Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 12, 2025

DIGITAL CRIME AND CYBER LAW MAKING IN PAKISTAN: UNDERSTANDING MOTIVATIONS, VULNERABILITIES, AND LEGAL REFORM NEEDS

Engr. Dr. Syed Ayaz Haider[*1], **Afzal Hussain**[2]

[*1]*Chairman & Founder Principal, Ghazi Foundation Schools & Colleges, Karachi, Pakistan.*
[2]*Assistant Prosecutor General, Sindh, Karachi, Pakistan.*

[*1]sahaider110@gmail.com, [2]afzaltalpur@gmail.com

DOI: https://doi.org/10.5281/zenodo.17972365

Keywords
Cybercrime, Cybersecurity, PECA 2016, Pakistan, Cyber Law, Digital Vulnerability, Legal Reform, AI-driven Threats

Article History
Received: 18 October 2025
Accepted: 30 November 2025
Published: 18 December 2025

Copyright @Author
Corresponding Author: *
Engr. Dr. Syed Ayaz Haider

Abstract

The rapid expansion of Pakistan's digital ecosystem has generated remarkable opportunities for communication, commerce, public service delivery, and socio-economic growth. However, this advancement has also exposed the nation to an unprecedented surge in cybercrimes ranging from identity theft and phishing scams to financial fraud, social media exploitation, ransomware attacks, and AI-driven manipulation. This study aims to examine the technological, socio-economic, and legislative drivers of cybercrime in Pakistan. A convergent mixed-methods design was employed, integrating quantitative data from 312 survey respondents—including IT professionals, law-enforcement officers, and legal scholars—with qualitative insights from semi-structured interviews. Data were analyzed using descriptive statistics and thematic analysis to identify patterns and points of convergence. The findings reveal that cybercrime in Pakistan is shaped by digital illiteracy, socio-economic distress, weak cybersecurity infrastructure, and outdated or insufficient legislation. National data from NCCIA (2025) indicate over 142,272 cyber complaints recorded within a single year, while cybersecurity firms such as Kaspersky report over 5.3 million attempted attacks. Participants emphasized urgent reforms to address cryptocurrency fraud, ransomware, deep fakes, AI-driven manipulation, and transnational cyber threats. Pakistan urgently requires a comprehensive and modernized cyber governance framework that integrates updated legislation, institutional capacity-building, digital literacy enhancement, and multi-stakeholder collaboration. Without systemic reforms, Pakistan's growing digital ecosystem will remain vulnerable, threatening economic stability, public trust, and national security.

INTRODUCTION

The 21st century has ushered in an era defined by extraordinary digital transformation. Technological innovations—ranging from global connectivity and mobile broadband to fintech systems, e-commerce platforms, and artificial intelligence—have revolutionized how societies function, transact, communicate, and govern. Today, digital technologies shape the everyday routines of billions, influencing education, healthcare, finance, public administration, and even political engagement. In Pakistan, this transformation has been especially striking, with over 100 million internet users and rapid growth

in digital banking, online businesses, and social media engagement.

Yet, alongside these advancements lie profound risks. Digital networks, despite their benefits, create pathways for exploitation, misinformation, financial theft, and privacy invasion. Scholars have argued that technological innovation without parallel development of regulatory and protective mechanisms produces an environment ripe for cyber malfeasance. Trust, Carpenter, and Krutka (2020) notably emphasize that online environments enhance empowerment but simultaneously expose users to vulnerabilities when oversight and digital literacy are insufficient.

This dual reality is sharply evident in Pakistan. Although the nation has made significant strides toward digitalization, the rapid expansion of online services has collided with systemic gaps: limited cybersecurity infrastructure, inadequate digital literacy, socio-economic pressures, and a legal framework that struggles to keep pace with technological change. The Prevention of Electronic Crimes Act (PECA, 2016) was introduced to address cyber offenses such as unauthorized access, cyberstalking, identity theft, and electronic forgery. However, PECA's scope has not evolved in proportion to emerging threats. Issues such as cryptocurrency scams, AI-generated deepfakes, synthetic identities, ransomware, and cross-border cyber intrusions often fall beyond the Act's current definitions and operational mechanisms (Rajput, 2024; Saleem et al., 2024).

