Indus Journal of Social Sciences

Online ISSN: 2960-219X
Print ISSN: 2960-2203
Volume 3, Number 4, 2025, Pages 615 – 630
Journal Home Page
https://induspublishers.com/IJSS/about

Assessing the Efficacy of the Prevention of Cyber Crimes: A Critical Analysis of Cybercrime Growth and Responses by NCCIA in Pakistan

Muhammad Arif Saeed[1], Dr. Muhammad Hassan[2], Afif Raza[3]

[1]*Assistant Professor, Department of Law, The Islamia University of Bahawalpur, Pakistan, Email: arif.saeed@iub.edu.pk*
[2]*Lecturer, Department of Law, The Islamia University of Bahawalpur, Pakistan, Email: Muhammad.hassan@iub.edu.pk*
[3]*Department of Law, The Islamia University of Bahawalpur, Pakistan, Email: i.am.afifraza@gmail.com*

ARTICLE INFO

Article History:

Received:	*September*	*12, 2025*
Revised:	*October*	*17, 2025*
Accepted:	*October*	*25, 2025*
Available Online:	*November*	*10, 2025*

Keywords:

Cybercrime; NCCIA; PECA 2016; Pakistan; Cyber Law; Digital Security; Cybercrime Prevention

Corresponding Author:
Muhammad Arif Saeed
Email:
arif.saeed@iub.edu.pk

ABSTRACT

Increased digitalization of Pakistan has revolutionized the spheres of communication, banking, education, business, government and community interaction. The rising reliance on Internet-based platforms has also led to a rise in cybercrimes like internet fraud, phishing, hacking, identity theft, social media abuse, cyber harassment and blackmail, financial scams. The Government then introduced the Prevention of Electronic Crimes Act 2016 which lays the primary groundwork in Pakistan for the definition, investigation and prosecution of electronic crimes. The establishment of the National Cyber Crime Investigation Agency (NCCA) is also an important institutional action towards the rise in complexity of cybercrime. The adopted research methodology in this study is Secondary Qualitative Research which is doctrinal, descriptive, analytical and critical analysis of legal documents, policy report, scholarly articles, digital rights report and credible secondary sources. The findings are that despite the important legal and institutional constructs provided by PECA 2016 and the NCCIA, there are many areas in cybercrime prevention that still lack sufficient capacity, commission reception times, lack trained investigators, prosecutor hurdles, public awareness, and rights-based concerns. Strengthening NCCIA with technical resources, trained NCCIA staff, forensic laboratories, complaint mechanisms, public awareness campaigns, judicial capacity and training, rights approaches and accountability are recommended in the study.

Introduction

The digitization of technologies rapidly has altered the socio-economic and political system and the administrative system in modern societies. In Pakistan, letting go of paper has been empowering individuals with revolution in communication, financial services, education, business, public information, and public services! The massive popularity of smart phones, Internet, online banking and payment systems, online businesses, social media platforms and the numerous other digital payment methods have brought forth new possibilities for most people, all institutions and the national economy (Tennis, 2020). These have been contributing to the convenience, speed and connectivity of daily life. But the very same digital revolution has added a set of risks and vulnerabilities too. With increased citizens and enterprises relying on online platforms, the possibilities of cyber misuse, digital fraud, and access to private and institutional data have also gone up. Among the most serious non-traditional threats of security in Pakistan is Cybercrime, which has grown to become a serious threat in Pakistan these days. It covers various offences including online fraud, phishing, hacking, identity theft, cyber harassment, cyber blackmail, fake social media profiles, financial fraud, financial misuse of information systems and others (Schoenebeck et al., 2023). These crimes impact on individuals, businesses, banks, schools, government agencies and national security systems. Cybercrimes are transnational, often hidden and complex crimes, unlike traditional crimes. Offenders can be at different locations, use fake identities and technological means to target victims. In terms of detection, investigation and prosecution for traditional policing systems, it becomes trickier. Therefore, cybercrime needs highly qualified persons, trained cybercrime investigators, digital forensics know-how, proper police and legal practices, and institutional coordination.

In response to the ever-increasing threat of Cybercrime, Pakistan enacted the Prevention of Electronic Crimes Act 2016. The PECA sets the fundamental laws of the land to identify, regulate, investigate and prosecute electronic crimes in the country. Outlines various types of online crimes and provides a legal framework for investigation of such crimes. With the escalation of cybercrime, however, it has been established that legal measures are not enough (Plachta et al., 2024). In addition to the technical capabilities needed for effective cybercrime prevention, institutional capacity, public awareness, timely complaint handling, and successful prosecution are necessary for effective cybercrime prevention. Within this context, this national establishment known as National Cyber Crime Investigation Agency is a significant development in the cybercrime response mechanism in Pakistan. NCCIA is likely to offer a more focused platform for the investigation of cybercrimes, cyber evidence and online grievances, and for the prevention of cybercrime. While these laws and institutions are in place, there are still some issues hampering the functioning of cybercrime prevention in Pakistan. These include inabilities on how the complaints are processed, limited forensic skills, absence of skilled human resources, low public awareness, problems in the prosecution and apprehension and concerns about possible misuse of cyber laws (Nouh et al., 2019). It is important therefore that existing mechanisms are critically evaluated and the efficacy of their cybercrime control needs to be assessed. The study focuses on tackling the effectiveness of cybercrime prevention in Pakistan, analyzing the growth of cybercrime and the legal, institutional and operational response of NCCIA to a convincing degree. The study will try to find the main challenges and suggest possible recommendations on how to improve the framework of cybercrime prevention in Pakistan. In today's digital age, online banking, social media, e-commerce, and online communication are widespread throughout Pakistan, leading to a sharp surge in cybercrime. While Pakistan has rolled out various legal and institutional measures to address cybercrime, it has unfortunately continued to flourish in a myriad of different forms, including financial fraud, phishing, hacking, identity theft, cyber harassment,

blackmailing, fake profiles, and the misuse of social media (Nazir et al., 2025). It is evident that if cyber laws are in place on their own, but no timely institutional response, public awareness or technical capacity, it is sure that they are not going to do the job.

