Pakistan Journal of Law, Analysis and Wisdom
Volume No. 3, Issue No. 8, August 2024
e-ISSN: 2959-0825, p-ISSN: 2959-0817
http://pjlaw.com.pk

Effects of Cybercrimes on the Criminal Justice System of Pakistan

Tayyab Shaheen
M.Phil Criminology, Minhaj University Lahore

Mian Muhammad Tariq Javed
Assistant Professor, College of Law, The University of Lahore

Dr. Muhammad Faisal Khan
Assistant Professor, School of Criminology, Minhaj University Lahore
(Corresponding Author) sardfaisal@gmail.com

Abstract

The objective of this study is to identify the effects of the cybercrimes on the existing criminal justice system of Pakistan. Cybercrimes have unique features and need a complete of investigation, trial and prosecution separately and different from the conventional one. The unseen burdens of the new crimes on criminal justice system slow down the performance of the system over all but also brought some latest technological advancement in the over parts of the criminal justice system. The study is qualitative in nature and based on the interviews of lawyers, judges, prosecutors, investigators and other related persons. The thematic analysis was used to carry out the results in this research. The study shows the tendency of cases is due to inefficiency of the stakeholders involved in the investigation, trial and prosecution.

Keywords: *Cybercrimes, Criminal Justice System, Effects, Pakistan*

1. Introduction:

Computer-mediated crimes conducted through global electronic networks are cybercrimes. Cybercrimes are the genuine preposterous and unpardonable behavior of cybercriminals which are spreading at an alarming rate all over the world including developing countries such as Pakistan. The life of human beings in every field, totally depends upon computers with the help of electronic networks. With the passage of time innovations are increasing day by day in the form of modernity but cybercrimes are also generating and getting added in numbers with high rates all over the world. But the legislative body of our country Pakistan is very slow and indolent for making cyber laws.

The impacts of cybercrimes on society, other institutions, performance of legal framework and recent developments in Pakistan. The causes of cybercrimes, the prevalence of cybercrimes, and the challenges of investigating and prosecuting cybercriminals. The need for global laws and legislation to combat cybercrimes and suggests ways to increase awareness and prevent

cybercrimes (Sattar, Riaz & Mian, 2018). Analyzing cyber harassment and victims of cybercrimes is crucial. Various types of cybercrimes affect victims. The legal framework, including the Electronic Crime Act, 2016, has limitations. Recent developments include the FIA's cybercrime branch and reporting website. Cybercrime poses challenges to Pakistan's criminal justice system, impacting operations, resources, and effectiveness. The rising number of cases burdens law enforcement, prosecutors, and courts. Dealing with complex evidence requires specialized skills and resources, straining the system.

The admissibility and use of digital evidence in Pakistan's legal system provides an overview of the current legal framework and highlights associated challenges. It targets legal professionals, policymakers, and researchers interested in the intersection of technology and the law. Digital evidence refers to binary data that can be admitted as proof in court. (Khan & Bhatti, 2023).

Crime is any action that goes against the law and is punishable by the legal system. According to "Black Stone", it's an act that breaks public laws, either by doing something forbidden or failing to do something required. Similarly, "Salin" defines crime as any behavior prohibited by law, with consequences like punishment. Cybercrime is when someone does something illegal using a computer or the internet. Usually, it's done by people who want to make money, but sometimes it's for other reasons like politics or personal grudges. Crime and cybercrime are both illegal activities, but they differ based on how they're done. Regular crime happens in the real world, like theft or fraud, while cybercrime involves using computers or the internet for illegal activities, like hacking or online fraud.

Both cyber and traditional crime having similarities because occur due act or omission which break the law. However, cybercrime is rapidly growing with different impacts on legal system of state. The internet is like a big mask for criminals. They can hide behind it to commit crimes that can hurt people all over the world. These crimes can damage economies, governments, and even how safe people feel. Basically, cybercrime is a super serious threat to everything from our money to our way of life (Gordon, & Ford, 2006). These intentional acts, termed cybercrimes, carry considerable ramifications for society, encompassing economic upheaval, emotional strain, and jeopardizing national security. Successfully addressing cybercrimes necessitates a thorough examination of their conduct and comprehension of their repercussions across societal dimensions. This manuscript endeavors to furnish perspectives on cybercrimes, their societal consequences, and forthcoming patterns within this realm (Saini, Rao, & Panda, 2012).

One important thing we noticed is that banks and other financial companies need to focus more on protecting their customers' trust and loyalty to reduce the risks of cybercrimes and keep their place in the market (Lagazio, Sherif, & Cushman, 2014). Unfortunately, criminals have also found opportunities for online fraud, leading to increased risks and threats. Securing cyberspace will enable safer online activities and positive outcomes (Jahankhani, Al-Nemrat, & Hosseinian-Far, 2014).

