Vol. 3 No.2 2025

RECOGNIZED IN "Y" CATEGORY BY

Research Consortium Archive
P(ISSN) : 3007-0031
E(ISSN) : 3007-004X
https://rc-archive.com/index.php/Journal/about

An Analysis of the Effectiveness of FIA Cyber Crime Laws in Preventing and Investigating Online Fraud in Pakistan: Challenges

Wahab Ahmad
Assistant Director (Investigation)
Cybercrime Wing, Federal Investigation Agency, Pakistan.
fiawahabahmad@gmail.com

Usman Asghar (Corresponding Author)
Ph.D. Law (Scholar), TIMES University, Multan, Pakistan.
usmanpasha225@gmail.com

Madiha Afzal
Ph.D. Law (Scholar), Shariah and Law,
International Islamic University, Islamabad, Pakistan.
madihahammad143@gmail.com

Publisher : EDUCATION GENIUS SOLUTIONS
Review Type: Double Blind Peer Review

ABSTRACT

The rapid expansion of digital technology and internet usage in Pakistan has led to a corresponding rise in cybercrimes, particularly online fraud. This study critically analyzes the effectiveness of the Federal Investigation Agency (FIA) Cyber Crime Laws, primarily governed by the Prevention of Electronic Crimes Act (PECA) 2016, in addressing online fraud. It explores the mechanisms in place for prevention and investigation, evaluates the operational efficiency of the FIA Cyber Crime Wing, and identifies key challenges hindering effective enforcement. The research finds that despite the presence of a legal framework, significant obstacles—such as lack of technical expertise, inadequate resources, delayed prosecutions, poor inter-agency coordination, and limited public awareness—undermine the law's impact. Additionally, issues related to jurisdiction, digital evidence collection, and judicial capacity further complicate enforcement. Through a combination of doctrinal analysis, case study evaluation, and expert interviews, the paper proposes targeted reforms aimed at strengthening institutional capacity, updating legal tools, and enhancing public engagement. The study concludes that a multi-faceted approach—incorporating legal, administrative, and technological advancements—is essential for improving Pakistan's ability to combat online fraud effectively and protect its citizens in the digital space.

Keywords: FIA, Cyber Crime Laws, Online Fraud, PECA 2016, Pakistan.

1. Introduction

In the digital age, the proliferation of information and communication technologies has transformed various aspects of life, enabling greater connectivity and convenience. However, it has also ushered in new forms of criminal activity, notably cybercrime and online fraud. In Pakistan, as in many other countries, the rapid growth of internet users—now numbering over 124 million—has been accompanied by a corresponding increase in cyber-related offenses. Online fraud, in particular, has become one of the most pervasive and damaging forms of cybercrime, affecting individuals, businesses, and government institutions alike. From phishing attacks and financial scams to identity theft and unauthorized access to personal data, the evolving nature of online fraud presents significant challenges to law enforcement and regulatory bodies (Wajahat et al., 2025).

To address this growing threat, Pakistan established the Federal Investigation Agency's (FIA) Cyber Crime Wing, tasked with investigating and prosecuting cyber offenses under the Prevention of Electronic Crimes Act (PECA) 2016. The FIA, as the principal federal institution for combating cybercrime, plays a central role in ensuring cybersecurity and protecting citizens from the financial

and psychological damage caused by online fraud. Despite the existence of a legal and institutional framework, concerns about the effectiveness of these mechanisms persist. Issues such as delayed investigations, lack of technical expertise, limited resources, jurisdictional conflicts, and inadequate public awareness have raised questions about the FIA's ability to prevent and investigate online fraud effectively (Azhar et al., 2025).

The importance of this issue cannot be overstated. Cyber fraud not only causes financial losses—sometimes amounting to millions of rupees—but also undermines public trust in digital platforms and e-governance initiatives. It can destroy reputations, endanger sensitive personal data, and in severe cases, impact national security. For vulnerable populations, including the elderly, women, and those with limited digital literacy, the risks are particularly high. In a developing country like Pakistan, where efforts are underway to digitize various sectors, the threat posed by cyber fraud has wide-ranging socio-economic implications. Thus, a critical evaluation of the existing laws and their enforcement is essential for strengthening cybersecurity in Pakistan.

This research seeks to answer the central question: *"How effective are FIA cyber crime laws in preventing and investigating online fraud in Pakistan?"* This question lies at the core of understanding whether current legislative and institutional efforts are capable of addressing the complex and fast-evolving landscape of online fraud. While PECA 2016 provides a legal basis for identifying and penalizing cyber offenses, its implementation by the FIA is often criticized for being slow, inconsistent, and reactive rather than proactive. These shortcomings necessitate a comprehensive investigation into the law's actual performance in the real world, particularly in terms of case resolution rates, technological capabilities, victim support, and public engagement (Kaifa et al., 2025).

