Migration Letters

Volume: 21, No: S9 (2024), pp. 1243-1255

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Cybercrime Legislation And Enforcement In Pakistan: Assessing Gaps And Solutions

Dr. Mian Muhammad Sheraz[1] , Dr. Fazli Dayan[2] , Muniba Murtaza[3] , Muhammad Umar[4] , Aniza Batool[5] , Dr. Muhammad Munib Khalid[6]

Abstract

Introduction: *An important challenge to Pakistan's legal and law enforcement systems is the emergence of cybercrime. This study looks at the current weaknesses in the country's cybercrime legislation and enforcement practices and offers solutions. With cybercrimes ranging from financial fraud to cyber terrorism on the rise, Pakistan needs to take strong legislative and enforcement measures. However, the efficacy of the law is hampered by poor enforcement and interpretation.* ***Research method:*** *This study uses a qualitative research method to examine cybercrime laws, policies, and their implementation through in-depth interviews with legal experts, law enforcement officers, and stakeholders. Qualitative analysis enables a deeper comprehension of the opportunities and challenges in Pakistan's cybercrime landscape.* ***Data analysis:*** *The analysis reveals several significant legal deficiencies, such as ambiguous jurisdiction, vague definitions, and insufficient fines. Furthermore, inadequate technology, a lack of professional expertise, and resource constraints plague enforcement procedures.* ***Conclusion and Recommendations:*** *To solve these issues, extensive reforms are ne[1]eded. Among the suggestions are modifications to the law to provide clearer definitions and harsher penalties. Other suggestions include boosting public-private partnerships, fostering international cooperation, and bolstering law enforcement capabilities with improved equipment and training. By implementing these strategies, Pakistan may lower cyber threats, safeguard digital infrastructure, and boost confidence in its cybersecurity ecosystem.*

Keywords: *Cybercrime, legislation, enforcement, financial fraud, cyber terrorism.*

Introduction

The spread of technology in the modern digital era has changed the nature of crime and presented a multitude of difficulties for legal and law enforcement institutions around the globe. Among these difficulties, cybercrime is particularly noteworthy since it is a persistent and dynamic threat that cuts across national borders and poses serious threats to people, companies, and governments alike. Pakistan faces the same challenges as many other countries: how to preserve its citizens' digital rights and privacy while also thwarting cyber-attacks (Saleem, Jan, & Areej, 2022)? Computers have radically revolutionized human existence and significantly improved its ability to be controlled and organized. In contemporary society, both individuals

[1]Assistant Professor, Department of Law, Grand Asian University Sialkot, Punjab, Pakistan.
[2]Associate Professor, Department of Law, Grand Asian University Sialkot, Punjab, Pakistan.
[3]International Islamic university, Islamabad, Pakistan.
[4]Lecturer, College of Law, University of Sargodha.
[5]Department of Criminology and criminal Justice system, Minhaj University Lahore.
[6]Assistant Professor, School of Political Science, Minhaj University Lahore.

and businesses heavily rely on computers, as they have become a crucial element of our everyday lives. We start our day with the alarm of our cellular phone, which operates using computer networking technology. Computers are essential instruments that empower us to effectively and precisely perform our daily tasks. Computers have become an essential and integral part of our everyday life, including mobile phones, laptops, and desktops (Anderez, Kanjo, Amnwar, Johnson, & Lucy, 2021). Cyberspace is a very influential realm where data and information are processed with remarkable precision and efficiency. Cybercriminals breach the digital domain and corrupt the data of persons or businesses. Computers are undeniably employed as instruments to commit illegal crimes. Cybercrime refers to any unlawful behavior that is conducted using a computer, either as a tool or as the ultimate goal (Vitus, 2023). Over the last few decades, there has been a surge in the use of automated technology, big data, the Cloud, and Artificial Intelligence. These advancements have greatly improved human existence, but they have also introduced novel risks and problems. These cyberspace-related issues have an impact on online crimes, data privacy, security, and storage. Handling these new issues is a difficult effort and a serious concern because technological improvements have also led to increased rivalry in cyberspace as organizations and proxy players have emerged to further their political and ideological agendas (Al-Khater, Al-Maadeed, Ahmed, Sadiq, & Khan, 2020).