2. Review of Literature:

The evolution of computer-related crime, commonly known as cybercrime, dates to the nascent stages of computing technology. With the increasing integration of computers into societal frameworks, the scope of criminal activities linked to them has expanded accordingly. The historical narrative of computer crime mirrors the dynamic interplay between technology and illicit behavior. As technological advancements persist, cybercriminals innovate new tactics and strategies. Concurrently, cybersecurity measures and law enforcement endeavors evolve to counter these ever-changing threats within the digital realm (Schjolberg, 2014).

Investigation and assertions are pivotal in the formulation of theories, serving as the cornerstone of theoretical frameworks by furnishing the requisite methodologies and logical approaches tailored to specific scenarios. Research serves as a vital instrument for refining and enhancing prevailing theories, thereby ensuring their continued relevance and efficacy (Leukfeldt & Yar, 2016).

Exploring theories of cybercrime is integral to comprehending the incentives, actions, and origins behind illicit conduct within the digital sphere. These theories furnish a structure for scrutinizing and elucidating the rationales behind the involvement of individuals and collectives in cybercriminal endeavors (Ngo & Paternoster, 2011).

Pratt & Reisig (2010) Routine Activity Theory is a crucial framework for examining and evaluating crimes, focusing on the mental state of offenders rather than their remorse. It aids in formulating policies and strategies for preventive measures, aiming to alter elements that increase crime risk, ultimately aiding in crime prevention.

Cybercrimes are rising with the passage of time and more due to the innovations or advancement in technology. But gradually many challenges are taking place against cybercrime in Pakistan like cyber terrorism, cyber threats, hacking, child pornography, internet or computer viruses, online financial frauds including cyber wars in the cyber world. Addressing these issues requires robust

prevention measures, increased awareness, enhanced cybersecurity practices, and effective law enforcement to ensure a safer digital environment in Pakistan (Anjum, 2020).

With technological advancements, safeguarding against cyber threats has become increasingly critical for national security. Incidents of data breaches have become alarmingly frequent, fueled by the expanding business landscape and evolving global information security regulations. The study explores cybersecurity concerns, obstacles, risks, attacks, and research directions. It categorizes cyber tactics into five classes and identifies six significant challenges impacting organizations, businesses, and governments. The study examines cybersecurity strategies in Germany, the UK, and the USA, providing guidance for researchers, strategists, scientists, technologists, and organizations to develop innovative tools and methodologies to address these pressing challenges (Schia, 2018).

The rapid growth of Information and Communication Technologies (ICTs) has increased cyber threats to Pakistan's security, but the country's cyber readiness is inadequate. The Securitization Theory from the Copenhagen School is used to examine Pakistan's cyber landscape, highlighting the importance of cybersecurity preparedness in mitigating vulnerabilities and enhancing cyber productivity. Key concepts like cyberspace, threats, cyber-attacks, critical infrastructure, and cybersecurity are explored (Broadhurst & Chantler, 2006).

The rise of cybercrime in Pakistan underscores the urgent need for robust legislation to combat it effectively. Additionally, law enforcement agencies encounter significant hurdles in addressing cybercrimes, including their intricate nature and the scarcity of skilled investigators. Addressing these challenges requires initiatives to raise public awareness about cybercrimes, enact stringent laws to deter perpetrators, and establish specialized bodies such as the National Response Centre for Cyber Crimes (NR3C) to tackle cyber threats. Furthermore, there’s a call for online consumer protection laws and measures to curb illicit online transactions (Usman, 2017).

The proliferation of internet usage has transformed organizations into predominantly virtual entities, facilitating remote work, global reach, and digital cooperation. This shift offers advantages like heightened productivity and innovation fueled by technology-driven connectivity. However, it also presents hurdles such as cybersecurity threats and concerns over data privacy. Organizations must navigate this virtual environment, leveraging its benefits while ensuring effective communication and mitigating risks effectively (Arachchilage & Love, 2014).

3. Methodology:

Qualitative research technique used in the research. The research approach allowed for a comprehensive exploration of the research questions and provide a deeper understanding of the experiences, perceptions, and challenges faced by various stakeholders and prevalent cybercrimes, their impacts on criminal justice system.

The population included the officials of FIA, judges and prosecutors of cybercriminal trial courts, cybercrime investigation officers, cybercrime technical officers, lawyers of cybercriminal trials and cybercrime victims. Only two cyber courts are in Lahore, two judges and two prosecutors are in both therefore population size is calculated as four (4) and sample is 25. To collect the representative unit of the population the sampling technique was purposive and only researched where our purposeful respondents were available. The interview guide was used as a data collection tool. Data was collected through primary and secondary sources. Direct interviews were used as primary source while documents, archival materials and records etc were used as secondary source. Thematic analysis used in the research study. The analysis was involve several steps, including data familiarization, coding, categorization, and interpretation.

