Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 3, Issue 3, 2025

POLICE STATION: UTILITY IN TACKLING DIGITAL CRIMES

Abdul Wahab (PSP)[1], Dr. Ayesha Nazuk[2]

[1, *2]SSP Punjab Police

[1]awahabjadon@gmail.com [*2]ayesha.nazuk@s3h.nust.edu.pk

DOI: https://doi.org/10.5281/zenodo.17876050

Keywords

Article History
Received: 03 May 2025
Accepted: 16 June 2025
Published: 30 June 2025

Copyright @Author
Corresponding Author: *
Dr. Ayesha Nazuk

Abstract

Theft of bicycles was a major crime in the 1980s. As time has passed, this crime has become obsolete. Presently, digital crimes such as cyber fraud, identity theft, and digital harassment are on the rise in Pakistan, posing new challenges to traditional law enforcement. Police stations, the frontline institutions for public safety, remain under-equipped to tackle these digital threats. This policy paper explores the readiness of police stations in handling digital crimes, identifies structural and operational gaps, and recommends actionable reforms. Using a mix of qualitative and quantitative data, this study draws comparisons with international best practices and proposes phased policy interventions, institutional reforms, and digital capacity building. Without urgent modernization, police stations risk obsolescence in the digital age. The paper concludes with a strategic framework along with risk analysis and mitigation strategies to enhance the institutional responsiveness of police stations in tackling emerging digital crimes.

The paper begins by analyzing the problem through a detailed literature review and field insights, followed by a situational analysis of PECA 2006 and its amended 2025 version. It utilizes Fishbone and PESTLE analyses to diagnose root causes and identify policy dimensions. Based on comparative global models, the report offers institutional, technological, and legislative reforms. Three core policy recommendations are provided, along with a strategic digital policing model and actionable implementation plan. The paper ultimately advocates for a shift from analog policing to a cyber-resilient, community-integrated police framework.

INTRODUCTION

The rapid increase in technology-based crimes in Pakistan has made traditional policing methods ineffective. Comparing 2023 to 2020, cybercrime complaints rose by 49 percent (PROPAK, 2025). Police stations, originally designed to prevent physical crimes, now face digital threats that go beyond borders, jurisdictions, and traditional investigation tool (PTA, 2024). This gap in governance threatens both public safety and the credibility of institutions. In the era of AI, cloud computing, and encrypted communication, Pakistan's police stations need to move beyond their 20th-century structure.

Cybercrime brings not just technical challenges but also social, psychological, and political consequences. With over 142.3 million broadband subscribers by September 2024 and mobile services covering 91 percent of the population, the public is increasingly exposed to cyber fraud, hacking, identity theft, and online blackmail (PTA, 2024). The police system must adapt quickly, work together, and plan ahead—but issues like outdated equipment, lack of specialized training, weak prosecution of digital crimes, and poor inter-agency coordination continue to hinder progress.

Looking forward, Pakistan's Universal Service Fund has approved Rs 7.49 billion for connectivity projects to provide high-speed internet and mobile services to over one million people in 347 areas across 10 districts, which will expand the digital attack surface (UniversalServiceFund, 2025). Additionally, with the No-Objection Certificate granted to Elon Musk's Starlink for satellite internet operations, rural and underserved areas will gain robust, low-latency connectivity. However, this expansion could be exploited by cybercriminals unless police capabilities are upgraded simultaneously (Reuters, 2025).

1.1. Statement of Problem

Police stations in Pakistan remain the backbone of law enforcement but are poorly equipped to handle modern, technology-driven digital crimes. Over 72% lack digital FIR systems, and only 18% have basic cybercrime detection tools (PICSS, 2023). At the same time, digital and modern crimes like cyber fraud and identity theft are on the rise. In 2024, the FIA received over 160,000 cybercrimes complaints, but fewer than 12% were formally investigated, with conviction rates below 2% (FIA, 2024). This shows a clear gap between traditional policing capacity and digital crime challenges. Without urgent reforms, police stations will struggle to stay relevant in the fight against digital crimes.

1.3. Research Question

Q1) How can Pakistan's police stations be transformed into modern hubs of efficiency—through institutional reforms, technological advancements, and legal updates—to effectively prevent, investigate, and respond to the growing threat of digital crimes?

1.4. Research Objectives

The purpose of this study is to assess the technological and operational capabilities of police stations in Pakistan to respond to emerging digital crimes, such as cyber fraud, identity theft, and digital harassment. In addition, policy reforms will be proposed to address the gaps identified in order to enhance the effectiveness of the police station in addressing these issues.

1.5. Scope & Significance

This study explores how prepared police stations in Lahore are to handle emerging digital crimes—like cyber fraud, identity theft, and online harassment—at the point where victims often turn first for help. While the NCCIA is officially tasked with tackling cybercrime, local stations play a crucial role as first responders, documenting incidents, securing digital evidence, and coordinating with specialized agencies. By assessing station-level infrastructure, staff skills, legal knowledge, and inter-agency collaboration, the study highlights key challenges: outdated forensic tools, inconsistent officer training, limited legal awareness, and poorly structured partnerships. These gaps leave frontline policing unprepared for modern threats. The findings are vital for policymakers in interior and provincial home departments, law enforcement leaders at the IG's office and district commands, and digital-governance stakeholders—including telecom regulators, platform providers, and civil-society advocates. Understanding "who does what, where, and why" is essential for allocating resources, improving training, reforming legal frameworks, and building public-private partnerships to strengthen Pakistan's digital security.

1.6. Literature Review

As crime increasingly shifts to the digital realm, the role of police stations is being critically re-evaluated worldwide. Scholars argue that traditional law enforcement institutions must evolve to meet the challenges posed by cybercrime, including fraud, identity theft, and digital harassment (Wall, 2021). Police stations, once designed for physical crime response, now often serve as the first contact point for victims of online offenses. However, the capacity to effectively investigate such crimes varies significantly across regions and countries.

In advanced jurisdictions like the United Kingdom, integrated national platforms such as Action Fraud and the National Cyber Crime

Unit (NCCU) offer structured support to local police units, enhancing investigation and victim support (HomeOffice, 2020). Similarly, Estonia has emerged as a global leader in digital policing through a fully digitized ecosystem that links police records with national identity systems and blockchain analytics (Kalvet, 2012). Singapore's model showcases how predictive analytics and real-time inter-agency coordination can modernize station-level policing for the digital age (Lim, 2021).

India's experience is particularly relevant to Pakistan. The Indian Cyber Crime Coordination Centre (I4C), launched in 2019, links local police stations with national cybercrime portals and forensic labs. Despite challenges in rural capacity, India has deployed cybercrime reporting portals accessible in multiple languages, thereby improving citizen engagement and centralized analytics (Mehta, 2022). However, gaps remain in real-time digital training for officers and integration across state lines.

Bangladesh, while earlier lagging behind, has made significant strides in recent years. The Digital Security Act (2018) led to the establishment of cybercrime units within district police stations, particularly in Dhaka and Chittagong. Training programs led by UNDP and national ICT divisions have empowered frontline officers, though resource disparity between urban and rural regions persists (Hossain, 2022).