Prevention of Electronic Crimes Act 2016 has been introduced by the Government of Pakistan to deal with electronic crimes. Later, the office of the National Cyber Crime Investigation Agency was established with the aim to improve the capability of investigation and prevention of cybercrime with a dedicated institutional mechanism. But some of the hurdles faced in the effectiveness of cybercrime prevention in the country remain in the face of the case (Munir, 2025). The obstacles are registration and processing delays, low capacity in digital forensics, scarcity of trained cybercrime investigators, poor prosecution processes, lack of public awareness, and challenges related to processing and handling digital evidence. Often victims are also not aware of proper reporting procedures, and others do not trust because institutional responses are slow. Another issue of concern is the potential misuse of the Cybercrime Laws, especially where freedom of expression, privacy and political critique/criticism of the political are at stake. However, it is important to have a balance between digital security and fundamental rights for cybercrime prevention. The effectiveness of NCCIA should be critically evaluated as it is expected to be a central unit for handling complaints, investigation, collecting digital evidence, coordinating, and preventing (Muhib et al., 2025). In response to this issue the study concentrates upon the appropriateness of the legal, institutional and operational strategies of NCCIA in building a counter-movement against the rising cybercrime in Pakistan, in order to mitigate the threats on citizens cyberspace.

The sophistication of the cybercrime activities continuously raised the issue of how to address cybercrime as a complex issue of governance in Pakistan. Cybercrimes aren't confined to individual harassment or to minor online fraud anymore and are now aimed at organized financial fraud or identity abuse, data breaches, and tech savvy tactics of deception by spreading misinformation via coordinated attacks. The fluidity of the cybercrime landscape necessitates a legal, institutional, technical and rights-based response. The ability to follow digital imprints, work with digital platforms, victim protection and timely legal proceedings have been shown to be important factors for effective cybercrime control (Nouh et al., 2019). However, in Pakistan, the effectiveness of Cyber Crime Prevention is hampered by weak Digital Literacy, weak public trust and taking too long to raise a complaint against cybercriminal. The establishment of NCCIA marks an important institutional change, and its success will depend on the credibility it instills in cybercrime enforcement, given its shortcomings in the past. The agency should be assessed on whether it does an efficient job in responding to complaints, keeps electronic evidence, can do forensic investigations, assist prosecution and track its business with transparency. Any cybercrime enforcement should not interfere with democratic principles, like privacy, freedom of expression and due process. One of the problems that have been cited by scholars is that when the vague provisions come into use beyond their original scope and purpose of preventing the real harm of cyber, it may become problematic (Haq & Zarkoon, 2023). A balanced policy in line with that, must be applied so that the citizens are safeguarded from cybercrimes whilst at the same time cyber laws are not to be misused. The amount of cybercrime is a matter of concern in Pakistan and this study tries to contribute towards answering the question of whether NCCIA has been able to respond in law, institutional and operational way to the emerging information security issues of Pakistani society to the extent that cybercrime is a threat to the city. This study is very significant because it critically examines the growth of cybercrime and realizes whether NCCIA has responded to the cybercrime in law, institutional and operational manner to keep it away from Pakistani society or not to make information security in Pakistan a threat to the city.

Research Objectives

1. To examine the growth, patterns, and major forms of cybercrime in Pakistan in the context of increasing digitalization.
2. To critically analyze the legal and institutional framework for cybercrime prevention in Pakistan, particularly PECA 2016 and the role of NCCIA.
3. To evaluate the effectiveness of NCCIA's responses in cybercrime prevention, investigation, complaint handling, and enforcement, and to suggest policy recommendations for improvement.

Research Questions

1. What are the major forms and emerging trends of cybercrime in Pakistan?
2. How effective are PECA 2016 and NCCIA's institutional framework in addressing cybercrime prevention and investigation?
3. What legal, technical, and operational challenges limit NCCIA's effectiveness, and how can Pakistan improve its cybercrime prevention framework?

Literature Review

Cybercrime is defined as any crime that is enabled by the use of computers, digital networks, Internet-based platforms or any other electronic communication technologies. The cybercrime is not "hand to hand" in the same sense as traditional crimes, but contact is often not needed between offenders and victims. It may be done by Networks, Online Platforms, Mobile App, Digital Banking, social media, Websites, Emails and Information (Mishra et al, 2024). Cybercrime can include illegal use of a computer, stealing personal information, fraud using a computer, hacking, phishing, cyber harassment or cyberstalking, blackmail, financial crimes, cyber identity theft, and harmful online manipulation or uses. The key element of cybercrime is that it is technologically driven. Criminals exploit new technology, false identities, encrypted communications and online networks to criminalize, conceal their venue and be undetected. Another obstacle to cybercrime regulation is its trans-border nature (Masmoudi, 2025). The victim could be in one country and the offender in another jurisdiction. This makes an investigation, evidence gathering, prosecution and international involvement difficult. Digital evidence may be also sensitive in that it can easily be deleted, changed, or concealed within a brief period of the time. Thus, prevention of cybercrimes demands special legislation, experts, computer forensic tools, cooperation between police, judiciary, Internet service providers, banks and international organizations. Cybercrime in this context represents not just a legal challenge, but also a technological, institutional, social and security one (Malatji et al., 2020).

As Pakistan is fast embracing digitalization, cybercrime incidence is also rising in the country. The increasing access to the internet, use of smart phones, e-banking, shopping, social media, digital payments and electronic communications have opened new avenues of opportunity for citizens and businesses. But it's not without controversy, as these advances have come with digital misuse risks. New opportunities for cybercriminals to target users are becoming more common as increasing numbers of people use online services to communicate, shop, bank, go to the doctors, school, etc. (Mafarafara, 2025). Fraud associated with online activities, fake investment schemes, links to phishing pages, hacked account, fake profiles, misuse of identity, cyber harassment, and financial scams are all widespread issues in the country. The first and foremost focus that has led to the rise of Cybercrime in Pakistan is the lack of awareness regarding cyber security among the public. A lot of citizens are not aware of how to keep up their password, distinguish a fake link, validate an identity on the web or secure their banking data. As a result of this ignorance, individuals are at a

higher risk of being targeted by phishing or online fraud, as well as by blackmailing or social media scams. Likewise, in small businesses and individual businesses, the digital security practices are weak, which enhances the likelihood of hacking and data theft (Kuzior et al., 2024) (Kuzior et al., 2024). With mobile banking and digital wallets becoming a growing part of financial transactions, opportunities for cybercrime are also expanding, particularly as customers are not well-educated in basic online safety protocols. Social media is also an important factor responsible for the spread of cybercrime in Pakistan. Facebook, WhatsApp, Instagram, TikTok and X are some of the platforms that are nearly universally used in communication, business promotion, political discussion, and social interaction. But these venues are also used for false profiles, defaming people, harassing, blackmailing, hate speech, and propagating misleading information. People who are online users, young people, students and women in particular may be targeted more often for harassment and reputation damage on the internet. Hence, cybercrime is not just about monetary loss it also relates to damage on the aspect of privacy, dignity, mental health, public trust, institutional credibility, and even national security.

