SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 3, 2026

CYBERCRIME AND LAW ENFORCEMENT: CHALLENGES & PROSPECTS

Dr. Muhammad Iqbal[*1], Dr. Fatimah Qadir[2], Muhammad Shahid Ashraf[3]

[*1]*PhD Law District and Sessions Judge*
[2]*PhD Management Assistant Professor (Adjunct Faculty) University of Chakwal, Punjab, Pakistan*
[3]*Advocate High Court LLM, University of Lahore*

[*1]c.muhammadiqbal@gmail.com, [2]fatimah19.qadir@gmail.com, [3]shahidashraf4047@gmail.com

DOI: https://doi.org/10.5281/zenodo.21989642

Keywords
Cybercrime, Law Enforcement, Pakistan, Prevention of Electronic Crimes Act, Digital Forensics, Cybersecurity, Digital Evidence, Artificial Intelligence, Cybercrime Investigation, Fundamental Rights, International Cooperation, Data Protection.

Article History
Received: 01 January 2026
Accepted: 16 March 2026
Published: 31 March 2026

Corresponding Author: *
Dr. Muhammad Iqbal

Abstract
Cybercrime has become a fast-growing challenge for law enforcement systems, especially in the context of the growing presence of cyber technology, financial services, social media, artificial intelligence, and cryptocurrencies in everyday social and economic activity. The article throws light on the key issues and opportunities in cybercrime law enforcement in Pakistan, highlighting the legal, institutional, technological, evidentiary, and constitutional dimensions of the problem. It discusses the history of cybercrime and Pakistan's legal efforts, including the Prevention of Electronic Crimes Act 2000 and the institutional changes brought in by the amended amendments in 2025. Investigation and digital forensics, electronic evidence, prosecution, adjudication, privacy and fundamental rights in the cybercrime justice process are discussed. Emphasis is placed on issues such as encryption, anonymization, cross-border crime, inadequate technical resources, institutional complexities, under-reporting, evidentiary problems, and delays in prosecution. The article also looks at international collaboration and new risks linked to AI, deepfakes, ransomware, criminal activity involving cryptocurrencies, and mass data breaches. It believes there is a need for more than legislation to control cybercrime effectively. Technically competent institutions, specialized investigators and prosecutors, judicial skills, robust digital forensic capabilities, inter-agency coordination, international cooperation, robust legal frameworks, robust data protection, and privacy and freedom of expression protection are all essential to sustainable enforcement. The article concludes that Pakistan's future cybercrime strategy should focus on a rights-based, technologically informed, victim-centered, and integrated approach.

INTRODUCTION

One of the more significant changes in the history of crime in the modern era is the way crime has been transformed by digital technology. Offences that used to be geographically and physically limited and had to be coordinated by humans can be planned, executed, and hidden across borders in seconds in many cases by an individual who never enters the jurisdiction where harm is done (Stoykova, 2021). No longer does it take the forger's hand to commit fraud; no longer does it require the burglar's foot to make entry to commit theft; no longer does it take the presence and proximity of a harasser to commit harassment. What has been the result is a borderless, technically mediated, evidentially fragile, and

continually evolving criminal landscape, ranging from the early days of hacking and computer viruses to today's ransomware gangs, frauds leveraging cryptocurrency, and artificial intelligence deception (Munir, 2025). This change is not simply the creation of a new class of crime in the traditional criminal code; rather, it undermines the fundamental assumptions underlying traditional law enforcement, investigation, prosecution, and adjudication (Borah & Borthakur, 2021).

To effectively fight cybercrime, more than just a law criminalizing unauthorized access or internet fraud is required. Whether investigators have the technical skills needed to locate an anonymized offender; whether digital evidence can be collected, preserved and authenticated in a way that is acceptable to the court; whether the prosecution and judicial bodies have the technical expertise to assess digital evidence; whether the functions of different institutions can be coordinated across overlapping mandates; and whether all of this can be done without compromising privacy and expressive freedoms that a constitutional order is supposed to safeguard (Selvarajah & Mailvagnam, 2021). The precursor must be legislation, but it is at best a remedy for a technological, institutional, and constitutional problem. This is clearly seen in Pakistan. In the last 10 years, the country has seen a fast increase in internet usage, mobile financial services, and social media usage, and with it, the amount of cyber-enabled fraud, harassment, data breaches, and online extortion. The state's key statute, the Prevention of Electronic Crimes Act, is itself the subject of ongoing debate and criticism, undergoing changes and challenges to its legality in the courts over the years. This experience is therefore not only relevant because cybercrime is a serious and growing issue in Pakistan but also because it provides an unusual degree of visibility of the institutional and political space that can become available between a nation's avowed stance to overcome digital crime and its institutional and political powers to do so in a manner consistent with due process and fundamental rights (Subair et al., 2022).