In Pakistan, the Federal Investigation Agency (FIA) handles the majority of cybercrime cases, leaving local police stations marginally involved. Literature highlights that the Prevention of Electronic Crimes Act (PECA), although comprehensive in scope, is not backed by sufficient provincial implementation capacity (Rashid, 2020). The lack of integration between FIA, National Cyber Crime Investigation Agency (NCCIA), and local police units leads to delays, duplication, and underreporting of cases (Ahmed, 2021).

Thus, the literature reveals that empowering police stations with legal mandate, digital tools, and institutional alignment—as seen in India, Bangladesh, and global models—can significantly improve the response to digital crimes. However, success hinges on resource allocation, policy coherence, and digital literacy among frontline officers.

The literature gap in current studies is while existing research sheds light on national and urban-center frameworks, there is limited exploration of the ground-level realities in individual police stations. These include challenges like inadequate digital infrastructure, limited legal knowledge among frontline officers, difficulties in inter-agency coordination, and gaps in victim feedback—all of which are essential for tailoring global best practices to Pakistan's local context.

2. RESEARCH METHODOLOGY

Mixed research methodology has been employed to conduct the research. The users' review feedback was taken from 233 police officers currently working in the police stations of Lahore. The said primary data extracted from the survey is expected to draw situational analysis regarding the readiness of the police station to tackle digital crimes.

In addition, primary data was also obtained during the structured interviews conducted on 17.06.2025 with:

i. Mr. Ahsan Younas (PSP), Managing Director PSCA **(Annex-A)**

ii. Mr. Hashmat Kamal (PSP) Director NCCIA, Islamabad **(Annex – B)**

iii. Mr. Tassawur Iqbal (PSP) SSP Operations, Lahore **(Annex-C)**

iv. Mr. Ahmad Usman (Acting SP) currently leading cyber laws application in police stations in Punjab police **(Annex – D)**

Secondary data and ideas were also compiled from multiple sources reports by international organizations, websites, periodicals and research publications.

3. LEGAL FRAMEWORK

The foundation of Pakistan's cybercrime response is the Prevention of Electronic Crimes Act (PECA), first introduced in 2006 and significantly updated in 2016, 2023 and 2025. This law addresses a broad spectrum of

technology-enabled crimes, including cyberstalking, data breaches, hate speech, financial fraud, and unauthorized access to information systems. The 2025 amendments strengthened investigative capabilities, improved digital evidence handling, and promoted collaboration among agencies. However, enforcement at the local police station level remains a challenge due to amendment in section 30 and entrusting cognizance by National Cyber Crime Investigative Agency (NCCIA) and also limited technical expertise and the lack of standard operating procedures (SOPs).

Beyond PECA, other legal frameworks also address digital crimes. The Electronic Transactions Ordinance (ETO) 2002 recognizes electronic documents and digital signatures, ensuring the validity of online evidence. The Qanun-e-Shahadat Order, 1984, was amended to accept digital and electronic records in court, though many investigators and prosecutors lack awareness of these changes.

The Pakistan Penal Code (PPC) criminalizes activities like impersonation, fraud, criminal intimidation, and publishing obscene material, many of which now occur online. While the Telegraph Act of 1885 is still used in telecom-related cases, its provisions are outdated for modern ICT systems. Additionally, the Anti-Money Laundering Act (AMLA) of 2010 targets financial crimes involving virtual currencies and illicit digital transactions.

To enforce PECA and related laws, the federal government established the National Cyber Crime Investigation Agency (NCCIA) and formed its relevant rules in 2024. This agency, operating under the Ministry of Interior, focuses on intelligence sharing, training, and building the capacity of police and prosecutors nationwide. Despite these efforts, provincial police departments, particularly in Punjab and Sindh, face persistent issues such as low digital literacy, insufficient forensic facilities, and limited judicial understanding of cyber evidence. These challenges underscore that while Pakistan's legal framework for cybercrime is advancing, enforcement capabilities remain a significant obstacle.

4. SITUATION ANALYSIS

The rise of technology-driven crimes in Lahore—such as digital fraud and social media harassment—has highlighted critical shortcomings in local police stations' ability to address these modern challenges. While some digital tools and complaint systems are in place, overall readiness is hindered by insufficient training, a lack of cyber-specific protocols, poor inter-agency collaboration, and outdated infrastructure. Real-time crime response is further compromised by non-functional surveillance systems and the lack of integrated databases connecting the police with agencies like PSCA, NADRA, and FIA. Although community outreach and digital complaint systems hold potential, their scalability and institutionalization remain limited. Without targeted reforms—such as overcoming organizational inertia, establishing cybercrime desks, providing digital forensic resources, and implementing standardized referral protocols—police stations risk becoming increasingly ineffective in addressing the growing cybercrime threat (TassawurIqbal, 2025).

Despite critical amendments to the Prevention of Electronic Crimes Act (PECA) in 2023 (via Amendment Act No. XXXVII of 2023), which granted police the authority to investigate cyber offenses under Sections 21 and 22, Pakistan's policing institutions have largely failed to operationalize this mandate. Interviews with officers reveal a stark lack of institutional preparedness: no formal standing orders or SOPs were issued post-amendment; Lahore Police formed a cyber unit only verbally without logistical or technical support; and key investigative tools like IPDR (Internet Protocol Detail Records) remain inaccessible. Moreover, police were not recognized as SPOC (Special Point of Contact), severely limiting their ability to liaise with global platforms for data requests—a critical shortcoming in a digital landscape where online incitement plays a significant role in mob violence and vigilantism. Although the 2023 amendments aimed to enhance policing capacity and address rising digital threats, their ineffective implementation rendered police efforts

disjointed and dependent on manual, under-equipped processes. Between 2024/25 a total of 533 cases were registered in Lahore (Usman, 2025). The January 2025 creation of the National Cyber Crime Investigation Agency (NCCIA) effectively stripped police of most cybercrime jurisdiction, reflecting a reactive and fragmented policy approach. This transition occurred without strengthening existing police cyber units or formally evaluating their performance, thus compounding institutional inertia. While Section 21 and 22 powers remain with police in cases overlapping with the Anti-Rape Act 2021, operational gaps, poor interagency coordination, and resource deficits have left police ill-equipped to respond to online incitement that often triggers vigilante violence. In the broader context of mob lynching incidents—such as the Sialkot factory case or Punjab College unrest—the absence of a real-time, police-led digital monitoring system continues to delay interventions and weaken prosecutorial outcomes. This situation highlights an urgent need for structural reforms, inter-agency clarity, dedicated cyber units with proper forensic tools, and alignment of digital legal provisions with ground-level enforcement capabilities (Usman, 2025).

