



Challenges Faced by the Judiciary in Implementing Cybersecurity Laws in Pakistan

Hafiz Abdul Rehman Saleem¹, Ali Bukhtiar², Babar Zaheer³ & Muhammad Asad Ullah Farooq⁴

¹Department of Law, University of Sahiwal, Sahiwal, Pakistan, Email: h.a.rehman@hotmail.com

²Department of Law, University of Sahiwal, Sahiwal, Pakistan, Email: alibukhtiar61@gmail.com

³Department of Law, University of Sahiwal, Sahiwal, Pakistan, Email: babarzaheerkhan@gmail.com

⁴Department of Law, University of Sahiwal, Sahiwal, Pakistan, Email: mianasadfarooq876@gmail.com

ARTICLE INFO

Article History:

Received: December 21, 2024
Revised: January 19, 2025
Accepted: January 24, 2025
Available: January 26, 2025
Online:

Keywords:

Cybersecurity, Cybercrime, Judiciary, Legal framework, Law enforcement

Corresponding Author:

Hafiz Abdul Rehman Saleem

Email:

h.a.rehman@hotmail.com



ABSTRACT

Due to the inherent growth of technological elements, today's world of governance, commerce, and societies has been revolutionized, opening new vistas of opportunity as well as new horizons of cyber security threats. Fraud such as hacking, identity theft, and ransom ware are important threats that are knowledgeable about to personal and business associations and the government. In Pakistan, law enforcement agencies and the judiciary are overwhelmed with inadequate resources lack of training, and technical knowledge. However, the institutions operating in the country still face legislative gaps and enforcement challenges even after the passing of the Prevention of Electronic Crimes Act (PECA) 2016 means. The paper deals with Pakistan's situation concerning cyber security enhancement judicial practices and legislation and compares it to the United States' strategic enhancement in the security domain. There are some leading projects like the National Judicial Automation Program and e-Courts, but still, it seems there are a lot more systems problems and no significant digital forensics available in the judiciary of Pakistan. The comparative analysis indicates that Pakistan needs to reform its laws, train its judges specialized in cybercrime and look for international cooperation when it comes to fighting transnational criminals engaged in cybercrimes. The importance of increasing the level of protection in cyberspace is highlighted by raising public awareness or engaging private structures. This research stresses the need to mitigate cyber security threats through legal, organizational, and social change. From best practices and international collaboration so that Pakistan can better address the issue, increase the capacity of its judicial system in combating cyber threats, and protect its critical IT assets. The actual findings of the research include ways to improve the efficiency of Courts, protect digital rights, and strengthen the governance of cyber security in the country.

Introduction

Considering the present-day world as a global village where technological advancement becomes important to the world, cyber security has become a critical structural pillar to the existing and emerging systems of governance, commerce, and societies. This occurrence in society is driven by technology. It presents exciting opportunities, but it also presents its likes for the first time. Vulnerabilities such as hacking, identity theft, and ransom system attacks¹ have been and are being experienced by individuals, businesses, and governments worldwide. Indeed, for countries like Pakistan, there are two significant hurdles to protecting the country from cyber threats: modifying threats and slow-moving judicial systems. The annual cost of cybercrime will likely increase to \$15.63 trillion in the year 2029 from the year 2024, with a 69.41% increment. The Cyber security market in Pakistan is projected to grow by 10.21% (2024-2029), resulting in a market volume of US\$263.10m in 2029. Among all the major threats, ransom ware has taken center stage and is responsible for 70% of cyber attacks worldwide. More incredibly shocking is that it has impacted essential industries like manufacturing, finance, and insurance industries that form the backbone of global economic stability.(Science & Eriotis, 2024) These statistics worsen the problem of cyber security in all countries and confirm the need for the development of proper legal and institutional provisions.

There are many gaps in Pakistan's cyber security architecture through which risks could be brought directly to individuals or institutions. A relatively young population with internet usage between 10% and 16% is efficient in Internet banking, social networks, and online shopping. However, problems are encountered systematically, as evidenced by recent attempts to introduce legislation, including the Prevention of Electronic Crimes Act (PECA) 2016.² These challenges are attributed to poor substantive knowledge of the judiciary, weak facilities, and minimal understanding of cyberspace risks. That is why the judiciary of Pakistan often lacks adequate ability to handle the increasing number and severity of cybercrime-related cases. Cybercrime in Pakistan includes different offenses such as computer hacking, identity theft, cyber stalking and cyber fraud. These crimes take advantage of technological flaws, and there are existing gaps in the law. For instance, inadequate academic qualification or training of the judicial officers may significantly limit the general handling of cybercrime. Furthermore, the currently low levels of knowledge among the population allow criminals to act without serious consequences and make it increasingly difficult to investigate the crime scenes and convict the offender.(Mofokeng & Aphane, 2022)

In the global community, enhanced awareness and, specifically, spending on cyber security have become essential in preventing these risks. About 40 percent of Internet users now know what 'ransom ware' is, indicating increasing awareness of information technology risks. Global corporations have adjusted by shifting focus to cyber security; the security budget grew by 5.7% year on year in 2024. However, statistics suggest that Pakistan is still far from being prepared, and more public and private sector reforms are required for judicial systems initiatives, education, and infrastructure improvements. Comparing its cyber security with that of more developed countries

¹ Ransom ware is a prevalent and hazardous form of malicious software. It prevents you from accessing your files by encrypting or locking them. A ransom is demanded to get the files back, typically in the form of crypto currency. Cybercriminals might also demand a ransom to prevent data and intellectual property from being leaked or sold online.