This article builds on a key premise that the effectiveness of cybercrime control in any jurisdiction and in Pakistan in particular is not just hinged on the availability of legislation but a broader spectrum of elements: investigative capacity, digital forensic capacity, institutional coordination, prosecutorial and judicial competence, international cooperation, and the protection of fundamental rights (Sumadinata, 2023). If one of these elements is lacking, whatever may be in the statute book on paper, the overall system underperforms. The discussion that follows charts the history of cybercrime and Pakistan's legal efforts to address it, reviews how cybercrime gets through the criminal justice system (from investigation to evidence to adjudication), examines the major challenges faced by law enforcement, puts Pakistan's experience in the context of international cooperation, and finally offers a realistic evaluation of how to reform. The analysis in this paper differentiates between the law as written, the institutions that are responsible for its enforcement, the actual process of enforcement, and the actual experience of the victims as a result of the law a distinction that is crucial to understanding why legal reform on its own seldom achieves the results that it promises (Nawawi et al., 2023).

Evolution of Cybercrime and the Legal Framework in Pakistan

1.1 Evolution and Emerging Forms of Cybercrime

Cybercrime was not a fully formed type of crime, but rather it developed in a gradual manner along with the technologies it uses. The initial type of computer crime was limited to unauthorized access to computer systems, modification of relatively simple data, and the proliferation of self-replicating viruses, with the goal of being either curious, notorious, or destructive in nature and not for the purpose of monetary gain (Nawawi et al., 2023). With the proliferation of networked computing, e-commerce and mobile banking, the incentive had fully turned to making money, and the sophistication of the offender followed suit. Hacking morphed into a tactic of exploiting systems in organized, and sometimes tolerated or

state-sponsored, campaigns to attack critical systems. Financial crime evolved from basic card skimming to sophisticated phishing attacks, BEC and SIM swap attacks. Loan fraud and impersonation extortion were just a few of the crimes that have been spawning from identity theft (Choi et al., 2024).

In addition to financially motivated crime, another type of interpersonal cyber harm has emerged as a growing issue, particularly impacting women and younger users, as well as nonconsensual sharing of intimate images and prolonged online harassment, which may not be captured by systems of law enforcement that are traditionally focused on property crime (Shah, 2024). Data breaches are now a fundamental part of the digital economy, threatening to put personal and financial information at risk on a scale that is beyond the reach of individual victims to monitor and remedy. Ransomware is now a full-fledged criminal business model, with affiliate networks, extortion negotiation processes, and, in many cases, money laundering operations across the border, using cryptocurrency. Two more recent developments warrant special mention as they are transforming the front lines of harm brought about by cyber technologies (Mouheb, 2024). The first relates to the criminal use of AI, which has reduced the technical hurdles in creating realistic phishing content, automated social engineering attacks, and created synthetic audio and video (deepfakes) of real people for fraud, extortion, or reputational damage. The latter is the rise of cryptocurrencies as an asset and as a tool for crime, which allows criminals to transfer funds internationally with some level of anonymity to make it harder to trace and retrieve assets. All these developments are part of the same trend: cybercrime is an ever-changing and evolving type of offense which is always ahead of the law and institutions that are trying to prevent it (Bartoli, 2025).

1.2 Development of Cybercrime Legislation in Pakistan

The cybercrime framework of Pakistan is a relatively new one. Cyber-related offences were previously dealt with, in a limited way, under the Electronic Transactions Ordinance 2002, which was enacted to promote electronic commerce and not to discourage cyber offending (Hakmeh, 2025). The substantive legislation came with the Prevention of Electronic Crimes Act, which was enacted on 11 August 2016 and commenced shortly after, as part of the government's overall National Action Plan against terrorism, and also due to the lack of an adequate framework to address the rapid development of digital technologies and use of the internet. PECA laid the foundation of Pakistan's stance, which is criminalization of unauthorized access to and interference with information systems and data, electronic fraud and forgery, cyberterrorism, cyberstalking, hate speech, and unauthorized interception, as well as providing a mechanism to enable the telecommunications regulator to block unlawful content on the Internet and mandating that cybercrime cases be heard by judges who have received training in electronic evidence and cyber forensics (Spiezia, 2022).

It is a statute that deals with many real kinds of harm competently on its own terms and has provisions at its own level that are so broad and vague as to routinely be the subject of judicial and civil society contestation especially in the content section, where the breadth and vagueness of provisions such as those governing false and offensive content and those relating to reputation harm have repeatedly drawn criticism. It is still unclear whether this framework will be able to meet the rapidly changing technological challenges of AI fueled fraud and deepfakes, as successive amendments have focused disproportionately on speech based crimes, over technical and evidentiary provisions most relevant to tackling financially and technologically advanced crime (Birzhanov et al., 2023).