4.1 Police Officers Reviews

The survey (Questionnaire attached at **Annex-E**) assessed how well police stations in Lahore, are prepared to handle digital crimes like cyber fraud, digital harassment, identity theft, and online scams. With cybercrime on the rise and police infrastructure struggling to keep up, the survey gathered insights from officers on the ground. It looked at challenges they face, digital tools available at stations, coordination with other agencies, and their understanding of cyber laws and investigations. The goal is to guide policy changes and improve resources, creating a stronger, tech-savvy policing system for the digital era.

Summary of Key Findings (% of Respondents Reporting Issues)

Table (1) and Fig (1) below reveal significant disparities in digital readiness and operational effectiveness among police stations in Lahore faces the most challenges, with 50% of issues in staff training and 56% in cyber tool availability. Further, Lahore, a central hub, has notable weaknesses in public awareness (59%) and victim support (40.6%), suggesting communication and service delivery gaps rather than infrastructure issues.

Moreover, a shared challenge across police stations is the access to internet & IT, lack of coordination with specialized agencies, insufficient cybercrime tools and legal framework knowledge gap, pointing to broader national-level policy and funding gaps. These findings highlight the urgent need for standardized digital SOPs, staff training, and public awareness campaigns in Lahore.

Table 1

Indicator	Access to Internet & IT	Digital Infrastructure for Cybercrime	Staff Trained in Digital Evidence	Availability of Detection Tools	Training on Cybercrime Investigation	Coordination with FIA	Public Awareness Campaigns	Victim-Friendly Reporting	Legal Framework Knowledge
Lahore	42.2%	56%	50.4%	61%	54.4%	58.2%	49.2%	40.6%	53%

This specific analysis emphasizes the need for targeted interventions and policy adjustments to ensure all urban centers are equipped to address digital crimes in today's hybrid warfare landscape.

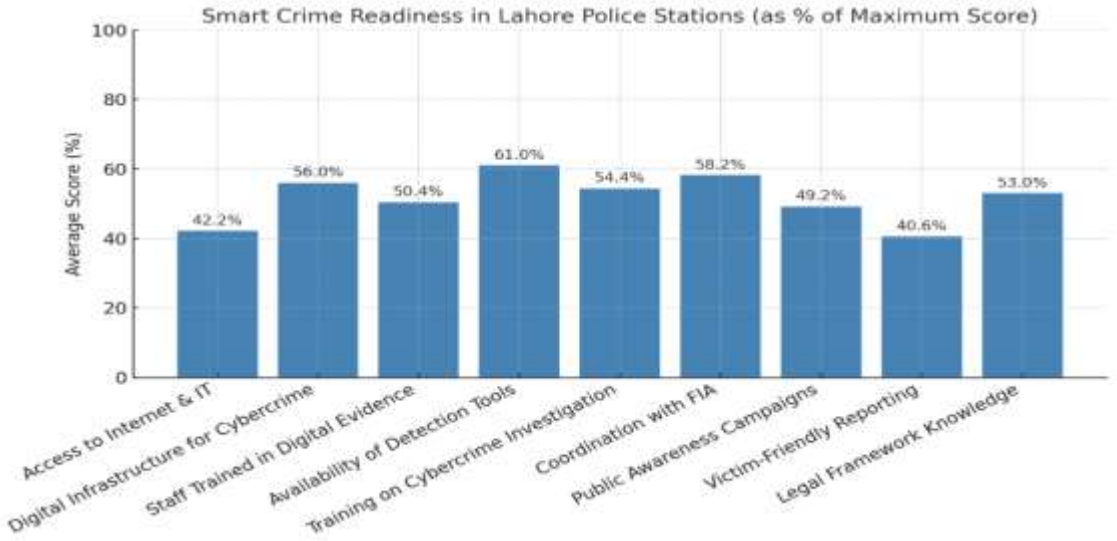


Figure 1

5. INTERNATIONAL MODELS

Several countries offer models of success in transforming police response to digital/modern crimes. Estonia, known for its advanced e-governance system, has fully digitized its police records, enabling real-time FIRs and integrated identity verification systems using national ID cards. The Estonian Police and Border Guard Board is equipped with cybercrime response units trained in digital forensics, blockchain tracking, and proactive online monitoring. The model serves an guiding role model for Pakistan police.

In the United Kingdom, the National Cyber Crime Unit (NCCU) under the National Crime Agency (NCA) operates in partnership with local police and industry players. It provides specialist training and investigative support while engaging with victims via digital portals. The UK's Action Fraud platform acts as a centralized mechanism for citizen reporting, increasing transparency and conviction rates.

These global models highlight the importance of centralized intelligence, multi-stakeholder collaboration, continuous officer training, and citizen-friendly technology. Pakistan's strategy must localize these innovations while addressing resource and capacity constraints at the provincial and station levels.

5.1 Comparative: Digital/Modern Crime Readiness at Police Station Level

Metric	India	Bangladesh	Pakistan
Cyber Units at PS Level	Present in urban Police Stations (PS) with trained Cyber Praharis (Cyber Sentinels)	Limited; major cases referred to Criminal Investigation Department (CID) Cyber Police	Mostly absent; some informal cyber desks exist (e.g., Lahore's verbal unit, 2023)
Legal Framework	Information Technology (IT) Act, 2000; Indian Penal Code (IPC) Sections 419 (cheating), 420 (fraud), 354D (stalking), 66C (identity theft), 66D (online impersonation)	Digital Security Act (DSA), 2018	Prevention of Electronic Crimes Act (PECA), 2016, amended 2025; Sections 21 & 22; overlaps with Anti-Rape (Investigation and Trial) Act, 2021

Digital FIR Integration	Fully operational through Crime and Criminal Tracking Network & Systems (CCTNS) and Inter-Operable Criminal Justice System (ICJS)	Electronic General Diary (e-GD) pilot in metropolitan police units	Partially operational e-FIR (First Information Report) and Police Station Record Management System (PSRMS); no unified national CCTNS
Public Complaint Portals	Cybercrime.gov.in – National online complaint portal linked with state police stations	Bangladesh Telecommunication Regulatory Commission (BTRC) portals and CSW helplines	FIA's (Federal Investigation Agency) National Response Centre for Cyber Crime (NR3C) handles complaints; not integrated with PSs
Mobile/Digital Forensics	Regional/state-run Digital Forensic Labs (DFLs) and mobile forensic vans	Centralized forensics under BTRC and CID Cyber Crime Units	Punjab Forensic Science Agency (PFSA) offers forensics; police stations lack direct access
Police Training Institutions	National Police Academy (NPA), Hyderabad, and State Police Academies provide cybercrime modules	Bangladesh Police Academy (BPA) and CID training centres	National Police Academy (NPA), Islamabad offers introductory cyber modules; district-level training lacking
Cyber Law SOPs at PS Level	Standard Operating Procedures (SOPs) and cybercrime manuals issued state-wise	Cyber Support for Women (CSW) desks use victim-sensitive SOPs	No official SOPs issued for PECA 2023 enforcement; police units act without formal mandate
Social Media Monitoring	State-level Artificial Intelligence (AI) tools and dashboards in major cities	Intelligence agencies do monitoring; not linked to PSs	No PS-level real-time monitoring; National Cyber Crime Investigation Agency (NCCIA) has limited provincial reach
Community Outreach	Cyber Jagrookta Abhiyan (Cyber Awareness Campaign) in schools, colleges, public forums	CSW desks + awareness drives with local NGOs and religious leaders	Limited to ad-hoc awareness sessions; no structured cybercrime education campaigns
Women/Youth Protection Units	Cybercrime protection desks for women and children in urban PSs	CSW desks in 70+ police stations offer gender-based digital protection	Gender desks exist, but do not specifically handle digital crimes; no cyber desks for women/minors