Cybersecurity has become increasingly significant worldwide due to the ubiquitous use of computers in many aspects of life. The importance of cybersecurity has grown significantly for developing countries in the third world, mostly due to the existence of imminent threats and the inadequate institutional structures already in place. Pakistan serves as a clear example. The country has enacted cyber security legislation to regulate and mitigate cyber threats and attacks. However, the effectiveness of these measures is compromised due to a lack of proper execution, which can be attributed to several factors (Prasad & Rohokale, 2020). Cybercrime is a broad term frequently used informally to refer to a wide range of criminal activities conducted through digital means. Cybercrime is the commission of a criminal act using a digital device and taking place on the internet (Holt, Bossler, & Seigfried-Spellar, 2022).Cybercrime refers to unlawful behaviors that involve the use of a computer, the internet, advanced technology, and the virtual environment called cyberspace (Rakhmanova & Pinkevich, 2020). The term "cybercrime" was introduced in 1995 to expressly refer to criminal activity conducted via computers. Cybercrime is the act of using a computer to commit illegal activities, either by directly targeting the computer or by employing a combination of technological tactics. Another distinguishing feature of this crime is that it does not require the perpetrator to be physically present at the location of the crime (Engle, 2020). Digital crimes, in contrast to conventional crimes, necessitate the use of cyberspace to cause harm to an individual or their possessions. For example, somebody with expertise in hacking can illicitly access a bank account situated in Pakistan, regardless of their geographical location. Similarly, actions of software piracy can be executed from a distant site (Wall, 2024).

Effectively combating intricate cybercrimes requires robust and unwavering management. To do this, it is imperative to build a robust and all-encompassing legislative framework. Pakistan has been classified as a country with a higher prevalence of cybercrime in comparison to other nations. Cybersecurity involves a variety of cyber threats and assaults, such as hacking, stealing someone's identity, committing financial fraud, executing phishing schemes, and launching ransom ware attacks. The increase in cybercrime can be attributed to a lack of understanding of cybersecurity, insufficient implementation of cyber laws, limited resources for law enforcement, and the increasing dependence on technology in the country (Anjum, 2020). Cyber laws pertain to matters that arise in the digital domain and target those involved in unlawful activity on the internet. The primary objectives of this study are to examine the

prevalence of cybercrimes in Pakistan and the corresponding cyber legislation. Despite the existence of the Prevention of technological Crimes Act, 2016 (PECA), it fails to encompass numerous modern technological activities. Consequently, Pakistan still faces a substantial amount of uncontrolled electronic offences (Sabiri & Sabiri, 2023).

Background and Context

The swift proliferation of digital technology and internet connectivity throughout Pakistan has given rise to cybercrime, which poses a significant threat to the nation's legal and law enforcement infrastructure. Pakistan's internet penetration rates have increased dramatically over the last 20 years due to a number of causes, including the widespread use of cellphones, the introduction of reasonably priced data plans, and government programs to encourage digital connectivity. Although the digital revolution has yielded many advantages, Pakistan is now vulnerable to cyber threats such as identity theft, hacking, online fraud, cyberbullying, and cyber terrorism (M. F. Khan, Raza, & Naseer, 2021). Cybercrime poses a wide spectrum of threats and is complicated, involving a variety of illegal actions carried out via digital means in Pakistan. Phishing and online banking scams are examples of financial fraud schemes that take use of cybersecurity infrastructure flaws to defraud unwary people and businesses of their money. In a similar vein, extremist organizations use the internet to radicalize people, enlist allies, and plan attacks; this presents a serious threat to national security. Furthermore, the growth in cyberbullying and online harassment brought about by the widespread use of social media platforms has heightened worries about online safety and privacy (Saleem et al., 2022).

Rationale of the Study

Given this, an assessment of Pakistan's cybercrime legislation and enforcement protocols is important. While the country has made strides in enacting laws and guidelines to address cyber threats, these efforts are frequently rendered less successful by implementation challenges, ambiguous legal precedents, and a lack of money. Furthermore, because cyber dangers are constantly evolving and technology is advancing quickly, regulatory frameworks must be regularly reviewed and modified to ensure their continued relevance and efficacy (Saleem et al., 2022).

This paper attempts to bridge a major research gap by providing a comprehensive analysis of Pakistan's cybercrime landscape and emphasizing the shortcomings and inadequacies in the nation's current legislation and enforcement procedures. By carefully analyzing the legal system, enforcement strategies, and stakeholder perspectives, this study aims to provide light on Pakistan's problems with combating cybercrime and practical solutions to these problems.

Objectives of the Research

1. To determine the main flaws and loopholes in Pakistan's cybercrime laws and enforcement procedures.
2. To evaluate how well Pakistan's present cybercrime laws and policies are working to combat the country's changing cyber threat environment.
3. To provide workable answers and suggestions for improving Pakistan's cybersecurity capabilities, laws against cybercrime, and enforcement systems.