² The Prevention of Electronic Crimes Act 2016 is a federal law in Pakistan. Any act carried out outside of Pakistan by anyone who violates this Act and impacts a person, piece of property, information system, or data located in Pakistan is also covered by the Act.

like the United States of America is promising for study. Strong legislation from the USA, like the Cyber security Information Sharing Act³ and specialized judicial training privileges, has strengthened the nation against cyber criminals. This paper reveals that real-time threat intelligence, the involvement of private and public sectors, and specially defined legal measures have empowered the United States in the face of such threats. On the other hand, Pakistan faces two significant constraints: fewer resources to invest in media development and the rapid transformation of digital media. The lesson from the USA's experience can help Pakistan learn how to practically reform its cyber security system and improve the efficiency and effectiveness of the judiciary system.

The following work aims to present the complexity of cybersecurity and the judiciary in Pakistan, focusing on the systematic impediments to progress. Given this, the *Literature Review* will extensively describe the existing laws and judicial practices of cybersecurity in Pakistan and establish appropriate recommendations for lacunae. The *Research Methodology* section explains the adopted qualitative and comparative analysis method of legislative and institutional provisions. The following sections will consist of the *Current Role of the Judiciary in Cybersecurity*, the Challenges faced by the judiciary and a comparison with the United States. Lastly, the recommendations section will outline recommendations as to how the cybersecurity landscape of Pakistan could be reformed and the judiciary's challenges mitigated. Due to the increased complexity and prevalence of cyber threats, legal and judicial flexibility in the Pakistani context makes or breaks the nation's prospects in defending its digital evolution. Pakistan can embark upon a course to improve its current cybersecurity risk exposure, fill the existing gaps in cybersecurity frameworks and policy, encourage partnerships with private sectors, and refer to the experiences of other countries. This research seeks to add to the existing literature on cybersecurity and aims to offer information that can assist policymakers and judicial stakeholders in this intricate and rapidly evolving subject.

Literature Review

The issue of cyber security has become one of the biggest problems for Pakistan in the context of the era that is affiliated with the use of information technologies. Recent technological developments have added to the country's cyber framework and, at the same time, created loopholes. Hansen (2009) has stated cybersecurity threats as a global issue as it has become evident that most economic, political, and even social activities rely primarily on ICT. As Pakistan's internet usage has gradually increased from 6.3% in 2005 to 17.8% in 2016, the country has become more vulnerable to cyber-attacks (ITU, 2017). While some legislation has been enacted recently, such as the Prevention of Electronic Crimes Act (PECA) 2016, Pakistan still lacks a strong cybersecurity framework. Some critics claim that PECA fails to address cyber threats appropriately by considering organized cybercrime, terrorism, and hacking. For instance, many banks in one of the most sensitive regions came under cyber-attack in 2018, with data from thousands of accounts being an issue (Dawn, 2018).

³ The Cybersecurity Information Sharing Act (CISA) is a federal law in the United States to enhance cyber security because it enables private organizations to share cyber threat indicators and information on defensive measures to agencies of the government, and in return, the companies are protected legally; it is a platform where organizations come together to fight cyber threats.

Shad (2019) adds that there is state-sponsored cyber warfare that adds to insecurity in Pakistan's cyberspace. Similarly, next door, India actively uses cyber capabilities for strategic and military threats under the Cold Start Doctrine⁴, which always poses a constant threat to Pakistan's key infrastructure. Moreover, the functions of terrorists reflect cyberspace utilization as a means of propaganda, recruitment, and work planning. He also pointed out that Singapore and the United States have high rankings at the cybersecurity readiness level, stating that they have a common integrated framework of institutions and sufficient PPP⁵. On the Global Cybersecurity Index, Pakistan stands at 66, which proves the chances of technical, organizational, and collaborative openings. Therefore, to meet the challenges, Pakistan has to bolster the legal mechanisms, cooperation between agencies, and important capacity-building programs. Education initiatives aimed at increasing the general population's understanding of cyber threats are particularly useful for raising defenses against cyber dangers. Such efforts are essential as Pakistan struggles to deal with a digital-age world.

New business models prompted by digitalization in Pakistan increase the incidence of cybercrime, undermining current laws and enforcement mechanisms. Computer crimes, from embezzlement to cyber terrorism, are on the rise again due to the dearth of professionals, poor funding, and the ambiguous nature of laws (Sheraz et al., 2024). However, in 2016, the government of Pakistan passed the Prevention of Electronic Crimes Act (PECA), which still does not handle most of the current cyber threats, some of which involve cross-border cyber criminal activities and other techniques and advanced technological innovations, to name a few, according to Haider et al. (2023). Most police departments are ill-equipped, in terms of training and equipment, to tackle, investigate, and prosecute cyber criminals. Jurisdiction issues also pose another challenge to enforcement, especially to transnational crimes (Zarkoon, 2023). At the same time, inadequate cooperation between agencies and the underdeveloped PPP negatively impacts the ability to respond to cyber threats (Collier et al., 2022).