6. GAP ANALYSIS

6.1 McKinsey 7S Framework

Element	Current Challenge
Strategy	No cybercrime integration at local police level
Structure	Rigid, non-digital hierarchy
Systems	Partially Paper-based, non-digital processes
Shared Values	Focus on physical crime, digital crimes de-emphasized
Skills	Low IT literacy, lack of cyber training
Style	Command-heavy, change-resistant leadership
Staff	Low motivation, fear of redundancy

The effectiveness of police stations in addressing digital crimes in Pakistan is significantly undermined by systemic issues across the McKinsey 7S framework. Strategically, there is no localized or cohesive plan to integrate cybercrime response at the station level. Structurally, the system remains rigid and hierarchical, with no specialized cyber units or mechanisms for inter-agency collaboration. Outdated systems persist, as most stations still rely on manual along with maintenance of digital versions FIRs and lack digital case tracking or forensic tools. Shared values within the force emphasize traditional crime control, sidelining the importance of addressing cyber threats. In terms of skills, officers generally lack IT literacy and receive minimal training in digital investigations. Leadership styles are top-down and resistant to change, often failing to foster technological adaptation. Additionally, staff are demotivated, overburdened with conventional tasks, and apprehensive about being replaced by digital tools, which hinders innovation and reform.

6.2 Fishbone Analysis



Organizational inertia in police stations significantly hinders the ability to address digital crimes like cyber fraud, identity theft, and digital harassment. This inertia is evident in outdated infrastructure, untrained staff, and rigid administrative structures that resist change. Despite the increasing complexity of digital crimes, many police stations still rely on traditional, paper-based systems with little technological integration. Legal ambiguities, such as overlapping court jurisdictions that require an Investigating Officer (IO) to appear in multiple courts simultaneously, further exacerbate the issue, leading to inefficiencies and delayed justice. The absence of clear SOPs, interagency collaboration with agencies like NCCIA, and inadequate funding compound these challenges. Even motivated officers often struggle with manual tasks, outdated tools, and limited institutional support, which undermines morale and accountability. Addressing this inertia requires comprehensive reforms that tackle legal, technological, and structural gaps while empowering police with the autonomy and resources needed to tackle 21st-century crimes effectively.

6. FACTORS LEADING TO FADING WILL

A. Internal Challenges

Police responsiveness to digital and cybercrime is significantly hindered by internal organizational challenges. A key issue is the lack of digital literacy among officers, particularly at the operational level, where even basic IT skills are often missing. Focal persons can centralize expertise and rationalize digital casework, but success depends on sustained training, clear career pathways, and ring-fenced budgets. Challenges include high staff turnover, competing station duties, and procurement of specialized equipment" (MrAhsanyounas, 2025). The absence of performance-based incentives reduces motivation to adopt or advocate for digital tools. Moreover, the rigid bureaucratic structure stifles innovation and hampers bottom-up initiatives, slowing adaptation to evolving crime trends. Many officers view technology as a threat to their job security, fearing redundancy rather than seeing it as a way to enhance their capabilities. Combined with outdated SOPs and limited access to practical digital training, these

factors create significant resistance to modernization efforts.

B. External Challenges

Political interference disrupts consistent policy implementation and undermines the independence required for lasting reform. Budget shortages for digital policing infrastructure—such as forensic labs, surveillance tools, and cybercrime units—particularly in smaller districts, deter capacity growth. No proper unit or SOPs were developed after police were granted these powers" under PECA, and "forensic tools, basic need of the cyber unit, were not given" (Usman, 2025). Poor coordination between provincial police and federal agencies like NCCIA leads to overlapping responsibilities and inefficiency. Legal ambiguities in court jurisdictions force Investigating Officers (IOs) to attend multiple courts at once, reducing case quality and focus. Low public trust in police and underreporting of cybercrime further demoralize officers and impede proactive efforts. These pressures weaken institutional resolve, even when strategic policies are in place.

7. CONCLUSION

The growing prevalence of cybercrime in Pakistan has exposed the limitations of traditional police stations, which often operate with outdated systems, insufficient technology, and a lack of specialized training. Pakistan's traditional police station model, designed for 20th-century, locality-based crime, is struggling to keep up with the rapid rise in cybercrime, which surged by 49 percent over the past three years. With over 142 million broadband users and more than 72 percent of stations lacking digital FIR systems, conviction rates remain below 2 percent despite over 160,000 complaints in 2024. Without swift reforms, including technological upgrades, legal updates, and better training, police stations will remain ill-equipped to handle cross-jurisdictional threats like cyber fraud, identity theft, and online harassment. It's time to transform these analog outposts into modern hubs capable of tackling the emerging challenges of digital crimes.

8. POLICY RECOMMENDATIONS

In Lahore, digital FIR systems exist—facilitated by initiatives like the Punjab Safe Cities Authority—but tools and specialized training necessary for the detection and investigation of digital crimes (e.g., digital harassment, cyber fraud, identity theft) are unavailable. This limits the operational effectiveness of local police despite digital entry points. Given the escalating nature of digital crimes, a multipronged strategy is needed to build nationwide capacity, link station-level policing with federal agencies like the NCCIA, and introduce the technological and procedural reforms necessary for 21st-century digital. The following policy recommendations are derived from identification of gaps in literature review, interviews and surveys.

A. PECA Amendment, Training and SOP Manual also Digital Infrastructure Investment

It is imperative to amend the PECA and give cognizance to the local police since in the wake of increasing digital crimes it is the only viable and cost-effective solution. With the current strength of 477 personnel and 15 Cyber stations, NCCIA is underequipped to deal with the quantum of complaints filed for action. Besides, developing and distributing practical training modules and SOP manuals to all station-level staff. Focus on interpreting the Prevention of Electronic Crimes Act (PECA), digital evidence handling, and inter-agency protocols. Moreover, Equip all police stations with IPDR tools, digital case management software, and crime mapping tools. Build a network of encrypted servers and databases to support evidence storage and inter-station communication.

PESTLE Analysis:

Political: Needs sustained political will and intergovernmental cooperation. Also Builds uniformity in enforcement across provinces

Economic: Requires upfront investment; can reduce long-term costs via efficiency. However, it is Cost-effective approach to improve legal capacity.

Social: Improves public trust by enhancing service delivery, professionalism and transparency.
Technological: Bridges the digital divide in remote stations also ensures optimal use of existing and future tools.
Legal: Facilitates legal compliance and digital evidence admissibility as already undertaken by law.
Environmental: Reduces physical documentation and storage requirements.