Prevention of Electronic Crimes Act 2016 has been promulgated in Pakistan to establish a legislative framework for dealing with that of the cybercrime. PECA 2016 classifies the various types of electronic crimes and sets out legal methods of investigation, prosecution and punishment in electronic crimes. It applies to offences like accessing information systems without authorization, tampering with information systems, interference with information systems, cyber terrorism, electronic fraud, identity-related offences, offences against dignity, offences against privacy, hate speech and uses for misuse of information and communication technologies (Khan & Ahmed, 2025). The intent behind the law would be to manage illegal Internet use and supply legal safety for the people, organizations, and the state. PECA 2016 is significant in that it signals that cybercrime is now codified as a legal problem and one that needs to be treated. Many cyber offences were not easily subject to offline criminal law enforcement prior to these types of laws. Cyber offences include technical evidence, digital communication, online identities, electronic records and information systems. Thus, it was a requirement to have a specially made law to establish crimes and procedures of investigation. PECA would offer a legal foundation to handle electronic evidence and would allow investigations into cyber offences (Johansen et al., 2025). In addition, literature shows that having a law does not automatically mean that it can be effective in the sense of being able to provide prevention. The legal provisions should be accompanied by adequate implementation, training, law enforcement personnel and electronic forensic expertise, plus judicial knowledge of electronic evidence. If complaints are not taken up timely, the investigators may not be technically trained or prosecution is not strong then the law may not fulfil its intent. However, while an important beginning, PECA 2016 relies on institutional capacity and actual implementation for effective results.

Cybercrime investigation is technically, complex, and constantly evolving, and thus, it takes special expertise and institutional capacities to deal with it. Policing practices are often inadequate for dealing with hacking, phishing, crimes of digital fraud, data theft, cyber harassment, and cyber offences in cross-border situations. They require well-trained cybercrime investigators, digital forensic labs, technical experts, up-to-date software tools, cyber intelligence systems and banks, telecom providers and Internet service providers, and social media platforms to be involved and coordinated. If this ability is not in place, the cybercrime complaints could be lost and the individual committing cybercrime could go unpunished (Jan, 2025). The National Cyber Crime Investigation Agency was established is a significant institutional development in Pakistan's efforts to combat cybercrime. Previously there was a lack of specialism in cybercrime prevention, investigation, evidence collection and complaints and this is where the introduction of NCCIA can

help. A focused, professional, technically competent and coordinated cybercrime agency will enhance focus and professionalism, technical investigation and institutional coordination. It is also meant to facilitate definition of procedures for complaints, speed up responses and facilitate prosecution through improved evidence collection. But several conditions are required for the success of NCCIA. This involves adequate financial funding, manpower skills in the region, digital forensic capabilities, public trust, complainant transparency, and accountability. The effectiveness of the agency might be constrained if citizens are also unaware of how to complain about cybercrime or there are delays in the complaint-processing. Likewise, without the tools and training, investigators will find it hard to track down offenders and maintain digital evidence. Hence, besides the legal mandate, the efficiency of NCCIA must also be assessed based on its operational efficiency and performance (Idrees et al., 2025).

While legislation is essential to combat the online kinds of criminal activity, scholars and rights groups have had concerns relating to the potential misuse of cyber legislation. A primary concern is when general or ambiguous legal clauses might apply to freedom of expression, private sphere, journalism or political dissent as well as social media activism. In democratic societies, the fight against cybercrime has to balance the need to shield citizens from harm on the Internet with their right to be free from interference by state and non-state actors with their online activities. Transparency, accountability and due process are required when implementing cyber laws, or else citizens will be afraid and lose faith in the state's institutions. Another major concern is privacy, as well (Haq & Zarkoon, 2023). Personal information, electronic devices, communications and the Internet accounts may be accessed during cybercrime investigations. Such powers should be utilized properly and within legal bounds. There is a need to be very cautious how investigation powers are used. Similarly, the importance of content regulation in cyber laws is balancing harmful online activities while not unduly restricting on legitimate expression. The report talks about the accountability, which is also relevant in institutional effectiveness. Effective legal protocols, oversight, and reporting must exist in all NCCIAs and other cybercrime institutions. Annual performance reports, tracking complaints, judicial reviews, and rights-based investigations can enhance the trust and chances of misuse being avoided (Chowdhury & Mostafa, 2024). Cyber-crime prevention has to be handled through a different lens and not a security lens alone, it should account for rule of law, transparency, safeguarding privacy and human rights. Existing literature showed mostly appeared on nature of cybercrime in Pakistan, introduction of PECA 2016 in Pakistan, cyber harassment, online fraud, legal issues in Pakistan and public awareness of cybercrime in Pakistan. The studies are somewhat meaningful due to the following reasons: they help to understand the nature of cybercrime and the strategies in which the legal system tries to tackle digital crimes. But there is a lack of critical investigation of the effectiveness of NCCIA as a special cybercrime investigation agency. The establishment of NCCIA is a significant institutional development in the cybercrime responses mechanisms in Pakistan and merits scholarly study (Basnayake et al., 2024). The institutional reform aspect also needs to be examined if it is having a positive impact on the prevention, complaints, investigations, prosecutions and public confidence around cybercrime. Existing literature suffers from a theoretical discussion of the law without an in-depth discussion of problems of implementation. Thus, this study differs in various aspects from the existing literature including the critical analysis of the trend of cybercrime in Pakistan and the assessment of the cybercrime responses of NCCIA in terms of legal, institutional and operational aspects. The study also identifies key challenges and policy recommendations that bring Pakistan a step closer towards the development of an effective cybercrime prevention framework.

There has been a communicative discourse in the literature that calls for an investigation of the cybercrime prevention framework both from an enforcement and a governance point of view.