Cybercrime requires the cooperation of countries since nobody can tackle the problem alone. Pakistan, in particular, is being called to harmonize its cybersecurity acts with those of other countries and enhance cooperation to share information and capacity (Hadi, 2024). Also, using digital forensic solutions for tools, threat detection, and encryption will increase resistance to cyber threats (Saeed et al., 2023). Cybercrime prevention depends heavily on society's level of awareness and education in technology-related matters. Public awareness campaigns can help lower a person's susceptibility to attacks. Intensifying cooperation with other agencies, improving the legislation combating cybercrime, and filling the previously used gaps are also necessary. Due to cyberspace's rapid expansion, strong laws governing cyberspace have been needed in various regions of the globe. These situations have prompted states to employ regulatory and criminal laws to deal with cyberspace problems. For instance, the United States employs the Sherman Anti-Trust

⁴ According to the doctrine, offensive operations are carried out by the Indian military's diverse branches cooperating as cohesive battlegroups. Within days of a conflict, this entails sending troops to the western border. Cyber, electronic, and network-centric warfare, unconventional warfare, and maneuver and psychological warfare are all components of the doctrine.

⁵ PPP, or "private-public partnership," is a term used in the cybersecurity context to describe a cooperative effort between public sector government agencies and private sector businesses to address cyber threats. This collaboration frequently entails information sharing, cooperative research, policy development, and coordinated incident response strategies with the goal of enhancing overall cybersecurity posture throughout an ecosystem.

Act of 1890 as its employment law for regulating tech companies. The EU passed the GDPR⁶ in 2016, placing individual privacy rights higher than commercial ones (Adil, 2023).

According to the author, Pakistan, too, has established a theoretical basis for cyberspace's governance and criminality regulation based on the constitution of Pakistan and certain acts such as PECA, 2016. The FIA Act, 1974, and the Pakistan Telecommunication (Reorganization) Act, 1996. Currently, the Federal Investigation Agency Act 1974 identifies FIA as the leading cybercrimes investigating agency in Pakistan. The FIA operates across borders and works with Interpol. Therefore, it stands at the forefront of dealing with transnational cyber threats. However, capacity building and resource distribution, which are core requirements for an agency's efficient operation, are some of the challenges that the agency experiences. The Pakistan Telecommunication (Reorganization) Act 1996 gives the PTA sovereign rights to license, restrain, or ban material in cyberspace altogether. Using delegated legislation, the PTA implements other cyber regulations, including the Citizens Protection Rules, 2020 and Critical Telecom Data Security Regulations, 2020, to further elucidate its role in preventive measures.

The foremost law in the realm of cybercrimes in Pakistan is under the titled "The Prevention of Electronic Crimes Act, 2016." It introduces 23 crimes of terrorism by electronic means, fraud, and other electronic crimes, as well as provisions on procedure and prevention. However, because the act covers only three offenses, its enforcement power is limited by its scope. According to PECA, legal entities and government departments must establish CERTs⁷ and coordinate with international organizations; however, enforcement is difficult due to process intricacies (PECA, 2023). CISA defines cybersecurity as the processes and practice of safeguarding assets in computer networks and other computerized systems and protecting their confidentiality, integrity, and availability. This broad definition highlights cybersecurity's mainly preventive, often preemptive, certainly rights-based dynamics. Adil (2023) notes that the legislative history of Pakistan started with the Pakistan Telecommunication (Re-Organization) Act, 1996, to make the PTA for regulating the telecommunications sector.

The subsequent laws, including the Electronic Transactions Ordinance of 2002, gave legal acceptance to electronic transactions. However, the most important was the Prevention of Electronic Crimes Act (PECA), 2016, which pertains to social media regulation, cybercrimes, and cybersecurity. This puts PECA under the joint authority of the Ministry of Interior and Information Technology and Telecommunication and makes it the framework for regulating Pakistan's cyberspace. CERT Rules, in particular, paved the way for a new order to enhance Pakistan's cyber security. These rules define sectoral, national, and organizational CERTs and are coordinated by a CERT Council with members from the Ministries of Interior, Defence, and others. This makes the Council inter-ministerial so that it delivers a composite response to threats in the cyber realm between law enforcers and defense hardware. CERTs perform anticipatory roles such as security assessment and virus examination, as well as reactive activities, including emergency handling and preserving activities centered on quality. CERTs include the Security Operation Centre, Technology Development, Cyber Analytics, and Digital Forensic facilities. All these facilities can provide criminal justice-grade timestamps and Autonomous System Numbers (ASNs) to meet the forensic needs of the cybercrime investigation.

⁶One EU law that safeguards people's privacy and personal information is the General Data Protection Regulation (GDPR).

⁷A team of information security professionals known as a Computer Emergency Response Team (CERT) is in charge of preventing, identifying, and responding to cybersecurity incidents within an organization.

Change in the judiciary of Pakistan is moving towards reforms like an increase in efficiency, accountability, and people people-friendly legal framework.(Kasur et al., 2022).The conventional systems of justice delivery have long been associated with cases of inefficiency, delay, and corruption that contributed to eroding public confidence in justice delivery systems. Understanding these hurdles, new programs like the National Judicial Automation Program (NJAP) and e-court systems have been launched to bring legal practices into the contemporary world. Launched in 2016, the NJAP seeks to promote the electronic archiving of case data, electronic case management information technology systems, and filing and case monitoring technologies. Most of these reforms have helped to perform administrative functions elegantly, enhanced records keeping, and accelerated the processing of cases (National Judicial Automation Committee, 2019).

In the same way, the setting up of e-Courts satisfies the increasing requirement for distinct systems that are outfitted to cater to cyber criminality and all other related matters, managing weak points in electronic proof, to name one, through the use of online platforms as well as video conferencing as tools for the promotion of procedural gains (Press Release, 2019). Nevertheless, there are still some problems such as the technological infrastructure, cybersecurity, and rural and urban divide. In addition, AI, blockchain, and other predictive analyses are also possibilities for improvement of the work of courts. Specific cases, such as the Estonian e-governance mode,l provide a wealth of information that can be utilized to benchmark the quality of governance in the digital environment. Nevertheless, persistent efforts are underway in Pakistan towards a digital transformation that holds the promise of a more efficient, transparent and fair legal system with further innovation and the right partnership (Rehman, 2024).

