Contemporary Issues in Social Sciences and Management Practices (CISSMP)
ISSN: 2959-1023
Volume 2, Issue 4, December, 2023, Pages 207-222
Journal DOI: 10.61503
Journal Homepage: https://www.cissmp.com

Exploring the Interplay of Cybersecurity and cybercrime in Pakistan's Digital Landscape

Mudasar Ali Nadeem[1], Sumaira Hashmi[2] & Muhammad Abbas Khan[3]

[1]Lecturer Sociology Government College University Faisalabad Chiniot Campus, Pakistan
[2]Visiting lecturer, Department of Sociology, Thal university Bhakkar
[3]Scholar, LLB, University Law College, University of the Punjab Lahore

Article History:

Received:	Aug	14, 2023
Revised:	Sept	22, 2023
Accepted:	Oct	23, 2023
Available Online:	Dec	30, 2023

Keywords: Dividend payout decisions, Profitability, Earning per share, Pakistan Stock Exchange, Pakistani Context, Free Cash Flow.

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

This study delves into the intricate dynamics between cybersecurity and cybercrime in Pakistan's rapidly advancing digital landscape. As the nation witnesses technological progress and heightened connectivity, the interaction between these two forces becomes pivotal. The research assesses the current state of cybersecurity measures employed by individuals, businesses, and government entities, evaluating their efficacy against the escalating wave of cyber threats. Concurrently, it investigates the tactics employed by cybercriminals, analyzing the nature and scope of prevalent cyber threats in Pakistan. The research involves an in-depth examination of cybersecurity measures and cyber threats in Pakistan. It employs a multi-faceted approach, including surveys, interviews, and data analysis, to comprehensively understand the evolving digital security landscape. The findings highlight the complex and diverse cybersecurity environment in Pakistan, shaped by the convergence of technology, government, and international connections. The research underscores the changing nature of cyber threats and their substantial impact on political stability, emphasizing the necessity for robust cybersecurity measures. This study contributes valuable insights into the evolving intersection of cybersecurity and cybercrime in Pakistan. It takes into account the historical context, societal challenges, and technological advancements, providing a nuanced understanding of the complex digital security landscape.

Corresponding Author's Email: mabbasghafoor224@gmail.com
DOI: https://doi.org/10.61503/cissmp.v2i4.94

Citation: Mudasar Ali Nadeem, Sumaira Hashmi & Muhammad Abbas Khan (2023). Exploring the Interplay of Cybersecurity and cybercrime in Pakistan's Digital Landscape. *Contemporary Issues in Social Sciences and Management Practices, 2*(4), 207-222.

Introduction

A few years ago, Dr. Fasihuddin, a prominent criminologist in Pakistan, noted that criminology does not get the recognition it deserves as a field of study in the country. Fasihuddin ascribed the lack of interest in criminology and the study of Pakistan's criminal justice system to the colonial history of the country, during which it was under British authority, similar to India. Nevertheless, in 1947, with India's attainment of independence, the nation was divided into India and the Dominion of Pakistan (Khan 2019). Pakistan has faced several challenges in the form of societal instability and elevated crime rates since achieving independence. Despite a modest decrease in violent crime from 2011 to 2016, Pakistan still has the 10th highest position in terms of total crime rate globally. Pakistan was listed as the third-most impoverished nation in the world by the World Bank, with around 75.4% of its population living on less than $5.50 US per day. According to Transparency International's Corruption Perceptions Index, Pakistan was the 117th least corrupt nation out of 175 countries in 2018. This marks a significant improvement from its previous ranking of 143rd in 2010 (Ashraf, König et al., 2023).

This delves into a comprehensive exploration of the complex terrain of cybersecurity in politics. We want to analyze the intricate relationship between technology, governance, and international relations in order to understand the intricacies of this field. We are doing a comprehensive examination that goes beyond just exploring cyberattacks. It extensively explores their changing characteristics and the resulting influence on political stability (Haque, Abbasi et al., 2023). Furthermore, this also reveals the tactical methods used to strengthen digital resilience, guaranteeing the integrity of political systems in the midst of increasing difficulties.

This research aims to shed light on the complex interplay of technological vulnerabilities, geopolitical dynamics, and ethical considerations that form the foundation of the constantly evolving field of cyber security in politics. It draws on real-world case studies, policy frameworks, and collaborative initiatives. As we explore the impact of cyber security on molding global political discourse, it becomes clear that our efforts go beyond technical limits (Rasool 2015). Our investigation has the capacity to protect the stability, credibility, and integrity of political institutions worldwide. This paper presents a method for comprehending the complex relationship between technology, governance, and international relations in the realm of cybersecurity in politics. While prior studies have mostly concentrated on the technical elements of cyberattacks, our inquiry adopts a comprehensive perspective that goes beyond the traditional limits of cybersecurity discussion. We explore the dynamic interaction of these three crucial variables to uncover the inherent complexity present in this field (Baker 2014).

Amis and Objectives Analysis, etc.

- Inclusive knowledge of cyber crime
- Analyze the criminal justice system and cyber law in Pakistan.
- Recognize key challenges in combating cybercrimes.
- Explore the impact of technology on advancements in cybercriminology.