Research Questions

1. What are the main flaws and shortcomings of Pakistan's laws and procedures for dealing with cybercrime?
2. To what extent do the current laws and policies against cybercrime effectively counteract the diverse cyber dangers that Pakistan is facing?

3. What particular actions may be taken to improve Pakistan's cybersecurity, bolster laws against cybercrime, and increase enforcement protocols?

Significance of the Study

This study is critical to Pakistan's legal and law enforcement systems' ability to address the grave concerns posed by cybercrime. In addition to endangering individual citizens, cybercrimes are becoming a bigger threat to national security, the US economy, and the country's standing in the international digital arena. By analyzing the shortcomings in cybercrime laws and enforcement practices, this paper provides invaluable insights into the shortcomings limiting effective responses to cyber threats. Furthermore, the study's emphasis on offering solutions offers policymakers, law enforcement agencies, and other stakeholder's helpful guidance meant to strengthen Pakistan's cybersecurity ecosystem. Ultimately, implementing these ideas might improve public safety, protect digital infrastructure, and restore trust in the judicial system—all of which would improve the nation's resilience to cyber-attacks and promote economic growth.

Literature Review

Pakistan is currently facing a range of challenges, including corruption, poverty, limited technological progress, and an unstable political system. The presence of these variables poses numerous obstacles to the organization's internal security, with cybersecurity emerging as a vital component. Pakistan's law enforcement authorities face numerous complex obstacles in their efforts to prevent cybercrime (Nadeem, Liu, Zulfiqar, Younis, & Xu, 2021). As cyber threats are becoming more frequent in Pakistan, there is growing worry about the country's cybercrime laws and enforcement. In the context of Pakistan, academics have studied the legal, technological, and sociological facets of cybercrime in great detail (U. P. Khan & Anwar, 2020). The Prevention of Electronic Crimes Act (PECA) 2016 is the main piece of legislation that governs cybercrimes in Pakistan. Cyber terrorism, electronic fraud, unlawful access to information systems, and online harassment are just a few of the many cybercrimes that are made illegal by PECA. Nonetheless, academics have identified weaknesses in the way PECA is implemented and how well it works to reduce cybercrimes (Haider, Ali, & Zubair, 2023).

One of the biggest issues in Pakistan's fight against cybercrimes is enforcement. Law enforcement organizations frequently lack the technological know-how, funding, and training required to adequately investigate and prosecute cybercrimes. Enforcement operations are further complicated by problems like jurisdictional ambiguity and the cross-border nature of cybercrimes (Haq & Zarkoon, 2023). Researchers have found a number of legal flaws in Pakistan's cybercrime laws, such as imprecise definitions, unclear jurisdiction, and insufficient sanctions. These flaws make the legal system less effective at handling the complexity of cybercrimes and bringing those responsible to justice (Jamshed, Rafique, Baig, & Ahmad, 2022). Given the transnational nature of cybercrimes, international cooperation is vital for their effective combatation. Academics underscore the significance of Pakistan's cooperation with foreign allies, encompassing the exchange of knowledge, proficiency, and assets to jointly confront cyber hazards. Improving cybersecurity in Pakistan requires fortifying public-private partnerships. Information exchange, capacity building, and the creation of cybersecurity solutions can be facilitated by cooperation between government agencies, businesses, and civil society organizations (Hadi, 2024).

Enhancing the ability of law enforcement agencies and judicial organizations to investigate and prosecute cybercrimes requires significant investment. Academics suggest workshops, training

courses, and skill-building projects to improve the technical proficiency of those working in cybercrime enforcement (Obidimma & Ishiguzo, 2023). It is crucial to educate the public on cybersecurity threats and appropriate practices. Education programs aimed at people, companies, and governmental organizations can enable participants to successfully reduce risks and defend themselves against cybercrimes (Collier, Thomas, Clayton, Hutchings, & Chua, 2022). The mitigation of cyber dangers is significantly aided by technological improvements. In order to improve Pakistan's cyber resilience, experts stress the significance of investing in cybersecurity technology such sophisticated threat detection systems, digital forensics tools, and encryption solutions (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023). Pakistan's cybercrime laws need to be changed in order to close the loopholes and contradictions that now exist. To make the legal structure more successful in thwarting cyber dangers, it is suggested to provide more precise definitions, stiffer punishments, and more efficient procedures (Akhlaq, 2021).

