem capable of supporting economic growth and innovation.

Limitations

This study relies on policy analysis and secondary data, which may not capture operational dynamics within institutions. Future research could incorporate empirical studies examining organizational practices and technical performance.

Conclusion

Artificial intelligence has the potential to transform cybersecurity by enabling proactive defense and enhancing resilience against evolving threats. In Pakistan, leveraging AI for cybersecurity requires coordinated policy action, institutional strengthening, and capacity building.

The analysis demonstrates that while progress has been made in developing policy frameworks, significant challenges remain in implementation and governance. Addressing these challenges can enable Pakistan to build robust cyber defense systems and support secure digital transformation.

Pakistan Case Examples: Cyber Incidents and Institutional Responses

Banking Sector Cyber Fraud and Phishing Campaigns

Pakistan's banking sector has experienced a steady rise in cyber fraud incidents, particularly phishing attacks targeting customers of commercial banks. Fraudulent emails and SMS messages impersonating banks have been used to obtain login credentials and one-time passwords, leading to unauthorized transactions. Several financial institutions have reported cases where customers' accounts were compromised through social engineering techniques rather than direct system breaches.

These incidents highlight the importance of AI-driven fraud detection systems capable of identifying unusual transaction patterns and flagging suspicious activity in real time. Banks in Pakistan have begun deploying machine

learning models for fraud detection, yet adoption remains uneven across institutions. The cases illustrate how human vulnerabilities combined with technological gaps can create systemic risks.

Data Breach Concerns in Public Sector Databases

Public sector databases in Pakistan, including citizen information systems, have faced scrutiny due to concerns about data security and unauthorized access. Reports of leaked personal information circulating on online forums have raised questions regarding the adequacy of cybersecurity measures and governance controls. While authorities have taken steps to investigate such incidents, they underscore the need for stronger security protocols and continuous monitoring.

AI-based intrusion detection systems could enhance the ability of government agencies to detect anomalous access patterns and respond to potential breaches more effectively. Strengthening cybersecurity governance is essential for maintaining public trust in digital services.

Ransomware Threats to Organizations

Private sector organizations, particularly small and medium enterprises, have increasingly faced ransomware threats. In several instances, organizations have reported disruptions caused by malicious software encrypting data and demanding payment for restoration. Many affected entities lack dedicated cybersecurity teams, making them vulnerable to such attacks.

The growing frequency of ransomware incidents highlights the importance of proactive threat intelligence and automated response mechanisms. AI technologies can help detect early signs of intrusion and mitigate risks before they escalate into major disruptions.

Cybersecurity Challenges in E-Government Platforms

Pakistan's expansion of e-government services has improved accessibility but also introduced new security challenges. Online portals handling taxation, licensing, and service delivery must manage large volumes of sensitive data. Ensuring the security of these platforms is critical for preventing unauthorized access and maintaining system integrity.

Periodic vulnerabilities identified in public sector digital systems demonstrate the need for continuous security assessments and monitoring. AI-driven vulnerability scanning and anomaly detection can strengthen defenses and support secure service delivery.

Social Media and Disinformation Risks

Cybersecurity in Pakistan also extends beyond technical infrastructure to include information security challenges such as misinformation campaigns and coordinated online manipulation. Social media platforms have been used to spread false information, highlighting the need for monitoring mechanisms that can identify malicious activities.

AI tools capable of detecting abnormal communication patterns can assist in identifying coordinated disinformation efforts, contributing to broader digital resilience.

Lessons From Case Examples

These cases reveal several recurring themes:

- Human factors remain a major source of vulnerability.
- Institutional coordination is critical for responding to incidents.
- Continuous monitoring is necessary to detect emerging threats.
- Public awareness plays an important role in reducing risks.

The cases reinforce the argument that cybersecurity requires an integrated approach combining technological innovation with governance reforms.

Case Synthesis: Lessons for AI-Enabled Cybersecurity Governance in Pakistan

Cross-Case Patterns and Structural Vulnerabilities

The case examples collectively reveal that cybersecurity risks in Pakistan are not isolated incidents but manifestations of broader structural vulnerabilities within the digital ecosystem. Across sectors, a recurring pattern emerges in which technological expansion has outpaced institutional safeguards, creating gaps that malicious actors

can exploit. Financial fraud incidents demonstrate the persistence of social engineering risks, while concerns related to public sector databases highlight weaknesses in access controls and monitoring systems. Ransomware attacks on private organizations further illustrate how limited preparedness and insufficient security investments increase exposure to cyber threats.