Moreover, public institutions tasked with cyber enforcement—particularly the Federal Investigation Agency's (FIA) cybercrime wing—struggle with limited resources, outdated tools, jurisdictional constraints, and growing case backlogs. As digital dependence increases across urban centers like Karachi, Lahore, and Islamabad, so does the sophistication of cybercriminals, including both independent offenders and transnational networks operating across borders. Official statistics portray the severity of the situation. The National Cyber Crime Investigation Agency (NCCIA, 2025) recorded over **142,272 cybercrime complaints** in a single year, while global cybersecurity firms like Kaspersky (2025) documented **5.3 million attempted cyberattacks** targeting Pakistan's financial institutions, government portals, educational systems, and private enterprises. These incidents not only cause financial loss but also undermine national security, disrupt public trust, and destabilize vital digital infrastructure.

Given this background, the present study seeks to understand the deep-rooted factors that contribute to the rise of cybercrime in Pakistan. It explores how technological vulnerabilities—such as weak encryption, outdated systems, and inadequate network security—intersect with socio-economic pressures, digital illiteracy, and legislative shortcomings. By examining these interconnected dimensions through a mixed-methods research approach, the study aims to offer a holistic perspective on Pakistan's cybercrime landscape. Ultimately, securing Pakistan's digital future requires more than reactive policing. It demands a proactive, integrated approach involving updated cyber laws, public awareness initiatives, institutional strengthening, international cooperation, and investment in modern cybersecurity tools. This study, therefore, provides timely insights into the evolving dynamics of cybercrime in Pakistan and offers policy-relevant recommendations that can guide national cyber governance reform.

LITERATURE REVIEW

The phenomenon of cybercrime is a multidimensional challenge, encompassing technological vulnerabilities, socio-economic dynamics, regulatory insufficiencies, and behavioral patterns. Global scholarship emphasizes that as societies rapidly adopt digital technologies, the pace of cyber threats often exceeds the capacity of existing legal and institutional frameworks. Trust, Carpenter, and Krutka (2020) argue that online platforms empower users and foster innovation but simultaneously expose individuals to significant risks when governance mechanisms are weak or fragmented. Prestridge (2019) underscores the importance of cybersecurity literacy, noting that both professional and academic users require

continuous skill development to navigate the increasingly complex digital environment safely.

Cybercrime Trends in Pakistan

Pakistan's experience reflects a microcosm of these global dynamics, with cybercrime manifesting in diverse forms, including identity theft, financial fraud, phishing, ransomware, social media exploitation, and AI-generated content abuse. Reports by the National Cyber Crime Investigation Agency (NCCIA, 2025) reveal over 142,000 complaints in a single year, while Kaspersky (2025) documents over 5.3 million attempted cyberattacks targeting critical sectors. The concentration of offenses in urban hubs—Karachi, Lahore, and Islamabad—suggests that high internet penetration, dense digital infrastructure, and commercial activity create lucrative targets for cybercriminals.

Anjum (2020) highlights socio-economic drivers, showing that poverty, unemployment, and inequity often push individuals toward cyber offending, particularly in contexts where legal deterrents are weak or enforcement is inconsistent. Yusuf, Daneva, and van Sinderen (2025) further demonstrate that digital illiteracy significantly increases vulnerability to phishing and social engineering attacks, emphasizing the intersection between behavioral factors and technological exposure. These findings indicate that cybercrime in Pakistan is not merely a technical issue but a complex socio-technical phenomenon shaped by systemic vulnerabilities.

Legislative Framework and Limitations

The Prevention of Electronic Crimes Act (PECA, 2016) represents Pakistan's primary legislative instrument against cybercrime. The Act criminalizes offenses such as unauthorized access, electronic fraud, cyber stalking, and online harassment. While PECA laid a foundational legal structure, scholars critique its inability to address emerging threats adequately. Rajput (2024) and Saleem, Jan, and Areej (2024) note that PECA lacks explicit provisions for cryptocurrency-related crimes, AI-driven attacks, ransomware targeting hospitals and SMEs, and the misuse of deepfake technology for harassment or defamation.

Recent amendments in 2025 established the National Cybercrime Investigation Authority and introduced penalties for fake news dissemination (HRCP, 2025). However, these measures drew criticism for potentially infringing upon freedom of expression without providing robust technical solutions for emerging cyber threats. Shah (2022) emphasizes that gaps in PECA enforcement are compounded by insufficient institutional capacity, including inadequate staffing, training, and coordination between federal and provincial agencies.