Cybercrime regulation does not only focus on the punishment of cybercrime's perpetrators, but also on constitutionally secure regulation of freedoms, the protection of victims and procedural fairness and institutional trust. In fact, recent studies of PECA and its amendments have spurred a discussion of the impact of cybercrime regulation: new institutional structures have been established, but there have been concerns about excessive state control, less judicial oversight, and less available protection of civil liberties. The PECA Amendment 2025 brings about several significant adjustments to the country's digital governance, but along with it comes a set of risks to freedom of expression, privacy, due process, and digital democracy, says Zafar and Ali (2025). Law reforms therefore should be accompanied by laws that should help to ensure that the law is not misused and is not overreaching. In the same manner, Pakistan's Digital governance paradigm is in a pivoting position where a balance between digital security and digital freedom must be carried out (Idrees & Shahid, 2025). The report states that the original purpose of PECA, namely to address citizens' worries about cyber fraud, online harassment, and disinformation, has subsequently given rise to concerns regarding the vagueness of the definitions, the independence of the institutions, and accountability. These concerns are especially important given the nature of the NCCIA functioning as a legitimate body, both to be able to investigate cybercrimes and obviously to follow rights-based procedures. Thus, it was found that NCCIA needs to be evaluated outside its legally given duties, according to literature. It needs to be tested in terms of complaint handling, forensic capability, public accessibility, transparency, judicial supervision, privacy, and public trust. This study aims to fill this gap by critically examining NCCIA as a law enforcement body alongside as a rights sensitive cyber governance mechanism in Pakistan.

Methodology

The present study uses secondary qualitative research methodology to evaluate so far as cybercrime prevention is concerned, and to see how National Cyber Crime Investigation Agency in Pakistan is responding to cybercrime by concentrating on the efficacy measure of cybercrime prevention and the institutional response. A qualitative approach is used because they are trying to find out something other than numbers by survey or experiments. Rather, it is translated in terms of comprehension, analysis and evaluation of cybercrime prevention legal documents, policy structures, institutional liabilities, and literature (Al-Khater et al., 2020). The study examines the trend of cybercrime as a persistent digital menace in Pakistan and the legal and institutional frameworks in response to the rise of cybercrime. As this research is conducted on the documents that are already available and published materials, this research can be termed as Secondary Research Study.

Research Design

The research is a descriptive, doctrinal, analytical and critical research. Understands the nature, shapes and development of cybercrime in Pakistan and uses the descriptive design to explain it. Helps teach the basics of cybercrime such as the forms of internet fraud, phishing, hacking, identity theft, cyber-harassment, blackmail, financial fraud, and abuse of social media websites. The doctrinal design is employed because the research study involves analyzing legal sources, specifically the Prevention of Electronic Crimes Act 2016, amendments to the PECA and laws pertaining to investigation and prevention of cybercrime. This will assist in analyzing the legal controls which regulate cybercrime in Pakistan. To analyze the effectiveness of these legal and institutional tools in practice the analytical design is used. It is intended to enable the study to look at NCCIA's complaint handling and investigation, enforcement, collection of digital evidence and coordination with related institutions. A critical analysis of the study is important since the study not only describes existing laws and institutions but also analyzes their shortcomings. It pinpoints

shortcomings like slow nominations, insufficient forensic capabilities, slow handling of complaints, lack of officers trained to investigate CSEA complaints, inadequate prosecution, awareness deficit among the public, and apprehension concerns as to misuse of cyber laws.

Data Sources

The study purely involves secondary data sources. Legal documents, government notifications, official reports, policy documents, journal articles, digital rights reports and credible news sources are the main sources. The PEC Act 2016 is adopted as primary legislation with the main legal framework that defines cyber offences and investigation mechanism in Pakistan. Also, the PECA amendments are reviewed, to trace the changes in the institutional landscape and the existing legal framework for the functioning of NCCIA. Apart from that, the analysis on responsibilities of the institutions and developments in their operations is done from a selection of NCCIA and FIA-related reports, government publications and official notifications. To gain insight into the scholarly debates surrounding cybercrime, law enforcement response to cybercrime, cyber evidence, cyber harassment, cyber fraud, and institutional capacity, scholarly journal articles are included. Digital rights reports involve gauging concerns in connection with personal privacy and freedom of expression, misuse of cyber law, or liability. Where topic data, such as information on complaints against cybercrime, institutional reforms, or matters of general public concern are mentioned, they are relayed from credible news sources to give voice to the topic data, and to substantiate claims of the topic data. The topic data are also backed with credibility news sources for data that are official or recent, when such data are discussed, especially in matters of cybercrime complaints, institutional reform, and general public concern.

Data Analysis Method

The collected data will be analyzed by using content analysis and thematic analysis. Legal provisions, policy documents, official reports and institutional mandates will be analyzed under the rubric of content analysis. The study will undertake content analysis to evaluate the definitions of cyber offences in PECA 2016, powers accorded to cybercrime authorities and the approach to dealing with cybercrime cases by the NCCIA. It is helpful to learn and know the formal legal and formal framework on which cybercrime prevention is conducted in Pakistan. Thematic analysis will be applied to the documents or literature selected to identify the main themes and patterns which emerge within the text. Key themes are cybercrime growth, complaint method, investigations capability, digital forensic capability, legal enforcement, public awareness, prosecution challenges, institutional coordination, accountability, privacy concerns, policy gaps, etc. The themes will be used for organization of the discussion and to analyze the effectiveness of the response of the NCCIA to the growing problems in cybercrime. The thematic analysis method is appropriate because it provides means for the researcher to interpret the common theme found in studies among various sources of the research and relate it to the general scheme of the research.

Justification of Methodology

The methodology is suitable for the current study as a secondary objective of the current study is to determine the legal and institutional effectiveness, without collecting primary data on public opinion. This is where cybercrime growth is the focus and policy-level challenges, the NCCIA's institutional response, provide a solid foundation for critical evaluation, as indicated by secondary qualitative analysis. At this point no primary surveys or interviews are required, the study is largely based on legal texts, official documents, academic research, policy documents and digital rights reports. Doctrinal and analytical approach enables the study to explore the legal structure

and its applications (Ali et al., 2023). Content analysis can be used to assess the formal organising of cybercrime laws and institutional obligations, and thematic analysis to determine what the barriers and gaps in existing laws and institutional mandates are. Hence, this approach gives an overall picture whether the cybercrime prevention system of Pakistan, especially the NCCIA, can tackle the escalating threat of cybercrime or not. It further helps to formulate actionable solutions to enhance legal enforcement, institutional capacity, forensic capacity and legal awareness, accountability, and cybercrime governance in Pakistan.