The main objectives of this research are fourfold:

- **To analyze the current legal framework**, particularly PECA 2016 and its provisions related to online fraud, and assess their adequacy in dealing with modern cybercrime trends.
- **To evaluate the performance of the FIA's Cyber Crime Wing**, examining how efficiently it investigates and prosecutes online fraud cases and what internal or external factors hinder its effectiveness.
- **To identify key challenges** in law enforcement, including technological limitations, legal ambiguities, inter-agency coordination, training deficits, and public cooperation.
- **To propose practical recommendations** for improving cybercrime legislation and the institutional capacity of the FIA to respond to and prevent online fraud in the future.

The scope of this research is both descriptive and analytical, focusing primarily on the legal, institutional, and practical aspects

of cybercrime regulation in Pakistan. While it centers on the FIA's role, it also briefly considers the involvement of other stakeholders, such as the judiciary, internet service providers, financial institutions, and the general public. The study will employ qualitative methods, including content analysis of legal documents, review of case studies, expert opinions, and available statistical data, to construct a nuanced understanding of the issue (Saleem et al., 2025).

This introduction lays the groundwork for a detailed exploration of the effectiveness of FIA cyber crime laws in Pakistan. As cyber threats continue to grow in scope and sophistication, the need for a robust, agile, and well-resourced cybercrime response system becomes ever more critical. By investigating the current gaps and limitations and offering forward-looking solutions, this research aims to contribute to the development of a safer digital environment in Pakistan (Kanwel, Khan, et al., 2024a).

2. FIA Cyber Crime Laws and Regulations

Cybercrime has rapidly emerged as a major challenge for law enforcement agencies across the globe, and Pakistan is no exception. In response to the rising incidence of online fraud and digital offenses, the Pakistani government has developed a legal framework aimed at combating cybercrime. Central to this framework is the **Prevention of Electronic Crimes Act (PECA) 2016**, alongside the operational role of the **Federal Investigation Agency (FIA)**. This section provides an in-depth examination of the laws and regulations governing cybercrime in Pakistan, with particular emphasis on PECA 2016, and analyzes the role of the FIA in preventing, investigating, and prosecuting cybercrime, especially online fraud (Haque & Abbasi, 2025).

i. Overview of FIA Cyber Crime Laws

The primary legislation that governs cybercrime in Pakistan is the **Prevention of Electronic Crimes Act (PECA) 2016**, which replaced the outdated Electronic Transactions Ordinance (ETO) of 2002. PECA was enacted in response to the need for a robust legal structure to deal with the increasing complexity and volume of electronic crimes in Pakistan, especially with the exponential growth of internet usage and digital financial services. The law aims to provide legal recognition to electronic transactions, safeguard against unauthorized access and misuse of information systems, and facilitate law enforcement agencies in addressing digital offenses (Ch et al., 2024).

PECA 2016 covers a broad range of cyber offenses including:

- Unauthorized access to information systems and data
- Cyberstalking and cyberbullying
- Online harassment and blackmail
- Electronic fraud and identity theft

- Cyberterrorism and hate speech
- Distribution of illegal content, including child pornography
- Spamming and spoofing
- Criminal breach of trust via electronic means

Under PECA, cyber fraud—defined as the use of electronic means to deceive and unlawfully gain access to financial information, funds, or services—is a punishable offense, carrying penalties that include imprisonment, fines, or both. The Act also grants the government authority to remove, block, or restrict access to online content that is deemed unlawful or harmful to the public interest (Qasim et al., 2025).

Additionally, PECA lays out detailed procedures for investigation, evidence collection, search and seizure of electronic devices, and international cooperation in cross-border cybercrime cases. One of the key strengths of PECA is that it provides for the admissibility of electronic evidence in court proceedings, which is crucial for the successful prosecution of cybercrime cases (Kanwel, Asghar, et al., 2024b).

Despite these provisions, PECA has faced criticism from various stakeholders, particularly concerning vague definitions, inadequate safeguards for digital rights, and potential misuse of authority. Critics argue that while the law was intended to protect citizens from cyber threats, it has at times been used to suppress free expression and dissent (Khan et al., 2024).

ii. Role of FIA in Cyber Crime Investigation

The **Federal Investigation Agency (FIA)** is the principal law enforcement body responsible for the implementation of PECA and the investigation of cybercrimes in Pakistan. The FIA operates under the Ministry of Interior and has a specialized wing known as the **Cyber Crime Wing (CCW)**, which handles cybercrime cases across the country.