A number of studies have examined particular cybercrime incidences and their consequences for Pakistan through empirical research and case studies. These studies offer insightful information about the prospects and difficulties of fighting cybercrimes in the context of the nation (Akhtar, 2023). Studies that contrast Pakistan's cybercrime laws and enforcement methods with those of other nations provide insightful insights. These studies point out potential for improvement and areas where Pakistan can benefit from international best practices (Bokhari, 2023). After reviewing the literature, academics frequently provide policy proposals to remedy the gaps in Pakistan's cybercrime laws and enforcement. These suggestions are meant to give policymakers and practitioners useful information. They are grounded in theoretical frameworks, empirical data, and comparative assessments (Noor, 2021). A survey of some literature includes an analysis of Pakistan's current methods for enforcing laws against cybercrime. Academics may point out flaws in the laws and procedures that are in place now and suggest fresh approaches or creative fixes to solve the issues (A. A. Khan et al., 2022).

The involvement of international agencies in defining global cybersecurity rules and practices has a substantial impact, which can be intricate for particular nations such as Pakistan. Pakistan has experienced a significant increase in cybercrimes in recent years, including incidents such as data breaches, online fraud, and cyber espionage. Although the causes of these crimes are complex and have multiple roots, it is important to acknowledge the significant impact of international bodies. Partnerships with foreign intelligence agencies and multinational organizations can unintentionally contribute to the spread of cyber dangers in Pakistan's digital ecosystem (Radoniewicz, 2022).The presence of foreign intelligence agencies in Pakistan's cybersecurity arena has generated concerns over espionage and the pilferage of data. Intelligence agencies from many nations often execute advanced cyber espionage operations targeted at entering key government, military, and corporate networks in Pakistan. These efforts not only impair the security of a country but also lead to the breakdown of confidence between nations. Furthermore, the clandestine nature of these operations provides a substantial barrier for Pakistani authorities in successfully recognizing and resolving cyber threats, consequently strengthening the country's susceptibility to cybercrimes (Mirza & Akram, 2022). Multinational corporations (MNCs) exert significant control over Pakistan's digital infrastructure, but, their objectives may not always coincide with the country's cybersecurity requirements. Although multinational corporations (MNCs) bring about technology breakthroughs and economic benefits, their presence can unintentionally add to cyber risks. For example, the rapid growth of digital services and e-commerce platforms by international corporations may exceed the local cybersecurity skills, hence generating vulnerabilities that hackers might take advantage of. In addition, multinational corporations (MNCs) may place a

higher emphasis on financial gain rather than cybersecurity, resulting in insufficient investment in strong preventive measures (Anwar et al., 2022).

International cybersecurity initiatives, although intended to promote collaboration and enhance capabilities, can unintentionally make Pakistan vulnerable to cyber assaults. Engaging in global cybersecurity forums and information-sharing platforms puts Pakistani networks at danger of encountering various cyber threats, such as the spread of malicious software and cyber-attacks carried out by both governmental and non-governmental entities. In addition, the incorporation of global cybersecurity standards and protocols may not consistently correspond with Pakistan's distinct socio-political circumstances, resulting in difficulties in executing them and possible weaknesses (Haque et al., 2023). The involvement of global firms in Pakistan's cybersecurity scene presents both opportunities and challenges. Collaborations possess the capacity to enhance the dissemination of knowledge and technological expertise, yet they also render the country more prone to emerging cyber threats and vulnerabilities. Pakistan should exhibit prudence while aiming to strengthen its cybersecurity capabilities and navigate the complex dynamics of international partnerships. To guarantee the safeguarding of Pakistan's digital sovereignty and mitigate the risks of cybercrimes, it is imperative to prioritize national cybersecurity interests and engage in cooperation with international organizations (Anjum, 2020).

The literature analysis concludes by offering a thorough summary of the body of knowledge regarding cybercrime laws and enforcement in Pakistan. It provides insightful information for next studies and the formulation of policy by highlighting important problems, obstacles, and opportunities in the context of the nation's fight against cybercrimes.

Research Methodology

This study thoroughly examines Pakistan's cybercrime laws and enforcement procedures using a qualitative research methodology. Conducting lengthy, in-depth interviews with a wide range of stakeholders, such as legal experts, law enforcement personnel, government officials, and cybersecurity professionals, is a necessary step in qualitative analysis. Through these interviews, valuable insights into the complex aspects of Pakistan's cybercrime scene are gathered, enabling a more nuanced understanding of the opportunities and problems it faces. Through careful qualitative data collection through interviews and methodical analysis, this study aims to identify the underlying flaws in the current frameworks for law enforcement and legality and develop sound, workable alternatives to deal with them.