Results

Theme 1: Cybercrime is Increasing Despite Legal Reforms

The reviewed literature also highlighted the fact that the rise of cybercrime is a major concern in Pakistan even after the enactment of legislation and institutional frameworks in the country. With the increasing popularity of social media, online payments, online banking and the Internet, there are more pathways available for cyber criminals to exploit. "***These are sad news as in the past few years there has been a significant surge in reported cybercrime cases in the country too***", say Sohail and Naz. This means that cybercrime is not a local or somewhat trivial problem, but rather a serious problem in the nation. The following report also outlines a correlation between the increased number of people on online platforms and increased attempts at cyber-attacks, identity theft and financial frauds (Digital Rights Foundation). 2024). According to it, the meeting of the parliamentary committee was indicative of the fact that cybercrime cases have increased by 83 per cent in three years. This discovery goes directly to the heart of that growth, and to the state's growth to keep up with it. The introduction of PECA 2016 and institutionality have been made in Pakistan, however, increasing incidence of cybercrime has proved that law alone is not enough to stop cybercrime. There are also reports in the literature that both individuals and institutions are targeted by cybercrime. The negative impacts of online fraud, phishing, hacking, cyber harassment, and financial scams on various aspects of personal privacy, mental health, business trust, and national digital security are quite clear (Ahmad & Afzal, 2025). Explain why online fraud is one of the most harmful forms of online crime impacting people, companies and governments. The first finding is that Pakistan's cybercrime issues are increasing as the adoption of digital is increasing at a higher rate than digital literacy, institutional capacity and awareness of prevention.

Theme 2: Weak Public Awareness and Reporting Barriers

The second big theme is the absence of general awareness about cybercrime, cyber rights, reporting mechanism and security measures to be taken on being online. According to the duo Sohail and Naz, although the cybercrime cell is doing its job, public awareness regarding "***cyber rights***" is still lacking. ***The finding is very relevant to the work of NCCIA, as it is essential that victims of cybercrime understand how to report crimes to a competent investigative agency and have an acceptable level of confidence in the reporting process***. The articles reveal that too often victims fail to report cybercrime because they are afraid, embarrassed, feel labeled, have no knowledge of their legal rights and don't trust staff members. Sohail and Naz say just 22 percent trusted FIA to safeguard their data, and 24 percent had reported a cybercrime incident to FIA. This suggests a significant level of mistrust among citizens and cybercrime institutions. If the victim does not trust cybercrime agencies with their data and/or confidentiality, reporting of incidents will be low and many offences will remain unreported (Bada & Nurse, 2021). Lack of awareness is also a big concern identified, as most people, particularly illiterate and rural communities are not aware of how the online scams occur, how they can be reported or how to act after an online scam

is identified (Government of Pakistan. 2016). This indicates it is not possible to restrict cybercrime prevention to an investigation post-offence. It calls for public education, digital literacy and awareness campaigns. What this means for NCCIA is that the effectiveness of their laws and policies rely not just on legal provisions but also on the readiness and capability of citizens to report cybercrimes.

Theme 3: NCCIA as a Positive Institutional Development

The third theme is that NCCIA is an institutional change in Pakistan's Cybercrime Response system. Previously, the issues related to cybercrime received very little attention from the Cyber Crime Wing of FIA and NR3C. The literature searched indicates that the reviewed older structure was encountered with the problems of workload, resource limitation and technical problems. Through the NCCIA Specialization in the 2025 amendment, the Agency has been established as a specialized investigation agency for cybercrime offences. The 2025 amendment includes "***new definitions, new offence, new regulatory authority, complaints council, tribunals and investigation agency***", the HRCP report notes. This is a sign that NCCIA is coming as the part of a wider restructuring of the cyber governance regime in Pakistan. Likewise, the NCHR report reveals that Section 29 has been amended and a mechanism for investigating and prosecuting the crimes, named the National Cyber Crime Investigation Agency (NCAI) has been created under PECA. This institutional change is important because in order for cybercrime to be addressed IT specialized skills and technical knowledge are needed, in addition to digital forensic capacities and coordinated investigation processes. Farrukh's analysis also provides insight into the transition from the old NR3C-based system to the new NCCIA-based system which contains a dedicated NCCIA helpline as well as a complaint portal. Thus, NCCIA can be regarded as a positive, and as it is aimed to establish a focused and specialized mechanism to prevent and investigate cybercrime. But literature also states that developing an agency without resources, trained personnel, transparency, accountability and public trust is not sufficient.

Theme 4: Operational Challenges in Complaint Handling and Investigation

The fourth theme is that there is still a significant gap in the area of operational weaknesses which hinder successful cybercrime prevention efforts. Many problems are repeatedly mentioned in the reviewed sources regarding delays, high caseloads, lack of trained staff, lack of forensic tools and lack of coordination and complaint tracking. In addressing these issues, Ahmad, Asghar, and Afzal report that the FIA encountered a number of limitations including scarce technical capacity, workload, admission delays, scope and authority issues, coordination and mistrust of victims. ***This theme is of particular interest to NCCIA and much of the earlier challenges may persist if the new agency is not adequately supported by capacity building efforts***. The same study notes that "Persistent under-resourcing, chronic backlogs, limited technical capacity and low public awareness continue to diminish its effectiveness". This reflects a reactive approach to cybercrime, instead of proactive. That is a comment suggesting cybercrime enforcement in Pakistan has been reactive rather than proactive. It also poses an operational challenge (Zafar & Ali, 2025). Trace amount of IP addresses, retrieve deleted data, examine mobile device, preserve metadata, and obtain data from social media or telecom firm. The archaic forensic labs, slow co-operation of telecom operators and global platforms makes it hard to process forensic evidences. Thus, the efficacy of NCCIA will require development of modern forensic facilities, recruiting Cyber experts, enhancing case management system and establishing good communication with banks, telecom companies, PTA and International platforms.