1.3 Institutional Framework for Cybercrime Law Enforcement

The Federal Investigation Agency (FIA) had overseen the investigations of offences under PECA for almost a decade and had a dedicated Cybercrime Wing. The amendments in 2025 changed this scenario completely by establishing a National Cybercrime Investigation Agency which

was granted exclusive statutory powers to investigate and prosecute the offences under the Act and removing the FIA as the investigation agency, and introducing the National Cybercrime Investigation Agency for inquiry, investigation and prosecution under PECA.

In addition to the NCCIA, there are provincial police forces, which also have jurisdiction over some matters related to PECA offences; the Pakistan Telecommunication Authority that still has content blocking powers; and the ordinary courts, which historically had jurisdiction over PECA offences, and, under the Act, must have judges with cyber forensics and electronic evidence expertise; and, following amendments in 2025, a new tier of adjudicatory tribunals, the Social Media Protection and Regulatory Authority and the Social Media Protection Tribunals, which sit alongside the ordinary courts for some categories of content related offences. While specialized bodies, in principle, can add valuable technical expertise to a complex issue, this institutional multiplication is not itself problematic, it can create real risks of jurisdictional overlaps and lack of accountability between the NCCIA, provincial police, the telecommunications regulator and the new social media authority, and duplicated or competing processes for the same underlying conduct. The implications for practice, which are explored more fully below, is that institutional changes to improve enforcement capacity have produced more coordination issues than solutions as they are implemented to date (Mouheb, 2024).

Cybercrime Investigation, Digital Evidence and Criminal Justice

1.4 Investigation and Detection of Cybercrime

The nature of the detection and investigation of cybercrime is very different from that of traditional crime offences as the crime scene is often spread across several jurisdictions, service providers and technical layers and the perpetrator is, by definition, hidden. Investigation starts with reporting (complaints are a means by which the victim can bring the incident to the attention of the investigating agency) and moves to digital forensic techniques used to reconstruct the events that led to the incident from server logs, metadata, network traffic and device artifacts. Investigators need to be able to work with Internet service providers and platform operators to obtain information about subscribers and connections, track down IP addresses and digital footprints which offenders often try to hide with VPRs, proxy servers and anonymizing tools and if the offender is in another jurisdiction to initiate a process of cross border cooperation that is often slow in comparison to the rate at which digital evidence becomes degraded or deleted. The impact of this change on the capacity to investigate will depend significantly on the level of institutional knowledge, personnel, and forensic infrastructure that is transferred during the changeover (Zhang & Gong, 2023).

1.5 Digital Evidence and Its Admissibility

Digital evidence is in a special place, and in a very fragile position, in cybercrime prosecutions. Digital evidence can be manipulated, copied, and destroyed without leaving behind easily detectable evidence, and the value of the evidence is dependent upon the integrity of the process in which it was collected, preserved, and authenticated. Having a defensible chain of custody (CHOC), which is a documented, unbroken chain of evidence ownership, handling, and conditions, is critical for resisting a challenge in court and the ability to authenticate electronic records and metadata evidence in a way that a court can review and not just take on the investigating agency's word. Pakistan's evidentiary regime has been adapted in the light of electronic records and digital signatures by making amendments to the Qanun e Shahadat Order, and the provisions of PECA have also been framed regarding preservation and production of data. However, there are still many practical issues to be overcome (Sunardi & Kusuma, 2023).

1.6 Prosecution and Adjudication of Cybercrime

Investigations are followed by a new set of institutional requirements at the prosecution and adjudication phase in cybercrime cases. Prosecutors need to make technically complex

information, like server logs, forensic imaging reports, and blockchain transaction logs, accessible to a court, and be ready to face and refute technical objections to this information (Kasuri et al., 2024). This demands certain specialized skills which are not generally acquired by general Criminal prosecutors in Pakistan, as in many countries of the world. PECA's initial concept was to tackle the adjudicatory aspect of the issue by appointing cyber forensics-trained judges of the Court of Session to handle cybercrime cases. The amendments added a new chapter creating Social Media Protection Tribunals, which are composed of a member with a legal background, a member with a journalistic background, and a member with an information technology background, to hear appeals from decisions of the new social media regulatory authority, an adjudicatory mechanism that was added onto this system, which is structurally unusual (Dunsin et al., 2023).