B. Digital Police Station Pilots and Integrated Crime Data Platform

Launch fully digitized "digital stations" in each provincial capital (Lahore, Karachi, Peshawar, Quetta). These digital stations can also be launched in existing policing setups. Equip them with cybercrime reporting kiosks, trained digital units, and tools for cyber evidence collection. Further, establish a unified, real-time data platform connecting police, NCCIA, FIA, PTA, NADRA, and Safe City units. Also, intelligence sharing among the international organizations like UNO DC and INTERPOL may also be enhanced. This will support suspect tracking, pattern recognition, and inter-jurisdictional case handling.

PESTLE Analysis:

Political: Acts as a high-visibility governance reform initiative. It, also requires national consensus and legal data-sharing agreements.
Economic: Moderately expensive but high return in intelligence output also initial funding can be secured through international or local platform with Public-private partnership for funding.
Social: Allows proactive policing and enhances public safety. Moreover, it encourages public use through modern infrastructure.
Technological: The pilot project will Demonstrates readiness for digital transformation it will also Enables AI-driven analysis and predictive policing.
Legal: Needs strong data governance and privacy laws. Can serve as pilot sites for testing revised legal procedures. Pakistan National Digital Policy 2025 is in vogue.
Environmental: Digital-first solution reduces resource wastage.

C. Leadership Reform: DPO-Level Cyber Units along with tactical Reform: Cybercrime Focal Persons in Police Stations

Establish DPO-level cybercrime units to supervise police station operations, coordinate with NCCIA, and monitor station-level compliance with digital protocols. Deploy at least one trained focal person per police station, equipped with a handheld forensic kit and trained by NCCIA on frontline cyber detection techniques.

PESTLE Analysis:

Political: Supports devolution and specialized oversight along with allowing targeted action without systemic overhaul.
Economic: Enables more efficient allocation of digital budgets, highly scalable, low-cost intervention.
Social: Builds trust through stronger institutional leadership and Improves victim experience at the first point of contact.
Technological: Brings capability to the grassroots level. Improves integration and oversight of tools.
Legal: Streamlines supervision of PECA implementation. Strengthens digital evidence chain from the start.
Environmental: Enhances planning with minimal physical expansion. Limits physical movement of records and reduces delays.

Final Recommendation implementation of Policy A and B and afterwards merging it with Policy C: Integrated Digital Policing Strategy (IDPS)

To bridge the institutional and technological gap between Pakistan's traditional police framework and modern cybercrime realities, a holistic Integrated Digital Policing Strategy (IDPS) is essential. This strategy merges infrastructure, training, data integration, pilot testing, and community outreach into a single, scalable national plan. By leveraging agencies like the NCCIA, expanding tools and training at the station level, and building trust through citizen interfaces, the IDPS model offers the most sustainable, inclusive, and agile response to Pakistan's rising tide of digital crimes.

9- RECOMMENDATIONS

Short Term Measures (0-12 Months)

- Amend PECA and utilize and empower the police stations capacity to counter digital crimes.
- Train 1,000 officers, upgrade 50 pilot stations, launch awareness campaign for police officers.
- Launch public awareness campaigns using print, social, and digital media on cybercrime reporting.
- Appoint a designated cybercrime focal person in every district headquarters.
- Develop and disseminate PECA SOP handbooks across all provinces starting from Lahore.

Medium Term Measures (12- 24 Months)

- Establish cyber desks in 40% of all police stations nationwide.
- Formalize inter-agency SOPs between Police, NCCIA, FIA, PTA, and NADRA for real-time digital data sharing. Also, collaboration with international agencies like UNODC and Interpol.
- Procure and deploy forensic evidence kits and data backup servers at divisional level.
- Launch Mobile Digital Crime Reporting Apps tailored for urban and rural demographics.
- Integrate pilot station data into National Cyber Crime Investigation Coordination Cell (NC4).

Long Term (24 months+)

- Scale IDPS nationwide, use AI for crime prediction.
- Institutionalize cybercrime modules within all police academies and mid-career training programs.
- Expand pilot digital stations to 100% district headquarters.
- Introduce AI-driven dashboards for predictive analysis and resource deployment.
- Conduct third-party impact assessment and public audit of IDPS roll-out.

10- ACTION PLAN IMPLEMENTATION FRAMEWORK

Category	Objective	Specific Activity / Impact	KPI	Timeline	Target	Responsibility
Legal Amendment	PECA empowering police to take cognizance	Amend Section 30 of PECA to explicitly authorize police to register and investigate electronic crimes	Section 30 amended and published in the official gazette	0-12 months	Amendment enacted, gazetted, and police formally empowered under PECA	Ministry of Interior & Ministry of Law; Parliamentary Standing Committee on Interior
Training	Build officer capacity in cybercrime law and investigation	Train 1,000 officers on PECA, cybercrime detection, and digital forensics	Number of trained officers	0–12 Months	1,000 officers	Police Training Academies
Infrastructure	Equip police stations with essential	Upgrade 50 police stations with FIR	Number of stations upgraded	0–12 Months	50 stations	Home Departments & Police HQs

	digital crime capabilities	portals, terminals, and backup servers				
Public Engagement	Improve public trust and facilitate cybercrime reporting	Awareness campaigns, cyber helplines, and SMS complaint services	Increase in citizen reports (30%)	0–12 Months	30% increase in complaints	Public Relations / IT Cell
Inter-agency Coordination	Ensure seamless collaboration between police, FIA, NADRA, PTA	Develop SOPs & MOUs for real-time data sharing and case escalation	Number of SOPs signed, MoUs enforced	12–24 Months	All 4 agencies integrated	Ministry of Interior / Coordination Cell
Digital Tools	Enable field-level crime analytics and citizen interface	Launch Digital Crime Reporting App and AI dashboards	App usage statistics, dashboard reports	24+ Months	National deployment	IT Branch / MoITT

11- RISK ANALYSIS AND MITIGATION STRATEGY

Risk Category	Risk Description	Impact (H/M/L)	Likelihood (H/M/L)	Mitigation Strategy
Technical Failure	System outages, digital tool failures, or insufficient IT infrastructure	H	M	Implement redundant systems, regular audits, and vendor SLAs
Lack of Trained Personnel	Limited capacity of police officers in digital forensics and cybercrime handling	H	H	Launch regular capacity-building programs with NCCIA and police academies
Legal Ambiguities	Unclear jurisdiction and outdated cyber laws hinder enforcement	H	M	Amend PECA and synchronize jurisdiction with other laws
Inter-Agency Coordination Gaps	Lack of SOPs, MoUs, and platforms for case-sharing across institutions	H	H	Create formal coordination cells, SOPs, and integrated portals
Political Interference	Changes in political priorities or leadership impacting project continuity	M	H	Institutionalize reform through policy mandates, not individuals
Budget Constraints	Inadequate funds to sustain cybercrime units, tools, and training	H	H	Prioritize cyber budgets and engage private sector for support
Resistance to	Cultural and structural inertia in	M	H	Engage leadership in change

Change	adopting new policing models			workshops, link to promotions
Public Mistrust	Low public confidence in police's cyber handling deters reporting	M	M	Run consistent public outreach and feedback loops
Cybercrime Sophisticatio n	Smart criminals exploit advanced tools, making detection harder	H	H	Invest in AI-driven monitoring tools and real-time alerts
Data Privacy Breaches	Poor digital security leading to breaches of sensitive data	H	M	Adopt cybersecurity best practices and encrypt all digital evidence

REFERENCES

(n.d.).