These patterns suggest that cybersecurity challenges are deeply interconnected with institutional capacity and governance structures. The absence of standardized security protocols across sectors contributes to uneven resilience, reinforcing the need for coordinated policy responses.

Human Factors and Behavioral Risks

One of the most striking insights from the case analysis is the central role of human factors in shaping cybersecurity outcomes. Phishing campaigns and social engineering attacks exploit gaps in user awareness and training, indicating that technological defenses alone cannot fully mitigate risks. This underscores the importance of integrating cybersecurity awareness programs with technological solutions.

Artificial intelligence can play a role in addressing behavioral vulnerabilities by identifying suspicious communication patterns and detecting anomalies in user activity. However, technological solutions must be complemented by continuous education and institutional policies that promote secure practices.

Institutional Coordination Challenges

The cases highlight coordination challenges among regulatory bodies, financial institutions, and government agencies. Effective response to cyber incidents often requires information sharing and collaborative action, yet institutional silos can delay responses and limit effectiveness. Strengthening coordination mechanisms and establishing clear communication channels are essential for improving resilience.

From a governance perspective, these challenges illustrate the importance of adopting a whole-of-government approach to cybersecurity, where agencies operate within a unified framework that facilitates rapid response and knowledge exchange.

Implications for AI Adoption

The case evidence demonstrates that AI technologies could significantly enhance cybersecurity capabilities by enabling real-time monitoring and predictive threat analysis. For instance, AI-based fraud detection systems can identify unusual financial transactions, while machine learning models can detect network anomalies indicative of cyber-attacks. However, effective deployment requires addressing governance gaps and ensuring that institutions possess the necessary technical expertise.

The analysis suggests that AI adoption should be viewed as part of a broader institutional reform process rather than a standalone technological solution. Without appropriate governance frameworks, AI systems may not achieve their full potential.

Policy Lessons Emerging from Case Evidence

Several policy lessons emerge from the synthesis:

1. Strengthening regulatory oversight is essential for ensuring consistent security standards across sectors.
2. Enhancing institutional coordination can improve incident response and reduce systemic risks.
3. Investing in workforce development can address skills gaps and support AI adoption.
4. Promoting public awareness can reduce vulnerabilities associated with human behavior.
5. Integrating AI into cybersecurity strategies can enhance detection and response capabilities.

These lessons reinforce the need for a comprehensive approach that combines technological innovation with institutional strengthening.

Linking Case Evidence to National Cyber Resilience

The synthesis underscores that national cyber resilience depends on the interaction between technological capabilities and governance structures. Addressing vulnerabilities requires coordinated efforts that align policy frameworks, institutional practices, and technological investments. The case analysis provides empirical support for

the argument that strengthening governance capacity is critical for leveraging AI effectively in cybersecurity.

Table Cybersecurity Incident Synthesis: Causes, Governance Gaps, and AI Policy Responses

Incident Category	Immediate Causes	Underlying Governance Gaps	Potential AI Solutions	Policy Implications
Banking phishing and fraud	Social engineering, weak authentication awareness	Limitedpublic awareness programs, uneven fraud monitoring across banks	AI fraud detection systems, behavioral analytics, real-time anomaly detection	Strengthen banking cybersecurity regulations, expand awareness campaigns
Public sector data exposure concerns	Weak access controls, insufficient monitoring	Incomplete data governance frameworks, lack of continuous auditing	AI intrusion detection, automated access monitoring, anomaly detection tools	Enact stronger data protection standards and monitoring protocols
Ransomware incidents in organizations	Outdated systems, poor patch management	Lack of cybersecurity preparedness among SMEs, limited incident response planning	Predictive threat intelligence, automated malware detection, endpoint monitoring	Develop national cyber readiness programs for businesses
E-government platform vulnerabilities	Rapid digitization without security integration	Fragmented oversight, inconsistent security testing	AI vulnerability scanning, continuous monitoring systems	Mandate cybersecurity audits for government platforms
Disinformation and online manipulation	Coordinated fake accounts, automated messaging	Limited monitoring capacity, weak information governance	AI content pattern detection, network analysis tools	Develop digital information security strategies
Insider misuse risks	Weak internal controls, insufficient oversight	Lack of monitoring protocols and accountability mechanisms	User behavior analytics, AI-driven access monitoring	Strengthen internal security policies and audit systems