This structural change is a tacit admission that the traditional judicial system might not be well suited to handling today's high-speed content battles, but it also leaves some room for doubt as to the consistency of the tribunals, the precedent they set, and how the tribunals relate to the traditional appellate system. In general, cybercrime prosecutions in Pakistan continue to have the same problems as always: long duration of proceedings, increasing backlogs of cybercrime cases which increase at a much faster rate than the number of cases that can be adjudicated, and a lack of detail and publicly available information on case outcomes that makes it difficult to precisely measure conviction rates. These delays have a direct impact on the victim, in that the sense of a meaningful and timely remedy through the justice system is reduced (Tok & Chattopadhyay, 2022).

1.7 Privacy, Fundamental Rights and Due Process

The conflict between the effective implementation of cybercrime laws and the rights of fundamental freedoms is not an incidental part of the Pakistani experience, as the most fraught aspect of the legal system since its inception, but has become much more pronounced since the amendments made in 2025. The Constitution of Pakistan, Article 14, has established the dignity of the individual, which includes the right to privacy, and Article 19 guarantees freedom of speech and expression as long as it is reasonable (Tok & Chattopadhyay, 2022). The challenge is to make these pledges into enforceable restrictions on investigative and regulatory activity in the digital realm, where it is possible to monitor, search electronic devices, and remove content on a scale and speed that are hard to imagine in the physical world. This oversight has not sufficiently deterred the state from adopting such laws in the first place (Mahmood et al., 2025).

1.8 Institutional Coordination and Criminal Justice

Chain Coordinated action throughout the criminal justice chain is an important, but little discussed, aspect of cybercrime enforcement. Cybercrime investigation does not happen in isolation, working only for an investigating officer. An ongoing relationship between complainant, investigator, forensic examiner, prosecutor, service provider, and financial institution/court is needed. Any failure at any of the steps can destroy the effectiveness of the process (Kasuri et al., 2024). An investigator, for instance, can be able to trace an IP address that is suspicious, but if the service provider fails to keep such records for an adequate time, then the information may be lost. In the same way, forensic investigators may be able to get valuable information from the device, but if they do not follow the appropriate documentation and chain-of-custody, the value of that information becomes compromised. This can be a major issue when it comes to online financial scams. These investigations could necessitate a collaboration among cybercrime investigators, banks, mobile financial service providers, telecommunications and cryptocurrency service providers. Funds can transfer in and out of multiple accounts and via various digital means in a span of just a few seconds (Mahmood et al., 2025).

Thus, traditional investigative methods, which tend to be time-consuming and involve a series of requests and correspondence, could not always be

responsive to the pace of financial crime that is made possible by cyberspace. Yet another issue is the technical expert's involvement with the lawyer. Digital forensic experts may be aware of how a specific piece of evidence was acquired but it will be the prosecution and judge's task to decide if the evidence is legally relevant, reliable, and substantial enough to prove a crime. Technical evidence must then be "formulated" in a way that is legally comprehensible while maintaining the technical accuracy of the evidence. Requires regular communication between the investigators, forensic experts, and prosecutors, not just after an investigation has been completed (Gomez et al., 2023).

The establishment of specialized cybercrime institutions will augment these efforts to coordinate the fight against cybercrime, but institutional specialization is not sufficient to make enforcement more effective. Have clear protocols for responsibility for taking a complaint and requests for preservation, forensic examination, prosecution, and referral to other agencies. In the absence of such protocols, specialization can lead to institutional fragmentation, instead of efficiency (Dunsin et al., 2023). Additionally, there is a need for improved documentation of the cases of cybercrime and case resolution. Complaints, investigations, prosecutions, convictions and acquittals data are still publicly available and needed to gauge the effectiveness of cybercrime laws. Accurate figures would enable policymakers to determine which crimes are growing and where police failures are, and which offenses target which type of victim. In this way, any successful action against cybercrime has to be considered as a whole criminal justice process and not just the capability to register and investigate a complaint with the relevant agency (Tok & Chattopadhyay, 2022).

Major Challenges Facing Cybercrime Law Enforcement in Pakistan

1.9 Technological and Investigative Challenge

The cybercrime agencies are facing the same technological challenges as any law enforcement agency around the world, but Pakistan's agencies often lack adequate resources. Whilst necessary for privacy and security, encryption and anonymization tools also provide protection for criminals who can easily be identified and anonymized marketplaces on the dark web enable the trading of stolen data, malware and other illegal goods in a way that is largely outside the abilities of conventional policing methods (Mouheb, 2024). AI tools have made it easier than ever to create deep-fake images and videos for fraud or extortion and to carry out successful phishing attacks, while ransomware demands are increasingly being made in cryptocurrency, making it harder to attribute and recover assets. The traditional policing approach, based on physical evidence, witness evidence, and local jurisdiction, simply cannot deal with such offenses, and the introduction of a dedicated, technically specialized investigation agency (NCCIA) recognizes this. One of the biggest unanswered questions in Pakistan's cybercrime enforcement scene is whether that agency is capable of developing its own capacity in forensic skills and technical expertise in a timely manner to meet these threats, especially as it transitions through its own processes (Shoaib et al., 2023).