The COVID-19 pandemic clearly unfolded and amplified the issues pertaining to Pakistan's judiciary, mostly the pile-up of cases in the Supreme Court, where the number reached 48,594 by March 2021. Such high pendency has arisen mainly because of the pandemic and low technology adaptation in judicial proceedings (Malik, 2021). Though former Chief Justice Asif Saeed Khosa effectively cleared criminal case backlog, pandemic restrictions have undone those by daunting thousands of criminal and civil cases. As a result, there have been discussions of extending the utilization of technology, such as virtual hearings. Although some attempts have been made, for instance, the e-court system that was initiated in 2019, video-link technology for lawyers and others is scarce at the Supreme Court. Justice Qazi Faez Isa also mentioned the option to create more virtual hearings, and legal professionals agree that this change would notably increase effectiveness, decrease expenses, and maintain social distancing rules. Internationally, India and the United Kingdom have set examples as, during the pandemic, they worked digitally and responded to millions of cases and hearings. As Pakistan's legal professionals claim, envisioning the urgent need for modernization, virtual hearings might substantially change the judicial picture. Lawyers state that these technologies could create opportunities to spare time and resources and increase openness and approachability. Nonetheless, they are still present. One is the capacity, lack of infrastructure, no digital in lower courts, and there is a need for training in this setup. Nonetheless, virtual hearings accord with constitutional directives of efficient and affordable justice and provide a monumental chance to reform a legal system for future resiliency.

Methodology and Data Collection

Qualitative research is used in this study to understand the difficulties experienced by the judiciary in trying cybercrime cases in Pakistan. As a subject that focuses on legal norms, institutions and practices, the type of research that is most appropriate to the analysis of laws and practices is a qualitative one. Related literature, legal documents, journals, books and articles, and publicly

available reputable newspapers and magazines were used to obtain a rich set of information on the judiciary's efforts aimed at combating cybercrime.

Data Collection

The purpose of this paper is to approach the challenges from as many aspects as possible. The data for this study is sourced only from secondary sources. The sources included books and academic articles that offered theoretical-informational plans of the judiciary in the sphere of cybersecurity and comparative activities from other jurisdictions. Government Documents and Legal Texts these primary legal prescriptions, including the PECA and related procedural legal instruments, were also examined to determine their effects on judicial proceedings. Moreover, magazines and periodicals, including institutional constraints and achievements in engaging with the cybercrime laws, were documented in articles that addressed the judiciary. It also includes news reports data regarding the cyber-crime cases, judiciary decisions and public perception collected from the various famous Pakistani newspapers and news channels. The obtained data was properly sorted in order to receive the shots of all the investigated aspects of the selected topic.

Data Analysis

The approach applied in analyzing data was thematic, and the characteristics of incidence profiles where the concern of the judiciary was established. The Legislative and Procedural challenges facing the judiciary in engaging cybercrime laws such as the problem of interpreting or defining certain provisions in PECA, 2016. Institutional Limitations include the examination of the factors contributing to insufficient training and technical skills and lack of resources in the judiciaries. Hence, the thematic approach enabled elaborate analysis of each difficulty, thus presenting a varied picture of the judiciary's role in cybercrime cases.

Scope of the Study

The study focuses on the following aspects:

1. Looking at the extent to which the judiciary implements and gives meaning to PECA and other connected laws.
2. Identifying the weaknesses prevalent in the judicial training, resources, and working methodology that do not help in making better cybercrime cases.
3. Comparing legal patterns of jurisdiction to those of Pakistan and proposing improvements for the cybercrime judicial process.

Rationale for Methodology

Consequently, a qualitative research approach was used because the study was institutional and legal. Using secondary data made it easier to analyze the judiciary's concerns critically and make various recommendations. Such an approach enabled the research to apply a theoretical understanding of the issue under study as well as operational approaches to the judiciary's activities as control over cybercrime.

Ethical Considerations

Ethical concerns in the research were upheld in the sense that adequate references to materials used were made, and bias in reviewing the findings was avoided. To that end, only the data already in

the public domain was utilized to honor do-no-harm principles regarding privacy and intellectual property.

Data and Analysis

Enhancing cyber security in Pakistan – the judiciary’s perspective has also emerged as an important factor in the advancement of cybercrimes in the present era. This section focuses on modern efforts and concerns related to cyber threats in the judiciary as well as the evaluation of crucial trends, including e-Courts and the NJAP. This also discusses the advancement in digital judicial proceedings in Pakistan, the challenges faced while dealing with cybercrimes, and an overview of the systematic weaknesses that cause barriers to the proper execution of the process. This segment establishes a comparative relationship between Pakistan and the US to highlight the imperative and pressing call for technological compromise, legal definition, and institutional practices that are appropriately representative of the reformist Pakistan judicial system in order to counter changing cyber threats.