The **FIA Cyber Crime Wing** is tasked with:

- Receiving and processing cybercrime complaints
- Conducting preliminary inquiries and full-scale investigations
- Collecting digital forensic evidence
- Arresting and prosecuting offenders
- Collaborating with other national and international law enforcement bodies

The FIA has established **Cyber Crime Reporting Centers (CCRCs)** in major cities, which serve as operational hubs for the registration and processing of cybercrime complaints. Citizens can also file complaints through the agency's **online portal**, which has significantly improved accessibility and responsiveness.

In terms of technical capacity, the FIA has developed **Digital**

Forensic Laboratories, where trained professionals analyze electronic evidence such as emails, mobile phone records, IP addresses, and device data. The agency also runs **awareness programs** to educate the public about the risks of cybercrime and how to avoid falling victim to online scams and fraud (Iqbal et al., 2025).

However, the FIA faces several institutional and operational challenges that undermine its effectiveness in cybercrime investigation. These include:

- **Limited technical expertise and resources**: Cybercrime investigation requires specialized knowledge in digital forensics, encryption, and network analysis. The FIA's capacity in this regard remains underdeveloped, particularly in regional offices.
- **High caseload and delays**: Due to the rising number of cybercrime complaints, the FIA is overwhelmed with cases, leading to investigation delays and backlog in prosecutions.
- **Jurisdictional issues**: Cybercrime often transcends borders, making it difficult for the FIA to track perpetrators located outside Pakistan. Although PECA provides for international cooperation, the implementation of mutual legal assistance remains inconsistent.
- **Lack of coordination**: Effective cybercrime investigation often requires coordination among multiple stakeholders, including telecom operators, internet service providers (ISPs), and financial institutions. The absence of clear protocols for inter-agency collaboration hampers the investigation process.
- **Victim reluctance**: Many victims of cyber fraud, especially women and marginalized groups, are hesitant to report incidents due to fear of social stigma, lack of trust in law enforcement, or uncertainty about the legal process.

Despite these challenges, the FIA continues to play a pivotal role in addressing cybercrime in Pakistan. The agency has made notable arrests in high-profile cases involving phishing scams, financial fraud, data breaches, and online harassment. Its increasing engagement with technology partners, international law enforcement bodies, and civil society organizations reflects a growing recognition of the need for a multi-stakeholder approach to cybercrime prevention (Shoukat et al., 2025).

3. Effectiveness of FIA Cyber Crime Laws

The Federal Investigation Agency (FIA), under Pakistan's Prevention of Electronic Crimes Act (PECA) 2016, has become the primary law enforcement body tackling online fraud and cybercrime. Assessing its effectiveness requires examination through case studies, statistical trends, and the obstacles the agency confronts in both

prevention and investigation (Kanwel, Asghar, et al., 2024a).

i. Case Studies of Online Fraud Investigations

Examining selected high-profile investigations highlights both the FIA's capabilities and constraints.

- **Axact Fake-Degree Scam (2015–2018):** Perhaps one of the most notorious online frauds involved Axact, which ran a global fake-degree operation. The FIA executed coordinated raids, seized evidence, and arrested key individuals, including CEO Shoaib Shaikh. The case resulted in convictions—including 20-year sentences for Shaikh and top executives—which showcased the FIA's capacity for tackling sophisticated digital fraud.

- **Pakistani Hackers Targeting Banks (2016):** In another major operation, a network targeting financial institutions was dismantled through digital forensics and collaboration with international law enforcement. Arrests in this case prevented future monetary loss and demonstrated FIA's ability to trace cross-border cybercriminal networks.

- **K-Electric Ransomware Attack (2020):** When NetWalker ransomware crippled Pakistan's largest electricity provider, the FIA (through its NR3C strike unit) acted promptly—isolating systems, coordinating with cybersecurity experts, and restoring operations. The incident highlighted the agency's crisis response to critical infrastructure threats.

- **Cyber Harassment/Blackmail (2017–2021):** Numerous cases, involving blackmail and harassment, saw FIA employ forensic tracking to locate perpetrators. The arrest and prosecution under PECA created legal precedents and reinforced victim reporting pathways.

These examples reflect FIA's ability to navigate complex cyber investigations—from ransomware and financial theft to harassment and large-scale scams—while leveraging digital forensics and inter-agency coordination (Shabbir & Adnan, 2025).

ii. Statistics and Trends: The Rising Tide of Digital Fraud

The scale of online fraud in Pakistan has risen precipitously. According to HUM Investigates and FIA data:

- More than **550,000 complaints** filed over six years, with **Rs 600 billion** in reported losses. Over 350,000 complaints lodged in the past 2½ years alone.

- The FIA Cybercrime Wing logged **approximately 639,000 complaints from 2020 to 2024**, of which 414,260 were verified. These led to 73,825 detailed inquiries, 5,713 court cases, 7,020 arrests, and 222 convictions.