Socio-Economic and Behavioral Determinants

Research indicates that socio-economic and behavioral factors are significant predictors of cybercrime involvement and victimization. Anjum (2020) and Ibrahim (2019) report that financial stress, unemployment, and social marginalization often motivate offenders. Likewise, low levels of digital literacy and cybersecurity awareness among the general public amplify the impact of social engineering and phishing attacks. Cultural factors, such as high trust in social networks and informal communication channels, create vulnerabilities that cybercriminals exploit.

Women and vulnerable populations face amplified risks. Khilji (2025) documents how AI-generated harassment, deepfake pornography, and online defamation disproportionately affect women, exploiting legal loopholes and gaps in PECA's protective measures. This gendered dimension underscores the need for targeted legal, technical, and educational interventions.

Technological Vulnerabilities

Pakistan's technological infrastructure contributes to cybercrime susceptibility. NCCIA (2025) and Kaspersky (2025) identify several systemic weaknesses:

- Outdated IT systems in government and private sectors
- Weak encryption standards and unpatched software

- Limited cybersecurity monitoring and intrusion detection
- Lack of national-level early-warning mechanisms

These vulnerabilities are exploited by both domestic opportunists and international actors. Ahmed (2022) highlights that state-sponsored cyber incursions from adversarial countries further exacerbate the risk to critical national infrastructure, including energy grids, defense networks, and financial institutions.

Emerging Threats and Global Context

Emerging technologies have introduced new vectors of cybercrime. Ransomware-as-a-service, AI-generated deepfakes, and blockchain-enabled financial scams pose challenges not only to enforcement but also to regulatory adaptation. Wani, Jabin, Yazdani, and Ahmad (2018) argue that proactive governance, coupled with advanced monitoring and forensic tools, is essential to preemptively address these threats.

Globally, best practices emphasize multi-stakeholder collaboration. Lessons from countries with resilient cybercrime frameworks indicate that integrated legal updates, public awareness campaigns, digital literacy programs, and strong institutional capacities collectively mitigate the impact of cybercrime. In Pakistan, efforts such as Raast for secure digital payments and Cyber Aagahi for digital literacy represent steps toward inclusion but require scaling, policy alignment, and legislative reinforcement (Hussain, 2025).

Synthesis and Research Gap

The reviewed literature suggests that while Pakistan has foundational legal and institutional structures, they remain insufficient for managing modern cyber threats. Most studies focus on either technological or socio-behavioral dimensions, rarely integrating both with legislative analysis. Moreover, there is limited empirical research combining perceptions of IT professionals, law enforcement, and legal scholars, leaving a gap in comprehensive understanding of cybercrime motivations, vulnerabilities, and reform needs.

This study addresses this gap by employing a convergent mixed-methods design to investigate how technological, socio-economic, and legislative factors intersect to shape the cybercrime landscape in Pakistan. The integration of quantitative and qualitative insights aims to produce actionable recommendations for legal reform, institutional strengthening, and public awareness initiatives.

MATERIALS AND METHODS

Research Design

A **convergent mixed-methods design** was employed to examine cybercrime determinants in Pakistan. This design allows simultaneous collection of quantitative and qualitative data, enabling comprehensive triangulation of technical, behavioral, and legislative dimensions. Quantitative measures captured perceptions of technological vulnerabilities, socio-economic pressures, and legal awareness, while qualitative interviews explored motivations for cybercrime, institutional weaknesses, and reform priorities. Integration of these strands was performed during interpretation to ensure a holistic understanding of the phenomena.

Participants

A total of **312 participants** were selected using **stratified sampling** to ensure representation across professional sectors and urban centers. The sample included:

- **120 IT professionals** (software engineers, network administrators, cybersecurity analysts)
- **92 law-enforcement officials** (FIA cybercrime wing officers, prosecutors)
- **100 legal scholars** (academics, practitioners, cyber-law experts)

Geographic representation included Karachi, Lahore, and Islamabad.

Instruments

Two complementary instruments were used:

Quantitative Survey Instrument

- 24-item Likert-scale questionnaire
- Covered technological vulnerabilities, socio-economic factors, legislative awareness, and cybercrime exposure

- Cronbach's α = 0.87 (high reliability)

Qualitative Semi-Structured Interviews

- 12 open-ended prompts
- Explored motivations for cybercrime, system vulnerabilities, limitations of PECA (2016), and proposed reforms

Procedure

Ethical approval was obtained prior to data collection. Surveys were disseminated digitally, and interviews conducted via Zoom, with verbal and written consent. Verbatim transcriptions were produced for qualitative analysis.

.