Ahmed, A. &. (2021). Digital policing in Pakistan: Legal frameworks and enforcement challenges. Journal of Law and Society, 52(3), 110–124.

FIA. (2024). Annual report on cybercrime 2024. Government of Pakistan. Retrieved from https://fia.gov.pk/en/reports. Islamabad.

HomeOffice. (2020). . Cyber crime strategy 2020–2025. UK Government https://www.gov.uk/government/publications/cyber-crime-strategy-2020.

Hossain, M. &. (2022). Strengthening cybercrime response capacity in Bangladesh: Challenges and opportunities. Journal of South Asian Development, 16(2), 190–209.

Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. Electronic Government, an International Journal, 9(2), 142–157.

Lim, K. S. (2021). Smart policing in Singapore: A case study of digital transformation. Asian Journal of Criminology, 16(1), 25–42.

Mehta, V. &. (2022). Evaluating India's cybercrime response architecture: A federal challenge. Indian Journal of Criminology, 50(1), 45–63.

Mr.HashmatKamal. (2025, June 17). Interview with Mr. Hasmat Kamal Director Punjab NCCIA. (D. M. Abdul Wahab, Interviewer)

MrAhsanyounas. (2025, 06 30). Interview with Mr. Ahsan Younas PSP Director PSCA. (AbdulWahab, Interviewer)

PICSS. (2023). Digital readiness of police stations in Pakistan: A national survey. Islamabad: PICSS Publications. Retrieved from https://www.picss.net/publications. Islamabad.

PROPAK. (2025). Conviction rate in cybercrimes less than 3%: Mohsin Naqvi ProPakistani. https://propakistani.pk/2025/01/14/conviction-rate-in-cybercrimes-less-than-3-mohsin-naqvi/.

PTA. (2024). Telecom indicators: Mobile and broadband subscriptions. Retrieved from https://www.pta.gov.pk.

Rashid, M. &. (2020). The role of FIA in combating cybercrimes in Pakistan: An analysis. Pakistan Journal of Criminology, 12(2), 87–105.

Reuters. (2025, March 21). Musk's Starlink gets NOC to launch services in Pakistan, Ary News reports. Reuters.

TassawurIqbal. (2025, June 17). Interview with regarding smart crimes tackling in police station Mr. Tassawur Iqbal SSP Operations, Lahore. (D. M. Abdul wahab, Interviewer)

UniversalServiceFund. (2025). USF approves Rs 7.49 billion connectivity projects to expand high-speed internet in Pakistan. Digital Pakistan. Retrieved from https://digitalpakistan.pk/usf-launches-rs-7-49b-connectivity-projects/ digitalpakistan.pk.

Usman, D. L. (2025, June 17). Interview with Cyber Crime Cell of Lahore Police. (D. N. Abdulwahab, Interviewer)

Wall, D. S. (2021). Cybercrime: The transformation of crime in the information age. Polity Press.

ANNEX-A

Questionnaire for Sir Ahsan Younas MD PSCA

1. In your view, how relevant is the traditional police station model in combating modern, digital crimes such as cyber fraud, digital harassment, and tech-based financial crimes?

The police station remains indispensable for local intelligence gathering, community trust, and immediate response. However, to combat cyber fraud and digital harassment efficiently, PSs must integrate dedicated cyber units and digital tools alongside traditional beat duties

2. What role do you believe physical police infrastructure (police stations) can still play in a digital-first crime environment dominated by remote actors and cross-jurisdictional threats?

Stations serve as secure hubs for forensic analysis, evidence custody, and victim support centres. They also anchor multi-agency organization cells and community outreach, bridging the gap between remote cyber threats and on-the-ground policing.

3. How effectively are police stations currently integrated with platforms like Safe City, NADRA, FIA, and PTA for real-time crime monitoring and response?

Currently no such integration exists. However, Safe city provides crime analysis to the district police.

4. Do you believe assigning cybercrime focal persons in each police station is a sustainable solution? What structural or resource challenges may arise in implementing this?

Focal persons can centralize expertise and streamline digital casework, but success depends on sustained training, clear career pathways, and ring-fenced budgets. Challenges include high staff turnover, competing station duties, and procurement of specialized equipment

5. To what extent are station-level officers trained in handling digital evidence, online offenses, or AI-based surveillance inputs from Safe City systems?

Most station officers receive only basic workshops; a handful of nodal inspectors attend CTD courses. AI-driven inputs from Safe City systems are under-utilized due to lack of formal SOPs and analytic capacity at the station level

6. What technological upgrades would you consider essential at the police station level to improve their utility in tackling digital crimes?

High-speed secure Internet; standardized digital forensics kits; body-worn cameras; encrypted communication channels; local servers for e-evidence; basic intrusion-detection tools; and integration of CCTV and license-plate-reader data

7. Can community-level interaction at police stations (e.g., digital literacy drives or complaint cells) help in early detection or prevention of digital crimes? If yes, how can this be institutionalized?

Yes—regular digital literacy sessions and pop-up cyber-complaint desks build public awareness and expedite tip-offs. Institutionalization can occur via monthly outreach mandates, MoUs with telecom providers, and partnerships with local NGOs.

8. From a Safe City perspective, what kind of data-sharing protocols or digital dashboards can enhance the responsiveness of police stations to digital threats?

A unified API-driven dashboard that pushes real-time alerts e.g., anomaly scores on financial, vehicular, and network activities—into station control rooms, with role-based access and automated escalation workflows.

9. How do you evaluate the effectiveness of existing Standard Operating Procedures (SOPs) in police stations when dealing with cases involving digital platforms or encrypted communications?

After the amendment 2025 PECA is entrusted to the NCCIA.

10. Looking ahead, what structural reforms or strategic policy shifts would you recommend to modernize the role of police stations in a digital crime ecosystem?

Mandate a cyber desk in every PS with clear KPIs; integrate PS networks with NCCIA and PFSA for seamless data flow; amend Police Order to empower stations with digital search and data-preservation authority; and include hybrid-warfare modules in core training curricula.

ANNEX-B

Structured Questionnaire

Topic: Police Station Utility in Tackling Modern Crime

Interviewee: Mr. Syed Hashmat Kamal, Director Operations, National Cyber Crime Investigation Agency, Lahore

Strategic Perspective

How do you perceive the evolving role of police stations in the face of rising digital crimes and digital threats in Punjab?