Data Analysis

When analyzing Pakistan's cybercrime legislation and enforcement protocols, qualitative research provides a sound foundation for comprehending the complex issues and possible resolutions. This study intends to shed light on the current state of cybercrime in Pakistan through in-depth interviews with important stakeholders, including law experts, law enforcement personnel, government officials, and cybersecurity professionals. The present data analysis explores the insights obtained from the qualitative interviews, with a particular emphasis on finding legislative and enforcement gaps and suggesting workable alternatives.

Perception of Current Cybercrime Laws:

- **Legal Experts:** An overwhelming 83% of legal professionals in Pakistan have expressed serious concerns about the effectiveness and adequacy of the current cybercrime legislation. Their main goal is to identify and highlight the ambiguities,

loopholes, and antiquated provisions in the existing legal system that make it more difficult for law enforcement to effectively combat cybercrimes. These experts have a strong background in dissecting the finer points of the law in order to find gaps and ambiguities that make it more difficult to prosecute and discourage cybercrimes. Through an examination of the intricacies of the legislation, they want to draw attention to important domains in need of enhancement, promoting changes that tackle contemporary cyber risks and conform to global norms. Legislators and policymakers entrusted with creating and modifying legislation to address the changing demands of cyberspace find great value in their knowledge and ideas. Legal experts are essential in influencing the legal environment to better shield people, companies, and institutions from the dangers of cybercrime by their careful analysis and critique of current legislation.

- **Law Enforcement Personnel:** The implementation of cybercrime legislation in Pakistan is significantly hindered by several obstacles, as shown by 80% of the participants acknowledging the difficulties stemming from inadequate specialized training, resources, and collaboration protocols with other agencies. The lack of specialized training impedes their ability to efficiently investigate and prosecute cyber offences, leaving them unprepared to traverse the complexities of digital crime scenes and cyber forensic examinations. In addition, their capacity to implement state-of-the-art technology and tools needed to counteract cyber threats in a rapidly evolving digital environment is further hampered by scarce resources. Moreover, insufficient collaboration protocols impede the coordination between different agencies, leading to fragmented endeavors and inefficiencies in combating cybercrime. In order to overcome these challenges, it is crucial to allocate resources towards implementing comprehensive training programs specifically designed to equip law enforcement professionals with the necessary expertise and understanding to successfully address cyber threats. Moreover, it is crucial to allocate adequate resources and build efficient collaboration channels between law enforcement agencies and relevant stakeholders in order to improve the overall response to cybercrime. Pakistan can enhance its law enforcement skills and effectively protect against the increasing threats posed by cybercriminal activity by tackling these concerns.

- **Government Officials:** 75% of government officials in Pakistan acknowledge the pressing need to implement legislative reforms in order to tackle the increasing cyber threats and improve law enforcement capabilities. This recognition emphasizes the urgent requirement for modernized legal structures that can adequately tackle the changing characteristics of cyber threats and equip law enforcement agencies with the essential resources and jurisdiction to effectively combat cybercrime. These officials probably view the current legal framework as insufficient in addressing cyber-crimes and may identify limitations in enforcement authority or jurisdictional uncertainties that impede successful prosecution. Government authorities demonstrate their dedication to adjusting to the swiftly evolving digital environment and guaranteeing that Pakistan possesses strong legal frameworks to prevent, identify, and prosecute cybercriminal acts by endorsing legislative modifications. Legislative reforms may involve several actions, such as the implementation of new laws against cybercrime, modifications to current legislation, and the establishment of mechanisms for improved collaboration and coordination among relevant parties. In essence, these endeavors seek to enhance the nation's ability to withstand cyber dangers and maintain the principles of law in the digital realm.

- **Cybersecurity Professionals:** 80% of cybersecurity specialists emphasize the vital importance of implementing comprehensive cybercrime law that aligns with international norms to effectively combat the constantly evolving cyber threats. This endorsement indicates their recognition of the global extent of cybercrime and the need for cohesive legal structures that facilitate cooperation and coordination across international borders. This Act aims to provide clear and specific definitions of cyber offences, establish appropriate legal frameworks for the investigation and prosecution of such offences, and define punishments that are commensurate with the severity of cyber-crimes. Moreover, by following to global standards, governments ensure compliance with defined methodologies and criteria, thereby enhancing their capacity to collaborate and share information in order to effectively address cross-border cyber threats. Cybersecurity experts exhibit their commitment to improving the legal structure for cybersecurity and promoting a globally coordinated approach to cyber threats through advocacy for comprehensive legislation on cybercrime. These specialists are probably knowledgeable about deficiencies or insufficiencies in existing legislation that hinder the efficacy of cybercrime prevention and enforcement. They comprehend the importance of legislation modifications in addressing these challenges. Cybersecurity professionals play a vital role in creating legislative frameworks that may effectively mitigate cyber threats and safeguard digital ecosystems, leveraging their expertise and advocacy.