Current Role of Judiciary in Cyber security in Pakistan

This paper analyzes the judiciary’s engagement in cyber security as a country undergoing technological transition. In the current decade, Pakistan has gone through considerable progress toward digitalization, primarily in the judiciary, through transparency and access to justice activities. These technological advancements have also helped the judiciary handle new challenges posed by cybercriminals. With the emergence of new cyber threats, the participation of the judiciary in legal approaches to cyber security issues has increased. This part analyses the present-day involvement of the judiciary in addressing cyberspace threats in Pakistan along with the use of technology and also dealing with the limitations of the legal framework. Today, the situation in Pakistan is quite different, and in recent years, the country’s judiciary has turned to digital products for better work. It is necessary to use such technologies to address cyber security issues since cases of cybercrimes have increased. Among such steps is NJAP, the National Judicial Automation Program that started in the fiscal year 2015-2016, based on which it appears that record-keeping has been stepped up massively with the help of NJAP. One has noted noteworthy development where, through the program, the case management has been put on alert and has generally developed the working mechanisms of the courts. Another breakthrough in turning the judiciary of Pakistan more digital was made in 2020 with the introduction of e-Courts. These courts are meant to hear electronic cases only, such as hacking, identity theft, financial fraud, etc. These initiatives put forward a digital structure that can help the judiciary handle interconnected cyber security issues and deliver justice to people who such crimes have harassed on time.

Judicial Initiatives

The National Judicial Automation Committee (NJAC) which began in 2016, transformed digitized case files and the courts and enabled the cases to be monitored electronically. E-courts launched in 2020 are firstly designed for the trial of cases connected to cybercrime and secondly for handling electronic evidence. These platforms enhance the chances of justice for various persons and deny allegations of criminal offenses such as cybercrimes online. Online Dispute Resolution Platforms that began in 2021 help to expand minorities’ access to justice and suggest a method to solve problems, including cyber criminality, online. These initiatives have equipped the judiciary with a technological platform that can address growing challenges in cyber security and empower the courts to deal with cyber security activities better.

Cyber security and Case Backlog

A failure in Pakistan's judicial system is delayed justice because of the existence of a large number of unsolved case files. On the other hand, information technologies can help alleviate this problem in cybersecurity cases. The outbreak has also observed that courts used e-Courts, online dispute resolution platforms as well as video conferencing hearings and thus helped to reduce administrative delay by moving fast on cases. For instance, during the management of COVID-19 cases, the judiciary implemented measures such as videoconferencing of civil and criminal hearings in regard to computer-related crimes. This meant that justice could be executed without wasting time, regardless of global turbulence. Moreover, digital case management has helped courts manage cases and give priority to important cybercrime cases, as it is achieved through the integration of AI and other case tools for case processing. There is potential for reducing congestion within the cases to enhance the development of solutions to cybersecurity-related issues.

Development in Cases Through Technology

Some infamous recent case studies in Pakistan show the judiciary's increasing involvement in the domain of cyber security. An example of this phenomenon is the presence of the former Prime Minister of Pakistan, Imran Khan, in the Supreme Court on 16 May 2024, which was a significant step in the country's digital evolution. Despite the absence of live streaming in the session, the judiciary successfully conveyed that it can conduct hearings through virtual platforms whether it be for general or special circumstances like the cyber security issue. Another example is the NJAP leading to the resolution of land dispute cases for digitization of records of land. As much as it may not be directly connected to cyber security, it works as an imitation of dealing with electronic evidence, something that is very important while dealing with cybercrimes. Through records automation and record centralized, Pakistan's judiciary has established a better and more secure mechanism for managing and preserving sensitive records such as digital evidence in cyber security-related cases.

Challenges faced by the Judiciary

Due to the continuous development of technologies, independence and security in cyberspace pose considerable challenges to legal systems worldwide. In the following paper, the issues that Pakistan's judiciary encounters in enforcing its cybersecurity laws include a lack of experience and knowledge, confusing laws that do not clearly define the judiciary, a lack of adequate resources, and system problems within the judicial body.

1. Limited Technical Expertise

This phenomenon remains one of the significant challenges since the judiciary lacks adequate technical skills. Current and emerging cybercrimes solve puzzling digital evidence viz data in code, block chain sequences, and sophisticated hacking strategies. Unfortunately, most of these judges and many lawyers in Pakistan lack sufficient training to deem these technicalities necessary and helpful, which often results in faulty interpretation of the evidence or slow procedural work. Hence, this lack of insight leads to consultants, which prolongs the process and brings into confusion the neutrality of the consultant.

2. Legal Ambiguity

The primary law on electronic crimes in Pakistan is called the Prevention of Electronic Crimes Act (PECA) 2016. Although it covers a number of types of cybercrimes, it has loopholes, and it lacks clearance in some critical aspects. ‘Unauthorized access’ and ‘hacking’ are two of the many terms that are rather loosely described. It also fails to define new threats such as ransom ware or deep fake, leaving it difficult for judges to apply the law when handling new crimes. These reasons make judgments to be inconsistent thus eroding public confidence in the Judiciary.

3. Offenses Relating to Corruption and Illicit Conduct

This has been worsened by corruption within the judiciary and associated law enforcement agencies, whereby bribes may lead to the dismissal of cases or reduced sentencing for offenders who implement cyber security laws. The nature of crime makes it difficult for law enforcement to arrest and incarcerate offenders who breach cyber security laws effectively. (Japonica, 1994). The democratic institutions, labor organizations, or even citizens’ protests or demonstrations may be suppressed in the name of national security, which goes a notch higher to degenerate the rule of law. This creates another dimension of injustice in that influential people never face the law as compared to other individuals in society.

4. Prejudice and Public Trust

Many discriminated practices in Cybercrime cases against distressed women and minority groups, such as victims of cyber harassment such as women, are often blamed in courts. (Khan et al., 2023). Individuals and minorities who experience hate speech and or cyber-attacks stand to be discriminated against when seeking justice. They dissuade victims from reporting the crimes to courts and let hackers operate freely and without much consequence.