Data Analysis

- **Quantitative Analysis:** Descriptive statistics (means, standard deviations, frequencies) using SPSS v26.
- **Qualitative Analysis:** Thematic analysis following Braun and Clarke's six-phase model. Themes were iteratively refined.
- **Integration:** Narrative weaving approach highlighted convergences and divergences between quantitative and qualitative finding

FINDINGS AND RESULTS

Descriptive Analysis

Table 1: Key cyber vulnerability factors in Pakistan (2025)

Factor	Mean	SD	Observation
Technological gaps	3.7	0.9	Weak infrastructure and outdated systems
Socio-economic pressures	3.5	1.0	Poverty and unemployment drive risk behavior
Legislative awareness	3.8	0.9	Limited knowledge among citizens
Cybercrime incidents reported	4.0	1.1	High incidence in urban areas

Table 2: Cybercrime Incidents by Sector in Pakistan (2025)

Sector	Reported Cases	Percentage of Total	Observations
Banking & Financial	48,000	33%	High targeting due to online banking systems
Government & Public Services	25,000	17%	Phishing and data breaches common
Education & Academia	18,000	12%	Student accounts and online portals targeted
Healthcare & Pharma	14,000	10%	Patient data theft and ransomware attacks
E-commerce & Retail	20,000	14%	Payment fraud and account hacking prevalent
Social Media & Entertainment	17,000	12%	Fake profiles, scams, and harassment
Other Sectors	7,272	5%	Miscellaneous online crimes

Table 2: Sector-wise distribution of cybercrime in Pakistan (NCCIA, 2025; Kaspersky, 2025)

Table 3: Cybercrime Incidents by Region in Pakistan (2025)

Region	Reported Cases	Percentage of Total	Key Observations
Karachi	42,500	30%	Highest urban density and online penetration

Region	Reported Cases	Percentage of Total	Key Observations
Lahore	35,000	25%	Major commercial hub, frequent financial fraud
Islamabad	22,500	16%	Government offices targeted
Rawalpindi	12,000	8%	Banking and education sector affected
Peshawar	8,000	6%	Limited reporting infrastructure
Quetta	5,000	4%	Low internet penetration, underreported cases
Other Regions	17,272	11%	Aggregated rural and small city incidents

Table 3: Region-wise distribution of cybercrime incidents in Pakistan (NCCIA, 2025).

Table 4: Comparative Analysis of Cybercrime Type Across Sectors

Cybercrime Type	Banking & Finance	Government	Education	Healthcare	E-commerce	Social Media	Other
Phishing & Identity Theft	22,000	8,000	4,000	2,000	3,000	3,000	500
Financial Fraud	18,000	3,000	2,500	1,500	5,000	2,000	500
Ransomware Attacks	5,000	8,000	2,000	7,000	1,500	3,000	500
Social Media Exploitation	1,000	6,000	9,500	3,500	3,500	9,000	500
Other Cyber Offenses	2,000	0	0	0	6,000	0	1,272

Table 4: Distribution of cybercrime type across sectors in Pakistan (NCCIA, 2025; Kaspersky, 2025).

Qualitative Findings

Theme 1: Motivations

- Financial pressures, thrill-seeking, and political misuse were identified as key drivers of cyber offending.

Theme 2: Vulnerabilities

- Weak cybersecurity infrastructure, insufficient inter-agency coordination, and low public awareness exacerbate risk.

Theme 3: Legal Reform Needs

- Respondents highlighted PECA (2016) inadequacies in addressing cryptocurrency fraud, ransomware, AI-driven attacks, and deep fake exploitation.

DISCUSSION

Summary of Findings

The study confirms that cybercrime in Pakistan arises from a complex interplay of socio-economic pressures, technological fragility, digital illiteracy, and outdated legal frameworks. The high prevalence of cyber offenses in urban centers validates the participants' concerns and aligns with official statistics.

Theoretical Contribution

This research extends existing frameworks by demonstrating that cybercrime cannot be fully understood through technical analysis alone. Instead, it emerges from the convergence of social, behavioral, technological, and policy-related factors, highlighting the need for integrated approaches in national cyber strategy.