- Annual complaints peaked in 2022 at 152,136 and dipped to 123,893 in 2024—though the decline may reflect settlements rather than a true reduction in crime.
- From 2021 to 2023, about 386,600 complaints were lodged, 48,158 inquiries launched, 4,067 FIRs registered, and convictions rose from 38 to 92.
- A recent report noted daily averages in Lahore alone of **40–50 new fraud complaints**, with a backlog of over **16,700 pending** cases.
- Punjab recorded 26,924 online fraud cases between 2018 and 2022—out of 31,930 total cybercrime complaints—averaging around 15 fraud cases per day.

The data reflect escalating volumes of reported fraud—particularly in financial scams, phishing, fake loans, and unauthorized SIM use—amplified by widespread smartphone and internet adoption. However, conviction rates remain modest: e.g., only 222 convictions out of over 414,000 verified complaints since 2020 (~0.05%) (Zahid et al., 2024).

4. Challenges Faced by FIA

Despite legislative tools like PECA and institutional initiatives such as forming the National Cyber Crime Investigation Agency (NCCIA) in May 2024, the FIA confronts systemic barriers that impede its effectiveness.

A. Resource and Capacity Constraints

- The cyber wing is **understaffed**—HUM reported a 27% personnel gap. Only a small, technically trained core handles thousands of cases .
- Budgetary allocations are often delayed or inadequate. Officers may lack basic utilities, with chronic shortages in forensic tools and infrastructure .
- FIA's presence is limited to major urban centers, forcing rural victims to travel long distances—discouraging reporting and follow-up,

B. Case Backlog & Investigation Bottlenecks

- Hundreds of cases per day strain investigative capacity. Lahore alone sees 40–50 daily complaints; Punjab had 16,700 pending.
- Digital investigations are complex and time-consuming—tracking money through microfinance apps, Jazz Cash, SIMs, and shell accounts can take **1–3 months or more**, with some cases dragging up to 6 months.

C. Legislative and Judicial Shortcomings

- PECA classifications lead to some offences being non-cognizable, requiring warrants or accompaniment by cognizable crimes—delaying arrests and investigation.
- Courts are slow, and specialized cybercrime courts are often inaccessible outside big cities. Low conviction rates (e.g., 32 convictions from 56,000 complaints in 2019) highlight enforcement gaps.

D. Public Awareness and Reporting

- Public understanding of cyber fraud remains low. Many victims remain unaware of reporting mechanisms or don't report due to stigma or perceived complexity.
- Fraudsters exploit social engineering—posing as government or bank officials using fake SIMs or silicone fingerprints—to target vulnerable groups like the elderly.

E. Technical and Jurisdictional Barriers

- Fraud networks often cross borders; cooperation from global platforms remains limited. Only ~1,130 responses came from 16,000 requests between 2019–2023 to Meta and other platforms.
- Outdated forensic labs hamper digital evidence processing, and telecom operators may be slow to trace SIM issuance or usage.

iv. Conclusion & Way Forward

The FIA's cybercrime enforcement represents a significant step in Pakistan's battle against online fraud. Through major arrests and legal action under PECA, it has established important jurisprudence and deterred some cybercriminals. However, persistent under-resourcing, chronic backlogs, limited technical capacity, and low public awareness continue to blunt its impact. Conviction rates remain disproportionately low given the volume of verified complaints (Faisal et al., 2024).

To improve effectiveness, the following measures are essential:

- **Expand and equip investigative units**: Adequate personnel, forensic labs, and infrastructure, along with district-level outlets, can expand reach and reduce case timelines.
- **Simplify legal procedures**: Amend PECA to reduce non-cognizable classifications, enabling quicker arrests and digital evidence gathering.
- **Scale public awareness**: Nationwide education and outreach campaigns—especially focusing on financial fraud and digital hygiene—can help reduce victimization and improve reporting.
- **Strengthen inter-agency and international collaboration**: Enhance cooperation with PTA, SBP, telecom firms, banks, and

global platforms to trace cross-border and app-based fraud more effectively.

While the FIA has demonstrated notable successes, evolving technological threats demand structural reform and capacity-building to fulfill the promise of robust cybercrime enforcement under Pakistan's cybercrime laws.

5. Challenges and Limitations

The effectiveness of the Federal Investigation Agency (FIA) in curbing and investigating online fraud in Pakistan is significantly hindered by a range of challenges and limitations. These issues reduce the overall impact of cyber crime laws such as the Prevention of Electronic Crimes Act (PECA) 2016. While the legal framework provides a formal basis for combating cyber crimes, its implementation is hampered by several key obstacles, including lack of public awareness, insufficient institutional resources, and jurisdictional complications. Addressing these challenges is essential to ensure that the FIA's cyber crime wing can function more effectively in the digital age (Malik et al., 2024).

i. Lack of Awareness

One of the most critical challenges in tackling online fraud is the widespread lack of awareness among the public regarding cyber crime laws, digital safety practices, and available legal remedies. In many parts of Pakistan, especially in rural or less educated communities, individuals are unaware of how to identify, report, or respond to online scams. This knowledge gap makes them easy targets for cyber criminals who exploit their lack of understanding (Bukhari et al., 2024a).