Theme 5: Legal and Prosecution Challenges

The fifth theme is focused on legal and prosecution obstacles. While PECA 2016 creates a legal framework for investigation of cybercrime, literature shows that it is difficult to implement it. They discovered that the legal framework is in place, but that there were numerous barriers such as delayed prosecutions, limited inter-agency co-ordination, challenges arising from jurisdiction, issues with collecting digital evidence and a lack of judicial capacity in order to strengthen the law's enforcement. ***This demonstrates that investigating and treating cybercrime cases is complicated and so is the successful prosecution***. Digital evidence should be collected, preserved and presented in accordance with the rules of law. When investigators are not technically competent to preserve the evidence as evidence, or the courts are not sufficiently aware of digital evidence and how to handle it, it is tricky to be convicted. The literature shows that there is need to have specially training for investigator, prosecutor and judges in criminal justice system (Farrukh, 2025). If any of these attributes is lacking, then cybercrime investigations can languish, be inadequately prosecuted, or be thrown out because of a shortage of evidence. It can be concluded from the document of PECA 2016 that the very purpose of enacting the law was to prevent any unauthorized use of information system and to create the mechanism to investigate, prosecute and try the crimes and to cooperate with other countries for coordinated action. The difference between what the law says and what is actually done is still evident. As such, procedural clarity, digital evidence laws, prosecution training, and even judicial specialization should complement NCCIA's role as a lawmaker.

Theme 6: Rights-Based Concerns and Misuse of Cyber Laws

The sixth theme is related to rights concerns on PECA and amendments to PECA 2025. There are multiple arguments which criticize cyber laws providing citizens with protection against harmful elements of the online world but not as a means of curbing freedom of expression, privacy or political criticism. ***Rights to Privacy, in their report, points out that PECA 2016 has been applied to opposing voices, journalists, political activists and even women who spoke out against harassment. 2025***. This is an indication of the dual nature of Cybercrime Law in Pakistan as it can help defend victims, but could also be used as a tool for assaulting citizens. The HRCP report also condemns the 2025 amendment because of its "ambiguous and over-broad language. It says "***false and fake information***" has been criminalized with penalties of up to three years imprisonment, and that there's no clear definition for "false" and "fake". This gives rise to the danger that the rather loose wording may be interpreted subjectively. The report also outlines the problem of mere intellectual discussions on issues of public officials and institutions, as public officials should be available for discussion and accountability (Sohail & Naz, 2023). The NCHR report even contends that Pakistan has become a territory of digital security and digital freedom and that laws that are meant to keep citizens safe and secure must not be created to silence them. It also raises the concern that the replacement of FIA's Cybercrime Wing by NCCIA does not in the process automatically fix the other discrepancies of lack of efficiency and privacy violations faced in earlier instances unless precautions are taken. The effectiveness of NCCIA should be measured beyond the number of arrests or complaints acted upon, to the extent it follows due process, respects privacy, and is not subject to selective enforcement.

Theme 7: Vulnerable Groups and Gendered Digital Harm

The seventh theme has to do with vulnerable groups, in particular, women, transgendered people, journalists and other marginalized groups. According to DRF's Cyber Harassment Helpline Report 2023, online female-targeted and gender-based violence is changing significantly and online

facilitates GBV is a critical issue. DRF also places great importance to the protection of the security and privacy of online users and their awareness, digital literacy and policy protection (Idrees & Shahid, 2025). The Digital Security Helpline Annual Report 2024 also reveals that on average, 264 new Cases were received through the helpline each month, with more such Cases including gendered disinformation and AI-generated images of women politicians or journalists. This "discovery" demonstrates that the cybercrime world is gearing up for a more technologically advanced and gendered attack. New technologies including generative AI can exacerbate the problem of online harassment, misinformation and reputational damage. Another problem identified in an intern with NCCIA is a lack of trans-inclusive practices, including taking transgender people's complaints seriously, which is demonstrated by evidence of trans-complainants facing ridicule or being misgendered or ignored by staff. So, it is important that NCCIA takes the effort to reinforce technical investigation and create complaint handling systems for victims that are gender-sensitive, inclusive and victim-centered.

Discussion

From the discussion of this study, it had been identified that enacting legislation to curb cybercrime in Pakistan is not sufficient as such. More than an institutional framework and a legal framework, the success of cybercrime control relies on the capacity, skill, trust, awareness and effectiveness of the judiciary, the capacity, skill, will or trust of operational agencies and the skill of public trust. A response must be up to date, specialized, and a dynamic phenomenon, in line with the cybercrime which is dynamic and technology driven. For this reason, NCCIA has significant influence and importance in the capable response of the cybercrime prevention mechanism in the face of the digital nature of cybercrime (Zafar & Ali, 2025). One key conclusion from the analysis is that the effectiveness of the NCCIA's institutional capacity relates directly to the effectiveness of cybercrime prevention. As cyber-crime becomes more prevalent, it can lead to phishing, hacking, identity theft, online fraud, cyber harassment and financial fraud, which demands specialised investigation skills that are different from the traditional policing techniques. Ali et al. (2023) stated that the principles of cybercrime investigation are tracing of digital footprints, recovering deleted data, identification of perpetrators on Internet, and preservation of electronic evidence. This is implying that normal investigation protocols are not adequate in technologically advanced offences. Thus, the success of NCCIA is critically dependent on the availability of cyber experts and investigators, forensic experts, data analysts, or legal-technical experts. The agency could be at risk of not investigating cases effectively if they lack these human resources and may not be able to stay one step ahead of fast-moving cyber threats.