5. Resource Constraints

Currently, the judiciary in Pakistan works under a lack of resources, and it has a negative impact on its ability to address cybercriminal activities. They also pointed out that courts do not have access to sophisticated forensic instruments that are required to work on electronic evidence. Another challenge is that there is inadequate staff to execute the training in dealing with cyber security cases, hence means that there’s inadequate staff to handle the cases when they occur, hence delayed trials.

6. Nature of Cyber Threats

The area of computer and technological security is fluid and in constant development and, as such, poses a big challenge to the judiciary. Creation of fake media containing blackmailing messages with the help of artificial intelligence. Growing reports of ransom ware attacks on infrastructure organizations. The judiciary, in particular, is challenged to adapt to these threats and quite often is on the back foot rather than on the front foot.

7. Public Education and Communication

Lack of public awareness of the rights provided under cybersecurity laws reduces the strength of the common law of the judiciary. The reasons that victims of cyber harassment do not report cases include lack of confidence in the legal system and fear of stigmatization. Cyber-attacks victims prefer resolving outside the court since affected businesses rarely involve the judiciary. This

underreporting distorts crime incidences and, in the process hampers the judiciary in its efforts to tackle root causes.

8. Lack of Embrace for Digital Change

In this respect, attempts at reform through digitization of the judiciary have been hampered from within. Those judicial officers who have had traditional ways have determined change.

Perceived risks of technology and computing resources. Less competition facilitates Omni competent-tied adoption at a slow pace, slowing down innovative technological solutions that could enhance case management and increase efficiency. The problems associated with the judiciary in Pakistan while implementing cyber security laws can be categorized as technical, legal, systematic, and societal. Addressing these challenges will need to involve legislative changes, capacity development, financial investment, and community mobilization. Attacking these fronts, Pakistan can set a strong legal backdrop against cybercrimes and bring justice in the newly emerging digital era.

Comparison with USA

Governments all across the globe have been facing the rise of cybersecurity issues due to advancements in digitization. Cyber threats continue to pose a problem to developed and developing nations, which have strained the legal and judicial systems. This paper identified the challenges faced by the judiciary in Pakistan, wherein systemic and infrastructural issues pose hindrances to 'Cyber Security Laws.' On the other hand, the United States, which has a highly developed legal framework, provides an understanding of how a strong and elaborate judicial system can address the nature of modern and constantly evolving cybercrimes. Consequently, this comparative analysis aims to identify legal regimes and judicial structures in Pakistan and the USA and the mechanisms for addressing cybercrime.

Pakistan vs USA

Pakistan's cybersecurity laws are still largely encapsulated in the Prevention of Electronic Crimes Act (PECA) 2016. Although the passing of PECA was a major step in combating cybercrimes, it still needs to encompass the holistic approach in the US. On the other hand, the cybersecurity laws of the USA, comprising CFAA, CISA, and state cybersecurity laws, offer a multiple and evolving architecture. The legal framework is vital to the time-oriented resolution of cybercrime cases. The Lahore High Court noted that it does not have standard forensic labs or a proper system for the chain of custody of evidence. This causes the cases to last a long time, and in 2023, only thirty percent of cybercrime cases were prosecuted. In the USA, for instance, there exist well-developed infrastructure digital forensics units and secure case management systems that make the process efficient.

Statistical Insights

Cyber security crimes rose to 83% in Pakistan from 2018 to 2023, of which only 30 % were resolved, mainly due to a lack of judicial redress. In the United States, due to which positive legislative activities have been initiated to amend laws and enact new ones, the cybercrimes in the progress year have been reduced up to 10 % with the resolution rate higher than 75%. In 2023, digital evidence was declared inadmissible in 95% of Pakistani cybercrime cases because of procedural failures, and the U.S. has high requirements for evidence care.

Public awareness and Legal Education

An essential component of cyber security law enforcement is, therefore, public education. Their cyber literacy is low, especially since most victims do not report their crimes to the police or seek legal action. On the other hand, the USA has embarked on massive awareness-creating projects, including education, and consequently, the reporting levels and involvement with the judiciary have been high. The comparative analysis data shows how significantly different the two countries, Pakistan and the USA, are in applying cyber security laws through the judiciary system. When Pakistan faced problems with the lack of resources, legislation, and insufficient training of judges, the USA showed that it was possible to create a carried-out approach to combating cybercrime. These differences further signify the need for systemic solutions in Pakistan to address the difficulties thrown up by the changing nature of the cyber threat.

Recommendations for Handling Legal Challenges Faced by Judiciary in Implementing Cybersecurity

To overcome the issues pertaining to the implementation of cybersecurity laws in Pakistan, profound and pragmatic recommendations that can address the legislative and judicial gap and enhance public awareness are needed.