Moreover, many victims do not report cyber fraud due to fear, embarrassment, or the misconception that reporting will not lead to meaningful results. Some also confuse cyber crime with conventional crime and are unfamiliar with how to approach the FIA or utilize online complaint portals like the Cyber Crime Reporting Center. This disconnect between legal infrastructure and public knowledge limits the effectiveness of existing laws, as law enforcement cannot act on unreported crimes (Kanwel et al., 2024).

Even among educated urban populations, there is often a superficial understanding of digital security, with many individuals using weak passwords, ignoring privacy settings, or engaging with suspicious links and content online. The government and civil society organizations have not yet fully implemented large-scale awareness campaigns or digital literacy programs, particularly in schools and colleges, where early intervention could have a long-term preventive impact (Bukhari et al., 2024b).

ii. Insufficient Resources

Another major challenge facing the FIA's cyber crime wing is the lack of sufficient technical, financial, and human resources. As the volume and complexity of online fraud cases increase, the agency often finds itself overwhelmed and under-equipped to deal with

emerging threats. While the PECA 2016 grants the FIA authority to investigate a broad spectrum of cyber offenses, the implementation of these powers requires a robust infrastructure that is currently lacking (H. Khan et al., 2024).

The cyber crime wing suffers from a shortage of trained personnel, including cyber forensic experts, ethical hackers, and IT professionals. Investigating online fraud requires specialized knowledge and tools, especially in tracing digital footprints, decrypting communication, and collecting admissible digital evidence. However, many FIA investigators are not adequately trained or are overburdened with large caseloads, leading to delays in investigations and ineffective case handling.

Additionally, the FIA's technical infrastructure is outdated and lacks modern forensic labs and data analysis tools. With the rapid evolution of cyber criminal techniques—such as phishing, ransomware, fake websites, and cryptocurrency scams—the agency struggles to keep up. Budget constraints further exacerbate this problem, as cyber crime units often receive less funding compared to other departments, reflecting a broader institutional neglect of digital security (Shaheen et al., 2024).

Moreover, the existing FIA offices are centralized in major cities, making it difficult for victims in remote or rural areas to access services. Although the agency has launched online complaint portals and hotlines, their effectiveness is undermined by technical glitches, delayed responses, and a lack of multilingual or user-friendly interfaces (Zafar et al., 2024).

iii. Jurisdictional Issues

Cyber crime, by its nature, often transcends national and provincial boundaries, creating complex jurisdictional issues that impede effective investigation and prosecution. In Pakistan, jurisdictional challenges arise both within the country—between provinces and different agencies—and internationally, when crimes involve foreign actors or digital platforms based outside Pakistan (Kanwel, Khan, et al., 2024b).

Domestically, coordination between the FIA and provincial law enforcement agencies is often weak. For example, if a cyber fraud incident originates in one province and affects individuals in another, conflicts over jurisdiction can delay or derail the investigation. In some cases, local police are unaware of their roles in cyber crime cases, mistakenly considering such matters to fall exclusively under the FIA's purview. This confusion creates legal gray areas and fosters bureaucratic inertia (Sharmeen, 2024).

Moreover, the lack of a harmonized and standardized data-sharing mechanism between agencies further complicates matters. Without streamlined communication and cooperation, cases fall through the cracks, leading to low conviction rates and prolonged investigations.

On the international front, cyber crimes involving foreign entities pose even greater challenges. Many online fraud schemes operate through offshore websites, social media platforms, and digital

wallets registered in jurisdictions with limited cooperation treaties with Pakistan. The absence of effective mutual legal assistance treaties (MLATs) or slow diplomatic procedures makes it extremely difficult to obtain evidence, track suspects, or secure extraditions (Mukhtar & Siddiqah, 2024).

Furthermore, global tech companies such as Facebook, Google, or WhatsApp, which are often key to investigations, are headquartered abroad and are not legally obligated to comply with Pakistani requests without fulfilling lengthy legal formalities. This severely hampers time-sensitive investigations and gives criminals an undue advantage.