There is also discussion about the need for Digital forensic infrastructure. The success of crime cases in the cybersphere mostly relies on the timely collection, preservation and analysis of electronic evidence. Provincial investigations may be delayed if forensic laboratories fall short of the needs of a province or are even lacking. Digital evidence is susceptible to being changed, "deleted," encrypted, and changed to another platform in a short amount of time. Hence, a modern forensic laboratory at the federal and provincial level is important in order to minimize the time to investigate and enhance the quality of evidence presented in court. A modernization of investigation apparatus, cyber intelligence software, secure data management systems and ongoing training of investigators would enhance efforts to identify offenders and develop solid cases. This is also indicative of the need to make cybercrime prevention a continuous capacity building process and not just a one-off institutional reform. Complaint handling is yet another crucial issue. The research reveals that victims' experience is suppressed if complaints about cyber offenses are not filed and acted upon in time, further undermining trust in law enforcement bodies. The study

indicates that the failure to register and process complaints regarding the cybercrime may lead to a loss of trust in the law enforcement institutions, because of the victims' experience. In circumstances of blackmailing, cyber harassment, any type of account hacking, online financial crime, or identification abuse, service providers might need to supply instant assistance to their victims. Complaints must be dealt with promptly, otherwise there can be escalation of damage and loss of digital evidence. Nazir et al. (2025) underscored the importance of an online complaint tracking system, where complainants will be able to keep track of their complaints. This would be a system that would render NCCIA more transparent and accountable. It would also alleviate suspicion of victims and confidence in reporting. The creation of helplines that are accessible on weekends, mobile complaint applications, fast response teams and regional cyber crimes offices would enhance the ease of access especially for women, students, elderly citizens and rural communities.

Awareness of the public is yet another fundamental part of cybercrime prevention. But many of the victims of cybercrime are not targeted due to the high level of hacking skills, but rather due to a lack of digital savvy and poor online practices. People fall for fake links, share passwords, more often respond to fraudulent messages, trust fake profiles and don't properly secure their online accounts. Mishra et al. (2024) emphasized the importance of raising awareness in the public regarding a variety of phishing, fake links, password protection, cyber harassment, identity theft, and safe reporting procedures to curb cyber victimization. This demonstrates that NCCIA cannot just be tasked with investigating crimes which have already taken place. It should also be in the process of preventive education. Awareness should be created within the universities, schools, banks, workplaces, Telecom network and social media platforms. Pakistan has various linguistic and educational backgrounds, so this awareness material should be created into Urdu and various regional languages to reach to a larger level. From the discussion, it is also apparent that the first two areas of weakness in cybercrime enforcement are on the prosecution side and judicial understanding which needs improvement. In many instances, investigations are not successful in identifying offenders, or in some cases, although an offender is identified, the prosecution fails to build a case, because the investigation of digital evidence has not been well conducted or judges are not aware of the cyber law and digital forensics. Specific technical knowledge is necessary for cyber-crime proceedings, including understanding of IP logs, metadata, digital signatures, device recovery, online logs of platforms and chain of custody. Kuzior et al. (2024) noted that avoidance of such non-standard procedures in collection, preservation and presentation of electronic evidence such as digital devices is an issue of concern. This is especially crucial because any evidence that is not properly collected cannot be believed in court. Thus, prosecutors and judges should be trained in the specific topic of PECA, as well as in cyber forensics, privacy law, digital evidence, and in international cybercrime cooperation. Specialized Cybercrime benches or trained Judicial officers could also enhance the quality and timeliness of the cases disposal.

Concerns with rights are also at the heart of the discussion. The use of cybercrime prevention should not be taken by any means as an excuse to infringe on constitutional rights, privacy, freedom of expression or due process. A cybercrime agency should safeguard the citizens against online harm and ensure that there is no abuse of their legal capacities against legitimate criticism, journalism, activism or everyone's expression. When people think that action is being taken selectively based on some criteria or unfairly against a specific segment of the population, public trust in NCCIA will drop. Thus, transparency, legality, proportionality and accountability must be the guiding principles of cybercrime enforcement (Al-Khater et al., 2020). Annual performance reports should be issued by NCCIA, with respect to the number of complaints received, complaints investigated, FIRs lodged, arrests made, prosecutions initiated, cases convicted, pending ones and

average time taken for the disposal of complaints. This kind of reporting will enable policy makers, researchers and the citizens to have a more objective idea about the effectiveness of the agency. It can be concluded that in general, the development of NCCIA can become an efficient cybercrime prevention institution, but it is dependent on practical implementation. Legal reform and establishment of institutions is key, but it is not enough without the availability of resources, training, forensic capacity, public awareness, effective complaint mechanisms, and judicial capacity. A one-dimension enforcement only strategy may not be sufficient as cybercrime is associated with social behavior, digital literacy, technological change, and institutions trust. Thus, developing an all-encompassing cybercrime prevention model which includes cybercrime investigation, prevention, education, prosecution, accountability, rights, is important for Pakistan.

The findings suggest that upon implementing the following characteristics, it is possible for NCCIA to enhance the cybercrime prevention mechanism of Pakistan: technical competence, transparency, accessibility and respect for rights. Qualities of protection of fundamental rights, rapid handling of complaints, supporting victims, and successful prosecutions should be viewed in addition to the number of arrests or registered situations. Digital security and democratic safeguards can be blended to better equip Pakistan to deal with cybercrimes without hurting the public confidence in the digital justice system.

Conclusion

With the advent of digitalization in Pakistan, Cybercrime has become a major threat to Pakistan. New opportunities for social and economic development have emerged with the growing adoption of Internet services, internet banking services, e-commerce, social media, digital communication and mobile technology. It has also broadened the scope of cyber offences like online fraud, phishing, hacking, misuse of digital platforms, identity theft, financial scams and cyber harassment or blackmailing. Because such crimes are technologically sophisticated in nature, fast-moving and often trans-border in nature, they are a crime of opportunity and are particularly difficult to detain through traditional policing methods. Pakistan is still in the process of legal and institutional measures to fight cybercrime which have largely been introduced through the Prevention of Electronic Crimes Act 2016 and subsequent amendments to the law, such as establishment of the National Cyber Crime Investigation Agency. PECA 2016 outlines the fundamental laws regarding of what is considered a cyber offence, how it is investigated, prosecuted and enforced. Likewise, NCCIA is a vital institutional move in a specialized cybercrime investigation and prevention community. It was created to address the need for a specialized entity to handle digital evidence, complaints against the internet, investigations and enforcement relating to cybercrime.

There are several obstacles that hinder the effectiveness of cybercrime prevention in Pakistan. Some of these problems are delays in complaint treatment, the lack of trained investigators, the poor forensic capacity, deficient public awareness, prosecution challenges, lack of judicial knowledge of the digital evidence, and privacy and freedom of expression issues. The results reveal that there is a lack of practical implementation, institutional capacity, and trust in the legal reforms to curb cybercrime, if they are to be employed without such support. NCCIA can only be effective if it has adequate means for it, modern forensic laboratories, trained personnel, transparent complaint resolution processes and accountability mechanisms. Cybercrime enforcement, in turn, should demonstrate a respect for rights and respect for the citizens, while safeguarding citizens from harm online in a manner that does not abuse the cyber laws against legitimate expression. To solidify cybercrime prevention in Pakistan, a law and technology-driven regime with public awareness and judicial training, transparency, and rights-based obligations is crucial.