Challenges in Enforcement Procedures:

- **Legal Experts:** Procedural challenges and bureaucratic constraints are identified by 78% of legal experts in Pakistan as major hindrances to the timely investigation and prosecution of cybercrimes. These hurdles involve a variety of problems, such as complex legal procedures, excessive administrative regulations, and ineffective procedures that hinder the progress of cybercrime investigations and court cases. Legal professionals are likely to face challenges while dealing with the legal regulations surrounding cybercrimes. These challenges may include dealing with multiple jurisdictions, complex rules for presenting evidence, and lengthy court processes. In addition, the bureaucratic obstacles, such as the time-consuming process of obtaining warrants or collecting cooperation from several government departments, worsen the difficulties encountered by legal practitioners in promptly resolving cybercrime cases. To overcome these challenges, it is necessary to simplify legal processes, improve collaboration between different government agencies, and introduce steps to enhance the effectiveness of the judicial system in dealing with cyber-related issues. Pakistan can bolster its ability to promptly address cyber threats and ensure fast prosecution of cybercriminals by surmounting procedural challenges and bureaucratic hurdles.

- **Law Enforcement Personnel:** A significant majority of law enforcement professionals in Pakistan, specifically 75%, identify multiple significant challenges faced during cybercrime investigations. The challenges encompass jurisdictional problems, a lack of expertise in digital forensics, and restricted collaboration from service providers. Jurisdictional obstacles develop as a result of the transnational nature of numerous cybercrimes, which complicate investigations involving various jurisdictions or international aspects. In addition, the absence of specialized digital forensic skills impairs law enforcement's capacity to efficiently gather, examine, and safeguard digital evidence that is crucial for prosecuting cybercriminals. In addition, the lack of cooperation from internet service providers and other technological businesses poses challenges in obtaining crucial data and information required for

investigations. To overcome these obstacles, it is necessary to foster collaboration among law enforcement agencies, government entities, and private sector parties. Training programs that are improved can enhance the digital forensic capabilities of police, while legal reforms can address the complications related to jurisdiction. In addition, establishing stronger collaborations with service providers through regulatory frameworks or incentivization procedures can enhance the exchange of information and cooperation. By tackling these concerns, law enforcement may more effectively manage the intricacies of cybercrime investigations and bolster their efficacy in combatting digital threats.

- **Government Officials:** In order to strengthen enforcement processes, eighty percent of Pakistani government officials stress the significance of interagency cooperation and capacity-building initiatives. This broad agreement is a reflection of the understanding that coordinated actions from various government departments and agencies are necessary to effectively respond to cyber threats. Interagency cooperation makes it easier to share information, coordinate resources, and work together on collaborative projects to combat the multifaceted nature of cybercrime. Authorities can more successfully detect, investigate, and prosecute cyber offenses by combining knowledge and resources from other industries. Furthermore, it is imperative that capacity-building initiatives, such training programs and skill development campaigns, give staff members the information and skills they need to handle the complexity of digital forensics and cybercrime investigations. In addition to increasing the country's overall resilience against cyber threats, strengthening enforcement procedures through interagency coordination and capacity-building also promotes a more unified and well-coordinated response framework amongst government agencies. Government representatives show their dedication to strengthening cybersecurity and defending national interests in an increasingly digital environment by giving these initiatives top priority.

- **Cybersecurity Professionals:** Ninety percent of Pakistani cybersecurity experts emphasize how crucial public-private partnerships (PPPs) are for exchanging threat intelligence and improving incident response skills. These collaborations make it easier for government agencies, businesses, and cybersecurity specialists to share resources, knowledge, and insights on cyber threats. PPPs offer more thorough threat information gathering, analysis, and distribution by utilizing the resources and experience of both the public and private sectors. This improves our collective ability to effectively detect and mitigate cyber threats. PPPs also encourage increased collaboration and coordination in incident response activities, which makes it possible to respond to cyber incidents more quickly and efficiently. PPPs improve the nation's overall cybersecurity posture by facilitating information sharing, cooperative exercises, and cooperative projects. This makes it possible to take a more proactive and coordinated approach to cyber defense. PPPs also encourage cooperation and trust among stakeholders, which makes it easier to develop creative fixes and best practices to deal with new cyber threats. Cybersecurity experts show their dedication to creating a safe and secure cyber ecosystem that can effectively withstand growing cyber threats by acknowledging the importance of public-private cooperation.