4. Results and Discussions

4.1 Analysis Derived from Narrative Data Provided by F.I.A Directors and Deputy Director

Officials Interviewed	Analysis of the Responses of the Respondents
F.I.A Directors and Deputy Director	• The growing threat of identity theft and ransomware attacks on individuals and businesses is a result of evolving cybercriminal tactics. • Social engineering tactics, such as impersonation and manipulation, are frequently employed to highlight the human element in cybercrimes. • The rapid evolution of cyber threats necessitates continuous updates in investigative methods and tools. • The data reveals that the anonymity provided by the online environment significantly hinders the identification and capture of cyber offenders.

	• The lack of technology and skilled personnel resources is a significant obstacle in conducting effective cybercrime investigations. • The lack of technology and skilled personnel resources is a significant obstacle in conducting effective cybercrime investigations. • Advancements in digital forensics and dedicated cybercrime units are beneficial, providing adequate resources for addressing evolving cyber threats. • The focus is on investing in advanced tools, forming partnerships with the private sector, and expanding training programs for enhanced performance. • The data highlights the need for specialized forensic expertise in the dynamic digital evidence landscape, the importance of continuous adaptation of investigative techniques, and the global nature of cybercrimes necessitating international collaboration
Cyber Investigation Officers	• The investigator has observed a significant rise in financial fraud, primarily through phishing and online scams, indicating a growing sophistication in cybercriminal tactics. • The scenario depicts a shift towards cybercriminals targeting individuals and organizations, highlighting the widespread impact of cybercrimes. • The use of social engineering tactics, such as impersonation and manipulation, complicates investigations and underscores the need for a comprehensive response. • The continuous evolution of cyber threats necessitates continuous updates in investigative methodologies and tools, emphasizing the fluid threat landscape. • The anonymity of the online world significantly complicates the process of identifying and apprehending cybercriminals.

	• Cross-border cybercrimes present jurisdictional challenges, necessitating international cooperation and highlighting the global aspect of cyber threats. • The text emphasizes the significance of specialized forensic skills in gathering digital evidence due to its dynamic nature. • The rapid advancement of technology necessitates the continuous adaptation of investigative methods to address the challenges in evidence collection. • Legal frameworks may not keep up with technological advancements, emphasizing the necessity for timely legislative changes. • The global nature of cybercrimes presents jurisdictional challenges that underscore the importance of international collaboration and coordination.
Cyber Lawyers and Prosecutors	• The attorney acknowledges the widespread cybercrimes in Pakistan, particularly financial fraud, which is a significant issue through phishing and online scams. • The increasing sophistication of cybercriminal activities, including identity theft, ransomware attacks, and unauthorized access, necessitates increased awareness among legal practitioners. • Legal professionals must remain vigilant and adapt to changing trends in cybercrimes due to the evolving digital landscape. • The attorney faces significant challenges due to the rapid evolution of cyber threats, emphasizing the need for continuous updates in legal strategies and understanding. • The online anonymity presents a persistent challenge in identifying and prosecuting cyber offenders due to its complexity. • Legal professionals must swiftly adapt to the ever-changing landscape of technology, emphasizing the necessity of bridging the gap between legal processes and technological advancements.

	• The evaluation of existing laws reveals strengths and areas for improvement, as the legal framework has evolved to tackle specific cybercrimes, but identified gaps still need attention. • The call for laws to be more responsive to rapid technological changes and cybercriminal tactics acknowledges the dynamic nature of cyber threats. • The legal system's effectiveness in addressing cybercrimes is being enhanced through continuous updates, amendments, and streamlined evidence collection procedures. • The representation of cybercrime victims faces challenges due to the intricate nature of digital evidence, necessitating the expertise of legal professionals.

References

Adams, P. C. (1997). Cyberspace and virtual places. *Geographical Review*, *87*(2), 155-171.

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118-131.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47-88.

Agnew, R., Brezina, T., Wright, J. P., & Cullen, F. T. (2002). Strain, personality traits, and delinquency: Extending general strain theory. *Criminology*, *40*(1), 43-72.

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

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3-13.

Bazeley, P. (2003). Defining'early career'in research. *Higher Education*, *45*(3), 257-279.

Bennett, W. W., & Hess, K. M. (2007). *Criminal investigation*. Wadsworth/Thomson Learning.

Bernat, F. P., & Godlove, N. (2012). Understanding 21st century cybercrime for the 'common'victim: *Criminal Justice Matters*, *89*(1), 4-5.

Chess, D. M., & White, S. R. (2000, September). An undetectable computer virus. In *Proceedings of virus bulletin conference* (Vol. 5, No. 4, pp. 409-422).

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security*, *30*(8), 719-731.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society*, *19*(3), 355-375.

Loader, B. D., & Thomas, D. (Eds.). (2013). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology*, *11*(1).

Malik, M. S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, 26(1), 50-60.