6. Recommendations

To address the challenges hindering the effectiveness of FIA cyber crime laws in combating online fraud in Pakistan, a multi-pronged and strategic approach is essential. This section outlines targeted recommendations focusing on strengthening laws and regulations, capacity building for law enforcement agencies, and public awareness. These measures aim to enhance both the preventive and investigative mechanisms of cyber crime control in Pakistan.

i. Strengthening Laws and Regulations

Although the Prevention of Electronic Crimes Act (PECA) 2016 provides a legal framework for dealing with cyber crimes in Pakistan, it requires substantial refinement and supplementation to address the evolving nature of online fraud. The following recommendations focus on legislative and regulatory improvements:

- **Periodic Review and Amendment of PECA 2016:** The nature of cyber crime is dynamic, with new types of online fraud emerging regularly. Therefore, it is critical that PECA is periodically reviewed and updated in consultation with cyber security experts, legal scholars, and technology professionals to reflect emerging threats such as cryptocurrency scams, identity theft through AI-generated content, and phishing attacks via social media.

- **Introduction of Specific Provisions for Online Fraud:** While PECA criminalizes various acts related to cyber crime, it lacks detailed and specific provisions targeting different types of online fraud, including financial fraud, investment scams, and fraudulent online marketplaces. Clear definitions and penalties should be included in the legislation to close existing loopholes.

- **Establishment of Regulatory Oversight Mechanisms:** A dedicated cyber crime regulatory authority or oversight board should be constituted to monitor the implementation of cyber laws, ensure inter-agency coordination, and promote international cooperation in investigating cross-border cyber fraud cases.

- **Improved Data Protection and Privacy Laws:** Strengthening data privacy regulations is crucial, as many cyber frauds exploit poor data protection practices. Pakistan should enact comprehensive data protection legislation aligned with global standards such as the EU's GDPR, to protect citizens' sensitive information from misuse.

ii. Capacity Building and Training of FIA Officials

The effectiveness of FIA in investigating and preventing cyber crimes is directly dependent on the capability and expertise of its personnel. Several capacity-building initiatives are essential to improve institutional performance:

- **Specialized Training Programs:** FIA officials should undergo regular and specialized training in areas such as digital forensics, cyber law, ethical hacking, blockchain technology, and the use of artificial intelligence in cyber investigations. These training programs should be developed in collaboration with local universities, international law enforcement agencies, and private sector cyber security firms.

- **Expansion of Cyber Crime Units:** The current cyber crime units of the FIA are understaffed and overburdened. There is an urgent need to recruit more professionals with relevant backgrounds in information technology, computer science, and cyber law to meet the increasing volume and complexity of online fraud cases.

- **Investment in Technology and Infrastructure:** Upgrading the technical infrastructure of the FIA is imperative. This includes equipping cyber crime wings with state-of-the-art forensic labs, real-time monitoring systems, and secure databases for evidence collection and analysis.

- **Intra-Agency and Inter-Agency Coordination:** Stronger coordination among the FIA's cyber crime units across different regions, as well as with other relevant agencies such as the Pakistan Telecommunication Authority (PTA) and the State Bank of Pakistan, can lead to more effective investigations and timely responses to online fraud.

iii. Public Awareness and Digital Literacy

Public engagement and awareness are critical to the success of any cyber crime prevention strategy. Most online frauds succeed due to public ignorance of basic cyber hygiene practices. Therefore, the following steps are recommended:

- **National Awareness Campaigns:** The government, in collaboration with the FIA, media organizations, and educational institutions, should launch nationwide campaigns to educate the public about different types of cyber fraud, online safety protocols, and the process of reporting cyber crimes.

- **Incorporation into Educational Curriculum:** Cyber safety and digital literacy should be introduced at school and university levels as part of the regular curriculum. This will help inculcate responsible digital behavior from an early age and prepare future generations to navigate the online world safely.
- **Utilization of Social Media Platforms:** The FIA should use popular social media channels to disseminate educational content, alerts on emerging scams, and guidance on filing complaints. Engaging infographics, videos, and short tutorials can effectively reach a wider audience.
- **Engagement with Civil Society and Private Sector:** Partnering with NGOs, digital rights organizations, and private sector entities can enhance the reach and impact of awareness campaigns. These collaborations can also support victims of cyber fraud through counseling, legal aid, and recovery assistance.

7. Conclusion

The rapid proliferation of digital technologies has brought immense opportunities but also introduced significant vulnerabilities, particularly in the form of cyber crimes such as online fraud. In response, Pakistan enacted the Prevention of Electronic Crimes Act (PECA) in 2016 and designated the Federal Investigation Agency (FIA) as the primary law enforcement body to combat cyber crime. This study set out to analyze the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan, identifying the challenges faced by the agency and proposing key recommendations to improve outcomes.

i. Summary of Key Findings

The research reveals that while Pakistan has taken significant legislative steps through PECA and the establishment of FIA's Cyber Crime Wing (CCW), multiple gaps still undermine the overall effectiveness of these efforts. Firstly, it was found that the legal framework, though comprehensive in some areas, remains outdated and lacks the adaptability required to address the ever-evolving landscape of cyber crime. The definitions of certain cyber offences are ambiguous, enforcement mechanisms are weak, and penalties often fail to act as deterrents. Additionally, there is limited harmonization between national and international laws, impeding effective cross-border cooperation in cyber fraud investigations.