Proposed Solutions:

- **Legislative Reforms:** Eighty percent of those involved are in favor of comprehensive cybercrime laws being reformed and put into effect in Pakistan. These rules ought to define the precise behaviors that qualify as cybercrimes, address new risks that are appearing in the digital sphere, and provide suitable punishments for violators. Legislation that establishes unambiguous legal boundaries and penalties can aid in law enforcement, discourage cybercrime, and guarantee prompt and efficient prosecution of offenders. Comprehensive cybercrime laws can also be an essential instrument for defending people, companies, and vital infrastructure against the ever-increasing threat of cyber-attacks, strengthening the country's overall cybersecurity posture.

- **Capacity Building:** Seventy-five percent of stakeholders believe that skill development efforts and training programs are essential for Pakistani law enforcement professionals. They must complete these courses in order to advance their knowledge in digital forensics and cybercrime investigation. Law enforcement personnel that receive specialized training tailored to the unique challenges of cybercrime can acquire the necessary information, resources, and tactics to successfully battle digital offenses. Additionally, ongoing training ensures that law enforcement personnel remain knowledgeable about emerging threats and evolving investigative techniques, making them more effective adversaries of cybercriminals. Law enforcement can demonstrate its commitment to equipping people with the knowledge and skills needed to safeguard individuals, businesses, and critical infrastructure against cyber-attacks by sponsoring training and skill-building initiatives. This will help to create a more secure and safe online environment.

- **Inter-Agency Collaboration:** 85% of stakeholders in Pakistan support increased coordination and cooperation among different bodies to accelerate efforts in combatting cybercrime. This involves promoting cooperation among law enforcement agencies, the judiciary, government departments, and corporations in the commercial sector. Through the coordination of their endeavors and the exchange of knowledge and assets, these individuals or groups can establish a cohesive and collective defense against cyber-attacks. Improved coordination facilitates quicker response times, more effective investigations, and easier sharing of information, hence enhancing the overall efficacy of cybercrime prevention and enforcement endeavors. Furthermore, the cooperation between the public and commercial sectors enables the creation of all-encompassing plans and initiatives to tackle the intricate and ever-changing nature of cyber threats, ultimately enhancing the nation's ability to withstand and recover from cybersecurity risks.

- **Public Awareness and Education:** Seventy-seven percent of stakeholders in Pakistan strongly underline the critical importance of public awareness campaigns and educational activities. The purpose of these projects is to promote the adoption of cyber hygiene practices and raise awareness about legal responsibilities and cyber threats. By raising public awareness, these efforts empower individuals to take proactive steps to enhance cybersecurity, such as using strong passwords, regularly updating software, and exercising caution when sharing personal information online. Furthermore, disseminating knowledge to the general public regarding their legal obligations and the possible perils of cyber threats fosters a safer digital landscape and diminishes the prevalence of cybercrimes. Stakeholders may promote a stronger and more cyber-conscious society by launching targeted outreach efforts and educational programs that

provide individuals with the required information and skills to navigate the digital environment safely.

The data analysis unequivocally indicates that Pakistan faces significant challenges in terms of its cybercrime legislation and enforcement. Nevertheless, Pakistan has the opportunity to enhance its regulatory frameworks and enforcement procedures in order to efficiently counter cyber threats and safeguard its digital ecosystem. This may be achieved by addressing the identified deficiencies and implementing the recommended remedies. This research can serve as a valuable resource for policymakers, law enforcement agencies, and other interested parties to effectively prioritize and implement improvements and initiatives aimed at enhancing cybersecurity and protecting the rights of individuals in the digital age.

Conclusion

The examination of qualitative data highlights the urgent requirement for revisions in Pakistan's legislation and practices around cybercrime. Among many parties involved, there are widespread worries about the sufficiency and efficacy of existing legislation, and a general agreement is forming on the necessity of extensive legislative changes. The obstacles cited, which include procedural complications and resource limits, emphasize the complicated nature of addressing cyber threats. Nevertheless, within these difficulties, there are chances for enhancement, namely through programs that strengthen capabilities and promote better coordination among different agencies. Pakistan may enhance its cybercrime governance and reduce the risks associated with emerging threats by rectifying the identified shortcomings and implementing the suggested solutions. This research acts as a plea to policymakers, law enforcement agencies, and other parties involved to give priority and put into effect measures that aim to improve cybersecurity and protect the digital rights of persons in Pakistan.

Recommendations:

Legislative Revision: Pakistan's cybercrime laws need to be revised immediately in order to close the loopholes and uncertainties that have been found. To successfully deter cybercrime, this means passing thorough laws that specify particular cyber offenses, include clauses to address new risks, and specify suitable sanctions.