Ans The role of police stations is evolving from traditional enforcement hubs to digitally empowered intelligence centers. With rising digital crimes in Punjab, police stations must integrate cybercrime units, digital evidence handling competences, and real-time data analysis. This shift requires not just technology but skilled personnel, legal readiness, and inter-agency collaboration to effectively address modern threats and protect digital public spaces.

Infrastructure & Modernization

What Infrastructure and modernizations currently exists with NCCIA? Moreover, what's the annual complaints of digital crimes to NCCIA? And What key infrastructural or technological upgrades do you believe are essential at the police station level to effectively combat cyber-enabled crimes? Further how to do you see the collaboration of NCCIA with local police station in addressing citizen's complaints of digital crimes?

Answer: NCCIA now operates with a modern forensic lab, network security hub, and 1799 helpline. Pakistan saw over 160,000 cybercrime complaints in 2024. Police stations need digital desks, digital evidence infrastructure, and power-stable systems. Effective collaboration lies in joint cyber patrolling initiatives, standardized SOPs, shared digital platforms, and regular cross-training to ensure citizen complaints are handled efficiently and timely.

Capacity Building

How well-equipped is NCCIA staff and current police station staff (SHOs, Investigators) in dealing with modern crimes like cyber fraud, digital harassment, or tech-based **financial crime**

Answer:

NCCIA staff are relatively well-trained in cybercrime handling, with access to specialized forensic tools, digital evidence protocols, and technical expertise. However, most police station staff—especially SHOs and investigators—still lack formal cybercrime training and technical capacity, making them less equipped for modern digital threats. There's a pressing need for structured capacity-building, cross-training with NCCIA, and digital literacy programs at the station level to bridge this critical skills gap.

Coordination with National Cyber Crime Cell

What mechanisms exist for collaboration between local police stations and the National Crime Cell or FIA's Cyber Wing in cases involving digital or trans-jurisdictional crimes?

Answer: Collaboration mechanisms include joint investigations, formal referrals, inter-agency coordination cells, and MoUs. For trans-jurisdictional or digital crimes, local police coordinate with NCCIA or FIA through case escalations, technical support requests, and evidence sharing protocols. However, to improve effectiveness, there's a need for standardized SOPs, shared digital platforms, and regular joint training between local police and federal cyber units.

Data and Intelligence Integration

Are there any efforts to integrate crime data from local police stations into a central intelligence framework to identify patterns and prevent crimes proactively?

Answer: Yes, efforts are underway through systems like Police Station Record Management System (PSRMS) and centralized crime analytics platforms. These aim to integrate data from local stations for real-time monitoring, pattern recognition, and predictive policing. However, full integration requires improved data standardization, inter-agency access, and analytical capacity building across all levels.

Standard Operating Procedures (SOPs)

Have any SOPs been developed or standardized by NCCIA that can be adopted across Punjab's police stations for handling digital evidence and responding to digital crimes?

Answer: Yes, NCCIA has developed standard operating procedures (SOPs) for digital evidence handling, cybercrime reporting, preservation protocols, and chain-of-custody documentation. These SOPs can be adopted across Punjab's police stations to ensure uniformity, legal compliance, and efficiency in responding to digital crimes. However, widespread implementation depends on staff training and administrative enforcement at the district level.

Community Engagement in Digital Policing

How important is community involvement and digital literacy at the local police station level in preventing and reporting modern crimes?

Answer: Community involvement and digital literacy are crucial for preventing and reporting modern crimes. Informed citizens are more likely to recognize threats, report incidents promptly, and preserve digital evidence. Local police stations must engage communities through awareness campaigns, school outreach, and digital safety workshops to build a proactive and resilient frontline against cyber-enabled crimes.

Challenges and Gaps

What are the major operational or legal constraints that limit NCCIA and a police station's ability to handle modern crime effectively?

Answer: Key constraints include limited technical resources, lack of trained personnel, absence of real-time digital tools, and no dedicated budget. Legally, overlapping jurisdictions, slow MLA processes, and gaps in cyber-specific legislation hinder timely action. Addressing these requires policy reforms, inter-agency clarity, and capacity-building at both NCCIA and police station levels.

Best Practices and Innovations

Can you share any successful models or pilot initiatives from within South Asia Region where police stations through partnerships from specialized agencies have effectively responded to tech-enabled or complex crimes?

Answer: Yes, a notable example is India's Cyber Crime Coordination Centre (I4C), which integrates local police with central cyber units through Cyber Crime Portals, training hubs, and forensic labs. Similarly, Sri Lanka's CERT partners with law enforcement to tackle digital threats. These models show that central-local collaboration, shared platforms, and continuous training can significantly enhance response to tech-enabled crimes.

Future Outlook

What is your strategic vision for enhancing the capacity and relevance of police stations

in Punjab to meet the future landscape of crime? Are there any plans by NCCIA to manage its operation through police stations?

Answer: My strategic vision is to transform police stations into digitally enabled, community- connected crime hubs, equipped with cyber desks, trained staff, and digital reporting tools. NCCIA should act as a technical backbone, with future plans to decentralize operations via police stations, enabling faster response, localized expertise, and seamless case flow from complaint to conviction.

Respondent: SSP Operations, Lahore

ANNEX-C

Topic: Utility of Police Stations in Tackling Digital Crimes

1. How has the crime landscape in Lahore evolved with the rise of technology-driven offences such as digital fraud, mobile banking scams, and social media harassment?

Ans: The crime landscape in Lahore has undergone a serious transformation owing to the involvement of technology. Traditional crimes are now supplemented by a surge in technology-driven offences, including digital fraud, mobile banking scams, social media blackmail, and identity theft. These crimes often cross physical jurisdictions and require swift, tech-enabled responses. This incidence of crime in cyber space has made detection and prosecution very complex.

2. Are police stations in Lahore currently equipped—both technically and administratively—to address digital crimes effectively? What gaps do you observe?

Ans: While police stations in Lahore have made strides in adopting digital tools, the overall preparedness remains unsatisfactory. Though usage of CDRs, mobile forensics, PSCA, DIGITAL EYE softwares and other investigation tools are available, they fall short to meet the demands of increasing sophistication of crime besides scarcity of trained manpower with capacity and capability to deal with rising number of these crimes. Administrative bottlenecks, limited budgets, and the absence of standardized cybercrime SOPs further impede efficient handling of tech-based offences.

3. How are Station House Officers (SHOs) and investigating officers trained to deal with digital evidence and online offences at the thana level?

Ans: Currently, basic orientation on cybercrime is provided during induction and occasional refresher courses to investigation officers that help understand the nature of crime and conduct a preliminary enquiry into certain crimes under the given head. However, comprehensive training in digital evidence handling, metadata analysis, and cyber laws is limited. A Cybercrime Investigation Cell was established at DIG INVESTIGATION Office with the aim of building the capacity of investigation officers and giving them practical knowledge and understanding of cybercrime crime, but that remain an advisory office suggesting not more than section of PECA Act rather than helping investigate crime. Moreover, it is already abolished with the establishment of a Cybercrime Investigation Agency.

4. What role do police stations play in coordinating with specialized bodies like the Punjab Safe Cities Authority (PSCA), FIA Cybercrime Wing, or NADRA when dealing with tech-based offenses?