References

1. Ahmad, W., Asghar, U., & Afzal, M. (2025). *An analysis of the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan: Challenges and recommendations*. Research Consortium Archive, 3(2), 836–850.
2. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, *27*(3), 945-958.
3. Ali, B., Salam, A., & Ali, W. (2023). Digital Pakistan Policy: A Document Of Words Or Plans For Implementation, A Critical Analysis. *Pakistan Journal of Social Research*, *5*(01), 627-635.
4. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE access*, *8*, 137293-137311.
5. Bada, M., & Nurse, J. R. C. (2021). *Profiling the cybercriminal: A systematic review of research*. University of Cambridge and University of Kent.
6. Baig, K., & Jafary, H. A. (2025). Cyber harassment and online violence against women in Pakistan: Legal gaps and enforcement challenges. *Journal of Political Stability Archive*, *3*(4), 900-916.
7. Basnayake, D., Naranpanawa, A., Selvanathan, S., & Bandara, J. S. (2024). Financial inclusion through digitalization and economic growth in Asia-Pacific countries. *International Review of Financial Analysis*, *96*, 103596.
8. Chowdhury, R. H., & Mostafa, A. (2024). Digital forensics and business management: The role of digital forensics in investigating cybercrimes affecting digital businesses. *World Journal of Advanced Research and Reviews*, *23*(2), 1060-1069.
9. Digital Rights Foundation. (2024). *Cyber Harassment Helpline Report 2023*. Digital Rights Foundation.
10. Digital Rights Foundation. (2025). *Digital Security Helpline Annual Report 2024*. Digital Rights Foundation.
11. Farrukh, T. (2025). A Critical Analysis of the Prevention of Electronic Crimes Act (PECA): Legislative Gaps and Enforcement Challenges in Pakistan. *Pakistan Journal of Social Science Review*, *4*(4), 1439-1448.
12. Government of Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016*. National Assembly of Pakistan.
13. Haq, I. U., & Zarkoon, S. M. (2023). Cyber stalking: A critical analysis of prevention of electronic crimes Act-2016 and its effectiveness in combating cyber crimes, A perspective from Pakistan. *Pakistan's Multidisciplinary Journal for Arts & Science*, 43-62.
14. Human Rights Commission of Pakistan. (2025). *Prevention of Electronic Crimes (Amendment) Act 2025*. HRCP Legislation Watch Cell Report.
15. Idrees, R. Q., Hussain, N., & Shahid, A. (2025). Cybercrime Laws in Pakistan: A Critical Analysis of the Prevention of Electronic Crimes Act, 2016. *Journal for Current Sign*, *3*(4), 2390-2403.
16. Jan, A. (2025). Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials. *ASSAJ*, *4*(02), 914-920.
17. Johansen, K. L., Gilbertson, D. T., Li, S., Li, S., Liu, J., Roetker, N. S., ... & Wetmore, J. B. (2025). US Renal Data System 2024 annual data report: epidemiology of kidney disease in the United States. *American Journal of Kidney Diseases*, *85*(6), A8-A11.

18. Khan, M. N. I., & Ahmed, I. (2025). A systematic review of judicial reforms and legal access strategies in the age of cybercrime and digital evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01-29.
19. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies (2071-8330)*, *17*(2).
20. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies (2071-8330)*, *17*(2).
21. Mafarafara, N. G. (2025). SAAHIP Presidential Annual Report 2024/2025. *SA Pharmaceutical Journal*, *92*(1), 44-48.
22. Malatji, M., Marnewick, A. L., & von Solms, S. (2020). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability*, *13*(1), 291.
23. Masmoudi, S. (2025). Unveiling the human factor in cybercrime and cybersecurity: Motivations, behaviors, vulnerabilities, mitigation strategies, and research methods. In *Cybercrime unveiled: Technologies for analysing legal complexity* (pp. 41-91). Cham: Springer Nature Switzerland.
24. Mishra, S., Singh, P. K., & Ojha, J. S. (2024). Reporting Cybercrime: A Bird's Eye View of the Procedural Framework. In *Cybersecurity, Law, and Economics* (pp. 123-133). Routledge.
25. Muhib, M., Muhib, K., & Muhib, Z. (2025). Pakistan's Cyber Laws and International Legal Standards on Digital Rights. *Policy Journal of Social Science Review*, *3*(3), 151-165.
26. Munir, A. (2025). Cybercrime Laws and Digital Privacy in Pakistan. *Available at SSRN 5950694*.
27. Idrees, R. Q., Hussain, N., & Shahid, A. (2025). Cybercrime Laws in Pakistan: A Critical Analysis of the Prevention of Electronic Crimes Act, 2016. *Journal for Current Sign*, *3*(4), 2390-2403.
28. Nazir, S., Asif, M., & Khan, A. U. A. (2025). Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials: https://doi. org/10.55966/assaj. 2025.4. 1.0107. *ASSAJ*, *4*(01), 1941-1951.
29. Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *arXiv preprint arXiv:1902.06961*.
30. Plachta, M., Hong, E., & Wahl, A. (2024). Transnational Organized Crime and Economic Integration. *IELR*, *40*, 416.
31. Schoenebeck, S., Batool, A., Do, G., Darling, S., Grill, G., Wilkinson, D., ... & Ashwell, L. (2023, April). Online harassment in majority contexts: Examining harms and remedies across countries. In *Proceedings of the 2023 CHI conference on human factors in computing systems* (pp. 1-16).
32. Sohail, S. A., & Naz, F. (2023). Response and reporting of cybercrimes in Pakistan: Mass media as a mean of awareness, prevention, and protection. *Journal of Social Sciences and Media Studies*, *7*(2), 70–76.
33. Tennis, M. M. (2020). A United Nations convention on cybercrime. *Cap. UL Rev.*, *48*, 189.
34. Zafar, P., & Ali, S. (2025). *The PECA Amendment 2025: A critical analysis*.