Capacity Building Initiatives: To improve law enforcement officers' competence in cybercrime investigation and digital forensics, it is imperative to fund training courses and other skill-building activities. Officers should receive specialized training to give them the skills and knowledge they need to effectively combat cyber threats.

Inter-Agency Collaboration: The judiciary, government agencies, businesses in the commercial sector, and law enforcement agencies should all work together more closely. Dedicated task forces and collaborative projects can speed up information exchange, simplify investigations, and increase the speed at which cybercrimes are responded to.

Public Awareness Campaigns: To encourage cyber hygiene practices and inform the public about legal requirements and cyber hazards, public awareness campaigns and educational programs should be started. Working together, the government, academic institutions, and civil society organizations can increase public awareness campaigns and provide citizens more tools to defend themselves online.

References

Akhlaq, M. (2021). Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan. PCL Student Journal of Law, 1, 31-66.

Akhtar, S. (2023). Assessing the Cybercrime Legislation in Pakistan: a Comparative Study of European Union and Pakistani Cybercrime Laws. Available at SSRN 4519368.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE access, 8, 137293-137311.

Anderez, D. O., Kanjo, E., Amnwar, A., Johnson, S., & Lucy, D. (2021). The rise of technology in crime prevention: Opportunities, challenges and practitioners perspectives. arXiv preprint arXiv:2102.04204.

Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. Časopis o društvenom i tehnološkom razvoju, 2(2).

Anwar, S. U., Wuyi, Z., Ali Shah, S. Z., Ullah, Q., Amir, S. M., & Syed, A. (2022). The resilient economic impact of CPEC and future of MNCs: Evidence from Pakistan. Frontiers in Environmental Science, 10, 912975.

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. Social Sciences, 12(11), 629.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society, 32(1), 103-124.

Engle, N. (2020). Computer Crimes. Am. Crim. L. Rev., 57, 459.

Hadi, M. J. (2024). Safeguarding Critical Infrastructures Through Data Protection Laws: A Comparative Study with a Focus on Pakistan. Available at SSRN 4730720.

Haider, W., Ali, A., & Zubair, M. (2023). Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan. Journal of Educational Research and Social Sciences Review (JERSSR), 3(2), 48-54.

Haq, I. U., & Zarkoon, S. M. (2023). Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan. Pakistan's Multidisciplinary Journal for Arts & Science, 43–62-43–62.

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of Cyber Threat Landscape and Readiness. IEEE access.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction: Routledge.

Jamshed, J., Rafique, W., Baig, K., & Ahmad, W. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. International Journal of Business and Economic Affairs, 7(1), 10-22.

Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. International Journal of Electronic Security and Digital Forensics, 14(2), 124-150.

Khan, M. F., Raza, A., & Naseer, N. (2021). Cyber security and challenges faced by Pakistan. Pakistan Journal of International Affairs, 4(4).

Khan, U. P., & Anwar, M. W. (2020). Cybersecurity in Pakistan: Regulations, Gaps and Way Forward.

Mirza, M. N., & Akram, M. S. (2022). 3-Cs of Cyberspace and Pakistan. Strategic Studies, 42(1), 62-80.

Nadeem, M. A., Liu, Z., Zulfiqar, S., Younis, A., & Xu, Y. (2021). Does corruption impede innovation in developing economies? Insights from Pakistan: a call for policies reforms. Crime, Law and Social Change, 75, 93-117.

Noor, A. (2021). Overview of Internet Content Regulations in Norway and Pakistan.

Obidimma, E., & Ishiguzo, R. O. (2023). Legal and Institutional Framework for Cybercrime Investigation and Prosecution in Nigeria: The Need to Strengthen the Existing Structures. IJOCLLEP, 5, 1.

Prasad, R., & Rohokale, V. (2020). Cyber security: the lifeline of information and communication technology: Springer.

Radoniewicz, F. (2022). International regulations of cybersecurity. Cybersecurity in Poland, 53.

Rakhmanova, E., & Pinkevich, T. (2020). Digital crime concept. Paper presented at the 2nd International Scientific and Practical Conference “Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth”(MTDE 2020).

Sabiri, M. N., & Sabiri, M. S. (2023). Cyber Security in Current Era in Pakistan: An Analysis of Cyber-Crimes and Cyber-Laws of Pakistan. Pakistan's Multidisciplinary Journal for Arts & Science, 4(02), 64-79.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

Saleem, H., Jan, J., & Areej, A. (2022). Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges. Society, Law and Policy Review, 1(1), 10-22.

Vitus, E. N. (2023). Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users—A Case of African States. Tijer-International Research Journal, 10(9), 975-989.

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age: John Wiley & Sons.