1.10 Legal and Jurisdictional Challenges

There is considerable ambiguity and overlap in the legal structure that has made it difficult for Pakistani investigators to obtain the evidence and streamlined mutual assistance mechanisms that the convention offers, and has also been a cause of trouble in getting evidence from major foreign technology platforms: Pakistan has not entered into a mutual legal assistance agreement with the United States on cyber offences, and the Federal Investigation Agency has reported significant difficulties in obtaining data from alleged cybercriminals located in the United States, even after the convention was ratified, without such a treaty. Although Pakistan has a general mutual legal assistance statute since 2020, it still lacks the dedicated, fast-track cooperation tools that are offered by a cybercrime-specific statute (Vasoya et al., 2022).

1.11 Institutional and Capacity Constraints

Bottlenecks in institutional capacity are present at all stages in the cybercrime enforcement system in Pakistan. Specialized investigators with the technical expertise and skills necessary to perform digital forensic investigations are currently underutilized; the same applies to prosecutors who are technically competent to prosecute technically complex cases and judges who have been trained to have such cases heard (Sanna et al., 2025). These existing shortages are further exacerbated in the short term by the 2025 restructuring, which involves recruitment, training and investment in infrastructure The inter-agency coordination, provincial police and the telecoms and social media regulators is still evolving as an effective practice and coordination issues can lead to cases falling between the cracks or being repeated between agencies with overlapping mandates (Wilson-Kovacs et al., 2023).

1.12 Public Awareness, Victim Reporting and Enforcement Gaps

A rarely discussed but significant obstacle to effective cybercrime control is the gap between cyber harms that occur and those formally reported to authorities. Victims of online fraud, harassment, or non-consensual disclosure often do not report incidents because they are unaware of reporting mechanisms, do not know how to preserve evidence, fear social stigma, or doubt that reporting will lead to a meaningful outcome given delays and limited resources, especially where non-consensual images or videos are involved (Stoykova, 2021). This underreporting is worsened, rather than reduced, when the law is applied in ways that undermine public confidence. As discussed in Section 3.4, a statute intended to protect citizens from online harm has also been used against journalists, activists, and ordinary internet users to suppress content considered objectionable by authorities. Reports of PECA cases involving a citizen's video of a private wedding illustrate how enforcement can diverge sharply from the law's protective purpose. Building trust therefore requires more than awareness campaigns and accessible reporting systems; it requires a consistent record of investigating and prosecuting genuine cyber offences, not only cases that are politically convenient for the state (Shoaib et al., 2023).

1.13 Data Protection, Privacy and Technological Dependency

Another hurdle for cybercrime legal professionals in Pakistan is that they do not have an adequate personal data protection and management framework. A cybercrime investigation requires access to massive amounts of information that include communications, account information, location information, financial data, and information on electronic devices. The ability to access this information can be essential for investigations, but when access to this information is not controlled or regulated, there will be risks to privacy and individual rights (Mouheb, 2024). The challenge is especially acute because the same technology used to find criminal activities can be leveraged to enable extensive surveillance. This should be coupled with transparent legal protection for accessing information from telecommunications entities, social media and digital service providers. Powers of investigators should be well defined, and people should be well protected against arbitrary searches, unnecessary collection and misuse of personal information. Another problem is the reliance on foreign Tech giants and on foreign Digital Infrastructure in Pakistan. Much of the information that is needed for cybercrime investigations is outside of Pakistan. Companies in other jurisdictions may be involved, such as social media accounts, cloud services, email accounts, and payment platforms (Shoaib et al., 2023).

Cybercrime therefore requires continuous training of its officers more than ever in most other fields of policing. Also, the uneven access to resources among the major urban centers and smaller cities poses another challenge to enforcement. Cybercrime victims aren't just confined to the more technologically advanced metros, but large metros are more likely to have specialized forensic facilities and trained personnel (Vasoya et al., 2022). This results in an unevenness in access to justice. A victim in a smaller city might have more trouble reporting an

offence, keeping evidence and getting any kind of investigative help. Changing the number of investigators is not enough to overcome these challenges. A more comprehensive institutional approach, which involves technical training, establishing independent forensic capacity, several privacy protection measures, data protection, and better cooperation with technology firms and fair access to cybercrime reporting and investigation, is needed for Pakistan. Technology can only be a means of criminal justice if it is integrated in such a way that it doesn't create a problem for enforcement (Stoykova, 2021).