- Seminars for judges and other law enforcement persons are necessary to reduce the existing knowledge gap between cybersecurity laws and digital crime dynamics. These cases can be discussed during workshops and seminars, and general training can offer information on managing cases that include digital evidence, knowledge of cybercrime, and interpretation of technicalities of any law such as PECA 2016. This training should be practical based in order to equip the judiciary with the ability to handle new challenges as they emerge.
- Digital forensic tools and sophisticated technology support systems should be offered to police and the judiciary in order to enhance their capacity to prosecute cybercrime. In the absence of such resources, the gathering and investigation of evidence usually turns out to be substandard and, in some cases, results in delays and unwarranted dismissals. Through the application of modern technology in the judiciary movement, people can get fair trials in addition to enhanced movements of cases.
- New circuits of courts should be created to address cybercrime cases exclusively. Such courts would fast-track the disposal of cases and build a specialty in dealing with cybercrime cases. A high level of specialization is important as conventional courts rarely handle cybercrime cases effectively due to a lack of necessary technical expertise and are likely to end up with procedural, time-consuming, and erroneous decisions.
- A mandatory amendment in PECA 2016 is to clarify the destruction of vagueness and to avoid abuse, mainly of defamation clauses and freedom of speech. The law must spell out what is a cybercrime and how it should be handled, separate from mere frame-ups to hide democracy and freedom of speech. Reforms in the legislation have also ensured that the law is capable of keeping up with the increasing advancement of the digital world.
- Tying up with international policies will enhance the effectiveness of cooperation with other countries in the fight against cyber criminals and enable Pakistan to cope with modern tendencies in the sphere of cyber security regulations.
- It is very important to raise public awareness so that citizens are informed about the existence of cyber security laws, their rights, and the ways through which those involved in cybercrimes can be reported. Unfortunately, the public is unaware of most legal actions that are misused; by enlightening the public, the judiciary can prevent abuse and strengthen the

victims' confidence in reporting such cases. Partnerships with schools, colleges, universities, or other relevant organizations can complement such efforts.

- More efforts should be made to engage businesses and private organizations and inform people that anyone should not violate cyberspace laws. This partnership can also help develop strong information security systems in organizations to protect them against cyber threats.
- There needs to be a realized that working together with other agencies, especially the FIA, can help advance the investigation and provenance of cyber offenses. There are communication corners and media forms that make it easy to promote cooperative workflow within the team, avoid work redundancy, and ensure proper case management.
- Best practices for the acquisition, preservation, and sharing of digital evidence should be instituted because they have legal relevance. The judiciary must ensure the necessity of implementing adherent policies in relation to the chain of custody to avoid scrutiny of digital evidence. This is important to ensure that justice is served regarding crimes committed in cyberspace.
- A relationship that must be maintained for judicial independence is that these representatives, the judges, should be shielded from extraneous pressures and political and societal influences. Most cybercrimes involve celebrities, and such incidences may attract a lot of publicity; hence, the judiciary must act bias-free.
- Like terrorism, cross-border cybercrimes should be prevented through cooperation with the international community. Pakistan needs to join international cybersecurity communities and form regular cooperation in addition to investigations. In many cybercrimes, individuals in foreign or multiple jurisdictions may perpetrate this malice.
- Establishing links with overseas cybersecurity forums and studying what they do could be very helpful. Such exchanges mean that the judges, prosecutors, and investigators who attend and take part in the master classes improve on the advanced techniques they adopt when addressing their local issues efficiently.
- It is crucial to recruit technical specialists to help the judiciary assess and determine complicated cybercrime matters. Specialists can offer technical knowledge, thus making a decision based on substantial knowledge and the occurrence of the crime.
- Legal aid services should be provided to cybercrime victims to ensure that they are properly represented. Most victims realize that they do not have enough money or inadequate legal education to fight for themselves, thereby preventing justice. This way, the lack of efficient legal aid provision may be successfully met.
- Friendly websites that enable users to report cybercrimes and follow up on their complaints are needed. Such sites may help increase the awareness of these victims and hasten the police response to incidents. Open reporting of complaint handling can also increase the public's confidence in the system.
- Resource allocation involves improving technological support for courts and police departments. This investment will assist the judiciary in addressing all issues related to cybercrime expeditiously, thus delivering justice to the people.

Conclusion

Though Pakistan enacted the Prevention of Electronic Crimes Act (PECA) 2016 to regulate such crimes, the law has ambiguous provisions, and again, either defaming the law or discussing freedom of expression should be dealt with in need of reform. Thus, the aim of increasing the effectiveness of combating cross-border cybercrime and improving the intelligibility of the law in accordance with modern trends requires its improvement and bringing it in line with the

requirements of the modern world. Therefore, the judiciary and law enforcement agencies should have enough knowledge and practical measures to deal with cybercrimes. These courses help fill the knowledge gaps relating to cybersecurity laws, the handling of digital evidence, and technological advancements. Offering courts and investigating bodies digital forensic equipment will increase the identification, collection, and analysis of digital evidence to help prevent unjust judgments.

Devoted cybercrime courts staffed by professional judges are needed to reduce case-handling time and eliminate bias in court cases. It is just as important to increase citizens' awareness of their rights and of cases of abuse, as well as their safe behavior on the Internet. Engagement with private institutions can enhance the compliance level and the cybersecurity system. To improve the level of investigations and prosecution there is a necessity to enhance cooperation between FIA and other anti-corruption agencies. The high degree of formalization of the processes of collection and sharing of digital evidence will minimize procedural time costs, and participation in international organizations can aid Pakistan in the adoption of best practices in handling complicated cybercrime cases. Easy reporting procedures and services provided by legal agencies will compel people to take the law into their own hands. From the findings above, it will be important to have regular reviews and assessments from legal operatives and the public to enhance the cybersecurity laws.