Practical Implications

- Strengthening public digital literacy initiatives
- Upgrading IT infrastructure in both public and private sectors
- Implementing institutional cyber-resilience programs
- Developing early-warning mechanisms for cyber threats

Policy Implications

- Updating PECA 2016 to cover cryptocurrency crimes, AI-enabled offenses, ransomware, and deep fake misuse
- Establishing integrated national cybercrime response units
- Mandating cybersecurity standards across sectors
- Creating a national cyber observatory to forecast and mitigate emerging threats

Limitations

- Sample primarily reflects urban experiences
- Self-reported data may contain bias
- Longitudinal studies are needed to assess the impact of legislative interventions

CONCLUSION

Pakistan's expanding digital ecosystem is vulnerable to a variety of cyber threats driven by technological shortcomings, socio-economic pressures, and legal gaps. Official statistics indicate escalating incidents: NCCIA (2025) reports **142,272 complaints**, while Kaspersky (2025) identifies **5.3 million attacks**, predominantly affecting urban centers like Karachi and Lahore.

The study underscores the urgent need for **holistic cyber governance**, encompassing legislative modernization, institutional capacity-building, digital literacy programs, and public-private collaboration. Updating PECA to cover cryptocurrency fraud, AI-driven offenses, ransomware, and deep fake exploitation, alongside the establishment of dedicated cybercrime authorities and AI-based defense units, is imperative. Socio-economic interventions targeting unemployment and inequity may further reduce motivations for cyber-offending.

Global best practices, multi-stakeholder engagement, and international cooperation will enhance Pakistan's cybersecurity posture, safeguarding economic assets, public trust, and national security.

REFERENCES

Ahmed, S. (2022). Cyber security: A growing challenge to Pakistan. *Journal of the Ahmad Hassan School of Sciences*, 1(1), 1-15. https://ojs.ahss.org.pk/journal/article/download/942/983/1771

Aleem, Y., Asif, M., Khaliq, M., Imtiaz, I., & Ashraf, M. U. (2023). The Prevention of Electronic Crimes Act 2016 & shrinking space for online expression in Pakistan. *Elementary Education Online*, 20(2), 1019–1026.

Anjum, U. (2020). Cyber-crime in Pakistan: Detection & punishment mechanism. *STEDJ Univerzitet PIM, 1*(1), 1-20. https://stedj-univerzitetpim.com/wp-content/uploads/2020/12/Cyber-crime-in-Pakistan-detection-&-punishment-mechanism.pdf

Hussain, A. (2025). The role of cyber security in promoting digital inclusion: A case study of Pakistan. *Journal of the Ahmad Hassan School of Sciences*, 2(1), 45-60. https://ojs.ahss.org.pk/journal/article/view/894

Ibrahim, S. A. (2019). Cryptocurrencies & Pakistan: Challenges & risks. *Stratagem*, 1(1), 24-35.

Jamil, B., & Malik, S. (2021). Teaching science in Pakistan: Classroom challenges. *Pakistan Education Journal*, 18(2), 33–48.

Jamshed, J. (2022). Critical analysis of cybercrimes in Pakistan. *International Journal of Business, Economics & Applications*, 1(1), 1-15. https://ijbea.com/ojs/index.php/ijbea/article/view/234/197

Khilji, U. (2025). From fake profiles to deepfake porn: The war Pakistani women cannot win alone. *Asia News Network*. https://asianews.network/from-fake-profiles-to-deepfake-porn-the-war-pakistani-women-cannot-win-alone/

National Cyber Crime Investigation Agency. (2025). *Cybercrime statistics report 2025*.

Rajput, M. A. (2024). Prevention of Electronic Crimes Act, 2016: A critical review. *Federal Law Journal*, 3(1), 137–148.

Saleem, H., Jan, J., & Areej, A. (2024). Cybercrimes trends in Pakistan. *Society, Law & Policy Review*, 1(1), 1–20.

Shah, S. K. A. (2022). A critical analysis of PECA 2016. *Journal of Pakistan Administration*.

Trust, T., Carpenter, J. P., & Krutka, D. G. (2020). How & why educators use online communities. *Journal of Teacher Development*, 12(3), 45–67.

Wani, M. A., Jabin, S., Yazdani, G., & Ahmad, N. (2018). *A study of fake profiles in online social networks & the cyber law.* arXiv. https://arxiv.org/abs/1803.08810

Yusuf, J. A. B., Daneva, M., & van Sinderen, M. (2025). *Exploring risk factors for phishing victimization in Pakistan.* arXiv. https://arxiv.org/abs/2510.09249

Zahid, M. A., Muhammad, A., Khan Khakwani, M. A., & Maqbool, M. A. (2024). Cybercrime & criminal law in Pakistan. *Pakistan Journal of Criminal Justice*, 4(2), 102.