References

Asian Development Bank, “Governance Risk Assessment,” 2021.
Asian Development Bank, “Public Sector Reform in South Asia,” 2020.
Asian Development Bank, *Digital Economy Report*, Manila, Philippines, 2022.
Brookings Institution, “Digital Government and Reform,” 2021.
D. North, *Institutions, Institutional Change and Economic Performance*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
F. Fukuyama, “What is governance?” *Governance*, vol. 26, no. 3, pp. 347–368, 2013.
Government of Pakistan, “Public Sector Digital Transformation Reports,” various years.
Harvard Kennedy School, “Digital Government and Public Sector Innovation,” 2020.
IMF, “Digitalization and Governance,” 2023.
IMF, “Digitalization and Public Sector Transformation,” Washington, DC, USA, 2022.
ITU, “Global Cybersecurity Index,” 2023.
ITU, “ICT Development Index,” 2023.
ITU, *Measuring Digital Development: Facts and Figures 2023*. Geneva, Switzerland, 2023.
J. Fountain, *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC, USA: Brookings Institution Press, 2001.
M. Castells, *The Rise of the Network Society*. Oxford, U.K.: Blackwell, 2010.
OECD, “Digital Strategy,” 2022.

OECD, “Public Sector Innovation,” 2021.
OECD, “Regulatory Policy Outlook,” 2021.
OECD, “Trust in Government,” 2022.
OECD, *Digital Government Review*. Paris, France: OECD Publishing, 2020.
OECD, *Government at a Glance 2021*. Paris, France: OECD Publishing, 2021.
P. Dunleavy, H. Margetts, S. Bastow, and J. Tinkler, “Digital era governance,” *J. Public Admin. Res. Theory*, vol. 16, no. 3, pp. 467–494, 2006.
P. Evans, *Embedded Autonomy: States and Industrial Transformation*. Princeton, NJ, USA: Princeton Univ. Press, 1995.
Pakistan Bureau of Statistics, “ICT Indicators,” Islamabad, Pakistan, 2023.
Pakistan IT Board, *E-Governance Initiatives Report*, Lahore, Pakistan, 2023.
Pakistan Ministry of Information Technology and Telecommunication, *Digital Pakistan Policy*, Islamabad, Pakistan, 2020.
Pakistan Ministry of IT, “National Cyber Security Policy,” 2021.
Pakistan National Cyber Security Policy, 2021.
Pakistan Planning Commission, *Vision 2025*, Islamabad, Pakistan, 2019.
Pakistan Telecommunication Authority, *Annual Report 2023*, Islamabad, Pakistan, 2023.
R. Heeks, “E-government for development,” *Information Technology for Development*, vol. 14, no. 1, pp. 1–20, 2008.
S. Bannister and R. Connolly, “Defining e-government,” *Government Information Quarterly*, vol. 29, no. 1, pp. S3–S9, 2012.
State Bank of Pakistan, “Digital Financial Services Landscape,” Karachi, Pakistan, 2022.
UNDP Pakistan, “Digital Governance and Public Sector Innovation,” Islamabad, Pakistan, 2022.
UNDP Pakistan, “Public Sector Digital Transformation,” 2023.
UNDP, “Governance Reform and Institutional Strengthening,” 2020.
UNDP, “Institutional Capacity Development Framework,” 2021.
UNESCAP, “Digital Government for Sustainable Development,” 2022.
United Nations, “Public Administration Report,” 2021.
United Nations, *UN E-Government Survey 2022: The Future of Digital Government*. New York, NY, USA, 2022.
World Bank, “Digital Government Readiness Assessment,” 2022.
World Bank, “GovTech and Public Sector Innovation,” 2022.
World Bank, “GovTech Maturity Index,” Washington, DC, USA, 2022.
World Bank, “Inclusive Digital Economy,” 2023.
World Bank, “Pakistan Development Update,” 2023.
World Bank, “Public Sector Reform and Governance,” 2022.
World Bank, “Worldwide Governance Indicators,” 2023.
World Bank, *World Development Report 2016: Digital Dividends*. Washington, DC, USA: World Bank, 2016.
World Economic Forum, “Digital Transformation of Government,” Geneva, Switzerland, 2021.
World Economic Forum, “Digital Trust Framework,” 2022.