International Cooperation and Emerging Dimensions of Cybercrime

As an offence of structure, cybercrime is often a crime that crosses national boundaries, and no national legislation, however robustly drafted, can overcome an offence which has offenders and victims spread across multiple jurisdictions and an infrastructure that is international in nature. This requires cross-border investigation, prompt information sharing between law enforcement authorities, cooperation in the collection and exchange of evidence and, if it is required, extradition (Spiezia, 2022). The most developed multilateral instrument that has responded to these requirements is the Budapest Convention, which provides a uniform criminalization framework and a uniform procedural authority for signatories, and provides a 24-hour network of immediate mutual assistance requests. Since Pakistan continues to remain a non-member of the international community, the country is forced to rely on a set of bilateral deals and its own statute of 2020 on mutual legal assistance, which works but is not as speedy as dedicated cybercrime cooperation mechanisms and is less predictable (Hakmeh, 2025; Raza et al., 2025).

The actual "frontier" of cybercrime is continually evolving, as well as the institutional question of cooperation. Existing laws, designed to protect against older forms of deception, are just starting to recognize the harm that artificial intelligence generated fraud and deepfakes can cause and are doing so in a way that is poorly adapted to their new capabilities for creating believable fake audio and video at scale the risks range from financial fraud to disinformation to reputational destruction, and Pakistan's legal framework, like most elsewhere, has yet to include provisions specifically tailored to that new type of harm (Smith et al., 2021). The other interesting issue relates to cryptocurrency-related offenses, as the regulatory landscape for cryptocurrencies in Pakistan continues to be unsteady, and the anonymous and cross-border nature of cryptocurrency transactions makes it difficult to trace back to underlying crimes and recover any profits. The sophistication of the threat is growing much faster than most countries, including Pakistan, can keep up with, with ransomware, cyberterrorism aimed at government and critical infrastructure systems, and large-scale data breaches all playing a role (Eurojust, 2022a). Realistic lessons from comparative experience include the fact that those jurisdictions that have focused from the outset on building specialization and dedicated capacity in digital forensics, and have established clear data protection regimes, tend to be better equipped to meet the new threat than those that have cobbled together a legislative order largely on an ad hoc basis. One of the major omissions in Pakistan's current legal order, as discussed below, is a clear data protection regime (Eurojust, 2022b).

Prospects for Strengthening Cybercrime Law Enforcement in Pakistan

The need to build up Pakistan's cybercrime enforcement regime is more than just passing a law every now and again to make a new type of act illegal or to impose new fines. Addressing the precise wording of legislation, the capacity of institutions, technical infrastructure, judicial competences, international relations and rights protection all needs to take place hand in hand, for weakness in one area will ensure that the progress made in any other remains limited. Precise, not expansive, is the most pressing need on the legislative front (Mahmood et al., 2025). The language, in particular the false information offence and the "aspersion" concept that was introduced in 2025, would be better served with more narrowly drawn and clearly defined

provisions that would exclude legitimate criticism, satire and investigative journalism from the definition of false information (Munir et al., 2024). But this is not just a question of the protection of freedom of expression, important as that is; it is also a question of institutional credibility, because a law that is seen as used for political control and not as a tool for victim protection will continue to suffer from underreporting and a lack of public trust, as discussed in Section 4.4. PECA's criminal provisions represent an important and much needed complement, as of May 2026 Pakistan has no comprehensive, enacted personal data protection law, and the PECA 2016 is a criminal bill that fails to provide a general framework of principles for how organizations should collect, process, store and share personal data, and there is no requirement for organizations to notify the data subjects of a breach, nor a data subject rights framework, nor a dedicated data protection authority in place, to address a large class of data harms that is better suited to be addressed by a data protection statute (Shah, 2024).

For the institutions, the transition period holds potential for risk and opportunity with the NCCIA. The opportunity will be realized through a continuous investment in the recruitment and training of technically competent investigators; expansion of forensic laboratory facilities beyond the major urban centers; and the establishment of published, clear protocols for how the NCCIA, provincial police, the telecommunications regulator and the social media authority will work together, rather than in parallel, to avoid jurisdictional overlaps and gaps in action (Stoykova, 2024). The unprecedented mix of legal, journalistic and technical qualifications at the new Social Media Protection Tribunals may provide a useful model for addressing rapid digital disputes, if it is established with proper procedural protections and a clear connection to the normal appellate court system, rather than as a parallel system with its own fuzzy guidelines and uncertain authority (Choi et al., 2024).