References

1. Japonica, C. C. (1994). *MASTER OF SCIENCE IN Master of Science*. August.
2. Kasur, M. R., Abbas, S., & Ahmed, G. (2022). Imbalance Criminal Justice System of Pakistan: Joined Up Working is the Way Forward. *Global Social Sciences Review*, VII(I), 463–472. [https://doi.org/10.31703/gssr.2022\(vii-i\).43](https://doi.org/10.31703/gssr.2022(vii-i).43)
3. Khan, H., Basharat, T., & Hayat, I. (2023). *An Analytical Study of Unveiling Gender-Based Harassment in Cyberspace: An Exploration of Realities and Experiences*. <https://doi.org/10.20944/preprints202306.0813.v1>
4. Mofokeng, J. T., & Aphane, M. P. (2022). Evaluating Knowledge Management Capabilities During Crime Scene Processing in the Detective Service. *OIDA International Journal of Sustainable Development*, 15(9), 11–28.
5. Science, E. A., & Eriotis, N. (2024). *A historical analysis of the banking system and its impact on Greek economy*. October. <https://doi.org/10.55214/25768484.v8i6.2282>
6. Adil, K. (2023, March 7). *Legal Framework for Policing Cyberspace in Pakistan*. *Research Society of International Law | RSIL*. (n.d.). Retrieved from <https://rsilpak.org/2023/legal-framework-for-policing-cyberspace-in-pakistan-an-overview/>
7. Adil, K. (2023, November 24). *Strengthening the Legal Framework for Cybersecurity In Pakistan*. *Research Society of International Law | RSIL*. . (n.d.). Retrieved from <https://rsilpak.org/2023/strengthening-the-legal-framework-for-cybersecurity-in-pakistan-the-computer-emergency-re>
8. *Australian Cyber Security Centre*. (n.d.). *Ransomware*. *Cyber.gov.au*. (n.d.). Retrieved from <https://www.cyber.gov.au/threats/types-threats/ransomware>
9. *CISA*. (2024). *Information Sharing | Cybersecurity and Infrastructure Security Agency CISA*. *Www.cisa.gov*. . (n.d.). Retrieved from <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>
10. *Cybersecurity - Pakistan | Statista Market Forecast*. (n.d.). *Statista*. (n.d.). Retrieved from <https://www.statista.com/outlook/tmo/cybersecurity/pakistan>

11. <https://tribune.com.pk/author/234>. (2021, April 10). *The case for online hearings* | The Express Tribune. Tribune.com.pk. . (n.d.). Retrieved from <https://tribune.com.pk/story/2294089/the-case-for-online-hearings>
12. *Improving Pakistan's cybersecurity architecture using US and UK insights*. (2024). Ibanet.org. . (n.d.). Retrieved from <https://www.ibanet.org/Improving-Pakistans-cybersecurity-architecture-US-UK-insights?>
13. Joseph, J. (2024, July 13). *Pakistan's Digital Revolution: Enhancing efficiency, transparency, and accessibility in the Jurist.org; - JURIST - Features - Legal News & Commentary*. . (n.d.). Retrieved from <https://www.jurist.org/features/2024/07/13/pakistans-digital-revolution-enha>
14. Khan, M. F., Raza, A., & Naseer, N. (2021). *CYBERSECURITY AND CHALLENGES FACED BY PAKISTAN*. ResearchGate, 4(4), 865–881. . (n.d.). Retrieved from https://www.researchgate.net/publication/361218515_CYBERSECURITY_AND_CHALLENGES_FACED_BY_PAKISTAN
15. Khan, M. F., Raza, D. A., & Naseer, D. N. (2021). *CYBER SECURITY AND CHALLENGES FACED BY PAKISTAN*. Pakistan Journal of International Affairs, 4(4). (n.d.). Retrieved from <https://doi.org/10.52337/pjia.v4i4.408>
16. Mian, D. (2024). *Cybercrime Legislation And Enforcement In Pakistan: Assessing Gaps And Solutions*. Migration Letters, 21(S9), 1243–1255. (n.d.). Retrieved from <https://migrationletters.com/index.php/ml/article/view/10352?>
17. Muhammad Sheraz, M., Fazli Dayan, Murtaza, M., Umar, M., Batool, A., Muhammad, M., & Khalid. (2024). *Migration Letters Cybercrime Legislation And Enforcement In Pakistan: Assessing Gaps And Solutions*. 21(S9), 1741–8992. (n.d.). Retrieved from <https://migrationletters.com/index>.
18. National Response Centre For Cyber Crime. (2013). Nr3c.gov.pk. (n.d.). Retrieved from <https://www.nr3c.gov.pk/cybercrime.html>
19. National Response Centre For Cyber Crime. (2013). Nr3c.gov.pk. . (n.d.). Retrieved from <https://www.nr3c.gov.pk/cybercrime.html>
20. Petrosyan, A. (2023, November 15). *Global cybercrime is estimated to cost 2028*. Statista. (n.d.). Retrieved from <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>
21. Qarar, D. com | S. (2018, November 6). *“Almost all” Pakistani banks hacked in security breach, says FIA cybercrime head*. DAWN.COM. . (n.d.). Retrieved from <https://www.dawn.com/news/1443970>
22. Riaz, M. (2019). *Cyber Threat Landscape and Readiness Challenge of Pakistan*. . (n.d.). Retrieved from https://www.issi.org.pk/wp-content/uploads/2019/04/1-SS_Muhammad_Riaz_Shad_No-1_2019.pdf
23. Saleem, H., Jan, J., & Azzalfa Areej. (2022). *Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges*. . (n.d.). Retrieved from <https://doi.org/10.62585/slpr.v1i1.21>
24. Syed. (2023). *A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan*. Social Sciences, 12(11), 629–629. (n.d.). Retrieved from <https://doi.org/10.3390/socsci12110629>