Secondly, the analysis of case studies and statistics reveals a concerning rise in online fraud incidents, particularly financial scams, identity theft, and phishing attacks. However, prosecution rates remain low. Delays in investigation, lack of technical evidence, procedural inefficiencies, and poor conviction rates are symptomatic of structural and resource-related deficiencies within the FIA. There are significant delays in responding to complaints, and victims often face hurdles in accessing justice due to bureaucratic red tape and

poor coordination among law enforcement agencies.
Thirdly, capacity constraints severely hinder the FIA's performance. The agency is grappling with a shortage of trained personnel, advanced forensic tools, and modern investigative techniques. Many FIA officials lack adequate training in digital forensics and cyber law, leading to ineffective investigation and poor presentation of digital evidence in court.
Fourth, the study identified low public awareness and digital literacy as a critical limitation. A large segment of the population remains unaware of cyber crime laws and preventive measures, making them vulnerable to scams. Moreover, many victims do not report cyber crimes either due to fear of stigma, mistrust in law enforcement, or lack of knowledge on how to lodge a complaint.

ii. Implications and Future Directions

The findings of this research carry important implications for policymakers, law enforcement agencies, legal practitioners, and the general public. It is evident that legislative reform is urgently needed to make cyber crime laws more dynamic, enforceable, and aligned with international best practices. Revisiting and amending PECA to clearly define offences, update penal provisions, and facilitate timely investigations can significantly enhance its utility in combating online fraud.
In terms of institutional capacity, there is a dire need for consistent investment in training and equipping FIA officials. Specialized cyber crime units should be established in each province with adequate funding, autonomy, and accountability. Moreover, modern surveillance tools, artificial intelligence-based analytics, and real-time tracking systems should be deployed to proactively detect and deter online fraud schemes.
The importance of inter-agency and international collaboration cannot be overstated. As cyber crimes often transcend national borders, the FIA must work closely with international cyber security organizations, financial institutions, and social media platforms to exchange information and develop coordinated responses to online fraud.
From a policy standpoint, the government should launch extensive awareness campaigns to educate the public about cyber risks, fraud tactics, and reporting mechanisms. Schools, universities, and community centers should be engaged in promoting cyber hygiene and responsible digital behavior.
In the long term, a holistic approach that incorporates legal, technical, educational, and administrative reforms is essential. The digital ecosystem must be strengthened not only through law enforcement but also through preventive strategies, including robust data protection laws, mandatory compliance for online platforms, and public-private partnerships for cyber security innovation.
In conclusion, while the FIA cyber crime laws and the establishment of the Cyber Crime Wing mark a foundational step in addressing

online fraud in Pakistan, their current effectiveness remains constrained by legal ambiguities, operational weaknesses, resource shortages, and low public engagement. If Pakistan aims to safeguard its digital future and protect its citizens from the rising tide of online fraud, it must act decisively to implement the recommendations outlined in this research. Only through comprehensive legal reform, institutional strengthening, and enhanced public awareness can the country hope to build a resilient and secure cyber landscape that effectively deters, detects, and prosecutes online fraud.

References

Azhar, S., Ahmad, W., & Tahir, M. (2025). AN EXPLORATORY ANALYSIS OF THE NEXUS BETWEEN CYBERCRIME AND NATIONAL SECURITY IN PAKISTAN: EVALUATING THE EXISTING LEGAL FRAMEWORK, INVESTIGATIVE CHALLENGES, AND PROPOSING A COMPREHENSIVE STRATEGY FOR EFFECTIVE CYBERCRIME PREVENTION AND PROSECUTION. *Journal for Current Sign*, *3*(2), 615–632.

Bukhari, M., Sattar, S., Saleem, S., Khan, K. Z., & KHAN, A. (2024a). The Impact of Cybercrime Incidents and Artificial Intelligence Adoption on Organizational Performance: A Mediatied Moderation Model. *Journal of Excellence in Social Sciences*, *3*(3), 191–210.

Bukhari, M., Sattar, S., Saleem, S., Khan, K. Z., & KHAN, A. (2024b). The Impact of Cybercrime Incidents and Artificial Intelligence Adoption on Organizational Performance: A Mediatied Moderation Model. *Journal of Excellence in Social Sciences*, *3*(3), 191–210.

Ch, S. N., Abbas, R., & Asghar, U. (2024). Socio-Economic Implications of Delayed Justice: An investigation in to the recent practices in Pakistan. *Pakistan Journal of Criminal Justice*, *4*(1), 121–133.