Pakistan has a real dilemma in engaging with cybercrime cooperation treaties on the international stage. As the Budapest Convention and its alternative continue to develop, Pakistani investigators will continue to be structurally disadvantaged by not participating in the Convention and the new Convention alternative, a disadvantage which is not going to be fully compensated for by capacity building efforts at the national level, because many serious cybercrimes are inherently transnational in nature (Europol, 2024). A more practical strategy might be to focus on more limited and negotiated mutual legal assistance deals with key technology host jurisdictions in the short term and to consider accession to a broader multilateral instrument as domestic data protection and rights protections evolve and become robust enough to resolve sovereignty and privacy concerns that have thus far stifled participation (Dunsin et al., 2023).

Most importantly, sustainable progress must build public confidence in the ability of the law against cybercrime to protect. That involves investing in well-publicized reporting mechanisms, meaningful, victim-centric follow-through after a complaint has been made rather than sitting in procedural limbo, and showing by consistent practice with regard to implementation of the legislation that it targets real cases of fraud, harassment and exploitation and not political or journalistic expression (Wilson-Kovacs et al., 2023). It calls for effective institutions, technically sound investigation, strong evidence-based prosecution, judicially adept adjudication, effective international cooperation, and a long-term approach to upholding constitutional rights, all of which function together, consistently, over time. Pakistan's recent history over the last decade has shown the dangers of a fragmented approach to cybercrime control, and the ongoing realistic prospect of moving towards an integrated approach, if future reforms are not based on rights-centered drafting and institutional capacity-building but instead are reactive, politically charged, and driven by amendments (International Telecommunication, 2024).

Conclusion

Cybercrime has radically transformed the definition of crime and also made it difficult for traditional policing frameworks to deal with this.

Pakistan has seen that the presence of criminal law is a crucial element, but it is not enough for effective prevention, investigation, prosecution, and adjudication of cybercrime (Munir, 2024). The evolution of the Prevention of Electronic Crimes Act (PECA) and the institutional changes, on the one hand, are testament to the state's ongoing efforts to address new threats in the electronic space, while on the other, they raise serious issues about institutional capacity, jurisdictional coordination, digital evidence, technical expertise, procedural safeguards, and fundamental rights. The creation of specialized institutions like the NCCIA presents a chance to boost cybercrime investigation with specialized expertise and forensic capacities. But it would require continued investments in personnel, infrastructure, training, judicial capacity, prosecutorial capacity, and in working with other relevant institutions. Likewise, enhanced international cooperation and more effective arrangements to obtain cross-border digital evidence will be critical to Pakistan's efforts to combat ever more transnational cybercrime. Future reforms should thus go beyond a piecemeal approach of legislative changes and move towards a comprehensive rights-based approach. Ambiguous legal definitions, inadequate data protection, unreliable digital forensic processes, insufficient training for judicial and prosecutorial officials, victim reporting processes, and meaningful safeguards for privacy and freedom of expression are key. In practice, the enforcement of cybercrime needs security and rights to balance. The only way to bolster public trust in the justice system against cybercrime in Pakistan is for enforcement to significantly mitigate real-world harms that can be committed by cybercriminals while protecting legitimate expression from being infringed upon by this legislation.

REFERENCES

Ardian, Y., Juhana, U., & Kusumah, H. A. (2023). Law Enforcement Problems Against Cybercrime Performed Through Phishing Method. *Rechtsnormen: Journal of Law*, *1*. https://doi.org/10.55849/rjl.v1i3.435

Bartoli, L. (2025). Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*.

Birzhanov, B., Sakenova, A., Abeuov, A., Birzhanov, K., Sopyhanova, A., & Talapova, A. (2023). Electronic Proves as One of the Modern Independent Means of Evidence. *Journal of Law and Sustainable Development*, *11*, e1805. https://doi.org/10.55908/sdgs.v11i10.1805

Borah, U., & Borthakur, U. (2021). Cybercrime and Preservation of Digital Evidence in Criminal Trials. *International Journal of Legal Science and Innovation*, *3*, 289-301.

Choi, S., Dearden, T., & Parti, K. (2024). Understanding the Use of Artificial Intelligence in Cybercrime. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*. https://doi.org/10.52306/2578-3289.1185

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2023). A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. *Artificial Intelligence Review*.

Eurojust. (2022a). *Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence*.

Eurojust. (2022b). *Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence*.

European Union Agency for Criminal Justice, C. (2025). *International cooperation against cybercrime*.

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*.

Gomez, G., van Liebergen, K., & Caballero, J. (2023). Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage. *arXiv*.