Ans: Police stations serve as the first point of contact for victims and thus play a central role in

initiating coordination with specialized bodies. In cases involving digital or financial fraud, SHOs often refer cases to the FIA Cybercrime Wing. For CNIC verification or biometric trails, coordination with NADRA is critical. Similarly, PSCA assists with surveillance footage and digital trails. However, this coordination is often informal and reactive rather than institutionalized.

5. Have any police stations in Lahore piloted digital reporting tools, complaint kiosks, or community awareness programs related to digital crimes? If so, what impact have you observed?

Ans: Yes, digital complaint systems and kiosk-based reporting in collaboration with PSCA are in place. The complaints are often reported through a 15-Call falling in at PSCA and from there to field formations for immediate response and necessary legal action. Complaint Management System (CMS) generates an etag on every such call and thereby automatically registering the same complaint at Police Station. Similarly, there are Panic Buttons installed at various locations by PSCA for reporting harassment and other cases. Community awareness sessions, especially in educational institutions, have been conducted under various campaigns. The impact has been positive in terms of increased reporting, improved public trust, and faster complaint processing, but scalability remains a challenge.

6. What operational hurdles do you face in providing stations with access to tools such as cybercrime SOPs, real-time surveillance feeds, or digital forensics resources?

Ans: Major hurdles include budgetary constraints, lack of inter-agency data integration, insufficient training, and the absence of a centralized cybercrime protocol. Real-time surveillance from PSCA is available but often requires formal requisition, delaying response time. Forensics support is centralized and not easily accessible at the police station level. More than 50% of the cameras of PSCA installed in Lahore are not working due to budgetary and maintenance constraints. Decentralization and digitization of these resources would greatly improve operational efficiency.

7. To what extent are existing FIR registration and case progression systems integrated with digital crime tracking platforms at the station level?

The Police Station Record Management System (PSRMS) provides a digital platform for FIR registration and case tracking. However, it is not yet fully integrated with cybercrime monitoring systems. Consequently, digital crimes are often logged like conventional crimes, which limits analytical insights and real-time response capabilities. Integration with NADRA, PTA, and banking fraud units is still a distant dream.

8. Is there a designated process for referring cyber or technology-enabled cases from police stations to relevant specialized units? How effective is this handover mechanism?

Ans: Yes, there is a process in place wherein SHOs refer cyber-related complaints to the FIA Cybercrime Wing or seek technical support from PSCA. However, this mechanism is informal and varies from station to station. There is a pressing need to develop a standardized, time-bound referral and feedback loop to improve coordination and case resolution timelines.

9. How do you view the role of police stations in conducting public outreach on safe digital practices, especially in densely populated urban areas of Lahore?

Ans: Police stations are the fundamental unit in policing system of Pakistan. They are crucial outreach hubs. People come and look towards Police Stations for redressal of all their grievances. In collaboration with civil society, educational institutions, and digital rights organizations, they can play a proactive role in community sensitization. Programs aimed at safe internet usage, fraud prevention, and data privacy

can be routed through Community Police Officers, Public Laison Committees, and Peace Committees. Unfortunately, such initiatives are not yet institutionalized, though they hold great potential in crime prevention.

10. What key reforms or capacity-building measures would you recommend to enhance the ability of Lahore's police stations to address digital crimes proactively and efficiently?
Ans: Key recommendations include:
1. Establishing Cybercrime Desks at all police stations.
2. Specialized training programs for SHOs and IOs in digital crime and evidence handling, cyber laws, and investigation techniques.
3. Integration of police systems with PSCA, NADRA, PTA, and FIA platforms for real-time data access.
4. Deployment of digital forensic kits and basic IT infrastructure at the Police Station level.
5. Increasing outreach of PSCA and integration of private CCTV cameras with PSCA through legislation.
6. Formulation of SOPs to guide first responders in handling tech-based offences

ANNEX-D

Semi-Structured Interview Guide:
Digital Policing & Institutional Reforms in Lahore
Respondent: DSP Legal Ahmed Usman
Designation: Deputy Superintendent of Police (Legal), Lahore
Date of Interview: June 17, 2025
Interview Mode: Telephone

Section 1: Organizational Structure and Current Operations
Q1: Can you briefly describe the current structure of the cybercrime unit under Lahore Police?
A1: The unit is headed by DSP Cyber under DIG Investigation. A front desk at Investigation HQ receives applications. After verification, cases are forwarded to DIG Operations for FIR registration. There are 22 circles in Lahore; 11 inspectors cover 2 circles each. Unit strength is around 200 officials.

Section 2: Legal Powers and Amendments
Q2: Has the police retained powers under the Prevention of Electronic Crimes Act (PECA) after the January 2025 amendment?
A2: After the 2025 amendment, police still retain power to investigate Sections 21 and 22 of PECA, especially when these offenses are committed alongside Anti-Rape Act 2022 scheduled offenses.
Q3: What are the major legal or institutional challenges faced in exercising these powers?
A3:
No proper unit or SOPs were developed after police were granted these powers.
Forensic tools were not provided.
Police were not made SPOC (Special Point of Contact), thus blocking data access from platforms.
IPDR (Internet Protocol Detail Records), critical for investigation, was not made accessible.

Section 3: Performance and Institutional Reform
Q4: How would you evaluate Lahore Police's performance relative to other agencies like FIA?
A4: Police performed more efficiently than FIA but lacked institutional support and legal clarity post-PECA amendment.
Q5: What major reform occurred in 2025 concerning cybercrime jurisdiction?
A5: A new federal agency named NCCIA (National Cyber Crime Investigation Agency) was created in 2025, effectively removing cybercrime investigation powers from the police.

Section 4: Summary Observations

Q6: In your opinion, what are the critical gaps that must be addressed?
A6:
Lack of institutional ownership by senior police command.
Absence of SOPs and dedicated cyber units.
Lack of resources and data access (e.g., IPDR).
Missed opportunity to be recognized as SPOC.
Urgent need for coordinated digital policing reforms.

ANNEX-E

Survey Questionnaire

Q1) Where is your police station located?
Q2) Our police station has access to reliable internet and IT infrastructure necessary for handling digital crime.
Q3) Is your police station equipped with the necessary digital infrastructure to register and track cyber-crime cases.
Q4) The staff at our station is adequately trained to handle digital evidence.
Q5) Cyber-crime detection tools and software are regularly available to us
Q6) Our staff receives regular training to investigate cyber fraud, identity theft, and online harassment cases.
Q7) There is an effective system for coordinating with specialized agencies such as the FIA Cyber-crime Wing.
Q8) Please describe any Standard Operating Procedure (SOP) you are aware of for handling digital evidence or online offenses in your area of jurisdiction/department?
Q9) We actively engage in public awareness efforts on cybercrime prevention and reporting mechanisms
Q10) Victims of digital crimes can easily report incidents at our station and receive timely responses
Q11) We maintain updated knowledge on the legal frameworks surrounding cybercrime and data protection