Faisal, S. M., Khan, N. T., & Ahmad, I. (2024). Challenges in Combating Cybercrime: A Comparative Study of Pakistani and International Legal Frameworks. *The Journal of Research Review*, *1*(04), 228–242.

Haque, E. U., & Abbasi, W. (2025). 15 A Jurisprudence for Pakistan's Digital Forensic Investigation Framework Regarding Cybersecurity. *Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics*, 160.

Iqbal, N., Siddiqui, H., Jumani, A., & Khan, T. A. (2025). A Comparative Study of Cyber Law in India and Pakistan: An Analysis of Legislative Frameworks and Enforcement Mechanisms. *JOURNAL OF LAW, SOCIAL AND MANAGEMENT SCIENCES*, *4*(1), 21–26.

Kaifa, U., Yaseen, Z., & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications. *Journal of Climate and Community Development*, *4*(1), 39–54.

Kanwel, S., Asghar, U., & Khan, M. I. (2024a). Beyond Punishment: Human Rights Perspectives on Crime Prevention. *Pakistan JL*

Analysis & Wisdom, *3*, 14.
Kanwel, S., Asghar, U., & Khan, M. I. (2024b). From Violation to Vindication: Human Rights in the Aftermath of Crime. *International Journal of Social Science Archives (IJSSA)*, *7*(2).
Kanwel, S., Khan, M. I., & Asghar, U. (n.d.). *Crimes and Consequences: A Human Rights-Based Approach to Criminal Justice*.
Kanwel, S., Khan, M. I., & Asghar, U. (2024a). HUMAN RIGHTS AT THE CROSSROADS: NAVIGATING CRIMINAL JUSTICE CHALLENGES. *PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences)*, *4*(01), 139–149.
Kanwel, S., Khan, M. I., & Asghar, U. (2024b). In the Shadow of Justice: Human Rights Implications of Criminal Acts. *Journal of Asian Development Studies*, *13*(1), 578–585.
Khan, H., Shabbir, S. S., & Qureshi, A. N. (2024). *Revamping Cybercrime Laws In Pakistan: A Comparative Analysis Of Pakistan And United Kingdom*.
Khan, I. A., Irshad, S., & Din, H. (n.d.). Cyber Harassment and Online Violence Against Women: A Critical Analysis of Women Protection Law Regime in Pakistan. *Journal of Law & Social Studies (JLSS)*, *7*(1), 12–25.
Malik, A. A., Azeem, W., & Asad, M. (2024). Online shopping, Cyber frauds and Fraud prevention Strategies. *International Journal for Electronic Crime Investigation*, *8*(1), 49–56.
Mukhtar, M., & Siddiqah, A. (2024). A Critical Analysis of Pakistan's Efforts to Counter Financial Crime (Corruption and Money Laundering) in its Territory. *Available at SSRN 5057327*.
Qasim, M. S., Ahmad, Z., Maqsood, S., Zafar, S., & Azam, M. (2025). ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS. *Kashf Journal of Multidisciplinary Research*, *2*(01), 115–125.
Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan. *The Critical Review of Social Sciences Studies*, *3*(1), 1052–1066.
Shabbir, N., & Adnan, M. (2025). Cyber Security: A Growing Challenge to Pakistan. *Annals of Human and Social Sciences*, *6*(1), 372–384.
Shaheen, M. B., Zahid, M., & Ahmad, Z. U. D. (2024). The intersection of technology and law: Challenges and opportunities in prosecuting cyberstalking cases in Australia and Pakistan. *Journal of Politics and International Studies*, *10*(1), 213–228.
Sharmeen, H. (2024). Mitigating White-Collar Crime in Emerging Economies: A Case Study of Law Enforcement Agencies in Pakistan. *International Journal of Applied Business and Management Studies*, *9*(1), 28–41.
Shoukat, D., Ayaz, M., Kanrani, A., Mansha, U., & Shah, U. (2025). Financial Crime Mediation in Pakistan: Legal Ambiguities, Global Trends, and the Restorative Justice Approach. *PAKISTAN JOURNAL OF LAW, ANALYSIS AND WISDOM*, *4*(6), 25–41.
Wajahat, J., Khan, A. N., & Ali, R. N. (2025). Cybercrime Legislation in

Pakistan: Effectiveness and Challenges. *The Journal of Research Review*, *2*(02), 506–514.
Zafar, S., Asghar, U., & Zaib, M. S. (2024). Exploring Crimes against Humanity and War Crimes: The Role of International Criminal Law in Addressing Atrocities. *The Journal of Research Review*, *1*(04), 185–197.
Zahid, M. A., Muhammad, A., Khakwani, M. A. K., & Maqbool, M. A. (2024). Cybercrime and Criminal Law in Pakistan: Societal Impact, Major Threats, and Legislative Responses. *Pakistan Journal of Criminal Justice*, *4*(1), 223–245.