Guo, Z. (2023). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Hakmeh, J. (2025). The UN convention on cybercrime: a milestone in cybercrime cooperation? *Journal of Cyber Policy*, 125-130. https://doi.org/10.1080/23738871.2024.2441549

International Telecommunication, U. (2024). *Global Cybersecurity Index 2024*.

Kasuri, M. R., Abbas, S., & Mahmood, T. (2024). Adversarial and inquisitorial; two rival models of criminal procedure and theory of convergence: an appraisal. *Journal of Law Social Studies (JLSS)*, *6*, 73-84.

Munir, B. (2025). *Artificial intelligence for lawyers: Navigating novel methods and practices for the future of law*.

Mahmood, T., Rasool, F. G., & Samee, H. (2025). Technological innovations in criminal justice: The role of cybersecurity in crime detection, investigation and prevention. *Journal of Asian Development Studies*, *14*, 1579-1593.

Munir, B. (2024, December 31). Artificial intelligence and legal decision-making in the USA and Pakistan: A critical appreciation of regulatory frameworks. *Global Foreign Policies Review*, *48–58*.

Mouheb, H. (2024). Artificial intelligence, an accelerator of cybercrime: Understanding the complicit role of artificial intelligence in cybercrime. *Question(s) de management*, *49*, 93-98. https://doi.org/10.3917/qdm.229.0093

Munir, B., Ansari, A. A., & Mahmood, T. (2024). Judicial Activism in Pakistan and its Impacts on Tripartite Governance: Lessons from the US Constitutional Construct. *Global Political Review*, *9*, 44-57.

Nawawi, J., Darmawati, D., Tajuddin, M. A., & Nutakor, B. S. M. (2023). The Law Enforcement Related to Cybercrime by Involving the Role of the Cyber Patrol Society in Achieving Justice. *Jurnal IUS Kajian Hukum dan Keadilan*, *11*, 437-447. https://doi.org/10.29303/ius.v11i3.1289

Raza, A., Munir, B., & Khan, A. N. (2025). National security, artificial intelligence, and sovereignty beyond Earth: Reconstructing the legal architecture of space intelligence networks. *Global Foreign Policies Review, 8*(3), 29–37. Humanity Publications.

Sanna, S. L., Regano, L., Maiorca, D., & Giacinto, G. (2025). Improving Cybercrime Detection and Digital Forensics Investigations with Artificial Intelligence. *arXiv*.

Selvarajah, V., & Mailvagnam, J. (2021). A framework for handling digital forensic evidence and evaluation on cyber resilience. *Journal of Applied Technology and Innovation*, *5*. https://doi.org/10.65136/jati.v5i1.238

Shah, S. K. A. (2024). A Critical Analysis of Efficacy of the Prevention of Electronic Crimes Act, 2016: Irritants and Remedies. *Journal of Pakistan Administration*, *45*, 66-91.

Shoaib, M. R., Wang, Z., Ahvanooey, M. T., & Zhao, J. (2023). Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models. *arXiv*.

Smith, S., Torres, P., Mitchell, J., & Greene, R. (2021). Cybercrime and International Legal Cooperation. *Journal of International Commercial Law and Technology*, *2*, 22-25.

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum*, *23*, 101-108. https://doi.org/10.1007/s12027-022-00707-8

Stoykova, R. (2021). Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence. *Computer Law & Security Review*, *42*, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Stoykova, R. (2023). The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Stoykova, R. (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, *55*, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability Assessment of Digital Forensic Investigations in the Norwegian Police. *Forensic Science International: Digital Investigation*, *40*, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Subair, S., Yosif, D., Ahmed, A., & Thron, C. (2022). Cybercrime Forensics. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *1*, 41-49. https://doi.org/10.54938/ijemdcsai.2022.01.1.37

Sumadinata, W. S. (2023). Cybercrime and Global Security Threats: A Challenge in International Law. *Russian Law Journal*, *11*, 438-444. https://doi.org/10.52783/rlj.v11i3.1112

Sunardi, & Kusuma, R. S. (2023). Digital Evidence Security System Design Using Blockchain Technology. *International Journal of Safety and Security Engineering*, *13*, 159-165. https://doi.org/10.18280/ijsse.130118

Tok, Y. C., & Chattopadhyay, S. (2022). Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling. *arXiv*.

Vasoya, S., Bhavsar, K., & Patel, N. (2022). A systematic literature review on Ransomware attacks. *arXiv*.

Wilson-Kovacs, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. *International Journal of Evidence & Proof*.

Zhang, H., & Gong, X. (2023). The research on an electronic evidence forensic system for cross-border cybercrime. *International Journal of Evidence & Proof*.