2.0 Literature Review

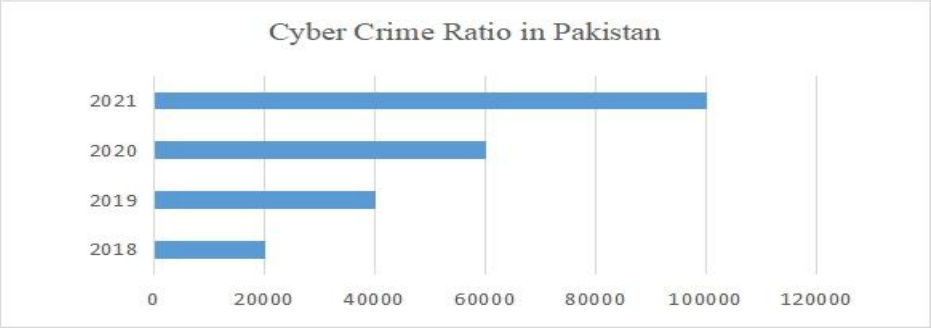
In Pakistan, where there is a large population of young people and a wide range of social

media platforms, it is crucial to understand how information is shared. The widespread availability of information has led to a population that is often oblivious of the origins and accuracy of the information they consume or share. The result is an unstable setting where inadequate or inaccurate information may cause individual conflicts, therefore unintentionally deceiving others. The rise of information culture in Pakistan poses a perplexing situation similar to an unmanned vehicle transporting information without defined sources or destinations. Contemporary technology, such as mobile phones and computers, seemingly streamline life, yet their less apparent repercussions are complex and diverse. The inadvertent dependence on data sourced from websites and social media platforms has inadvertently facilitated the emergence of a new kind of conflict, known as third-generation warfare, which is distinguished by the manipulation of information and the promotion of division. The essence of this conflict is in its intangible characteristics; it is a struggle of perspectives, storytelling, and manipulation resembling an imperceptible opponent.

2.1 The Geneses of Cybercrime

A group known as "Phreakers" arose during the 1970s in the United States. They would engage in criminal activities via the use of cellphones. John Draper was a renowned member of the ensemble. This organization aims to reproduce the frequencies used for telecommunication in the United States and provide the service of making complimentary telephone calls. According to several academics, the genesis and inception of cybercrime are intertwined with ARPANET (Advance Research Projects Agency Network). The project was financed by the US Department of Defense (Kabay 2012). The primary objective was to provide secure communication channels for military applications. Using the same method, communications may be segmented into packets and then reconstructed in their original form. The word "hacking" gained practical recognition when a group of highly proficient computer programmers began targeting telephones in the communications industry. The collective of very proficient computer programmers was often referred to as phreaks. They managed to illicitly infiltrate the system and discovered several methods to make free calls (Steinmetz 2016).

2.2 Cybercrime in Pakistan



The Internet became accessible to the public in the 1990s. Pakistan is among the nations with the highest number of internet users. The Internet has facilitated daily tasks and reduced time consumption. However, it has also spawned several criminal activities such as theft, fraud, child pornography, and extortion. In Pakistan, the Internet is often misused, with a significant portion

of its use being dedicated to engaging in illegal and illicit activities. Approximately 7,500,000 individuals were claimed to have used the Internet in Pakistan during the year 2004. In the past, we lacked a systematic approach and specialized knowledge for investigating cybercrime. There was a lack of established protocol, resulting in frequent release of the criminals (Ali, Malik et al. 2019). The government created a National Response Center for Cybercrime, which operates under the supervision of the Federal Investigation Agency (FIA). The primary objective of its formation was to prevent the abuse of the internet. This agency has the requisite knowledge and skills to handle matters related to cyber security, cyber fraud, technical investigation, and digital forensics. The first instance of cybercrime in Pakistan was recorded in 2003(Khan and Anwar 2020). A group of five individuals from Pakistan engaged in a commercial enterprise centered on the import and export of goods, using fraudulent information and exploiting credit cards. According to the FIA estimates, 65% of cybercrimes, including as blackmailing and harassment of women, occur on Facebook. The bulk of these incidents are reported in Karachi. The Karachi cyber wing gets around 20 daily reports pertaining to cybercrime. A total of around 5500 cybercrime instances were registered in Lahore in the year 2018 (LA VALORACIÓN, ÁMBITO et al. 2021).

These included various forms of misconduct such as harassment, blackmail, stalking, privacy infringement, impersonation, and fraud. Below is a concise overview of the cybercrimes recorded in Pakistan in recent years.

Year	Numbers of Inquiries Conducted	Number of case Registered	Number of arrests made
2016	514	47	49
2017	1290	207	160
2018	20295	255	209

It is essential to establish a dedicated court for cybercrimes and augment the number of cybercrime specialists. State-of-the-art methods are necessary to address the prevailing crime rate issue. The Prevention of Electronic Crimes Act was enacted in 2016 (Saleem, Jan et al. 2022).

2.3 Some Categories of Cyber Crime

i. Hacking
ii. Serious and organized Cybercrime
iii. Cyberterrorism
iv. Cyberwarfare

Cyber intrusion Hacking, which refers to the unauthorized access to computer systems with the intention of causing harm, disruption, or engaging in unlawful activities, is the primary and prevalent kind of cyber threats. There is a range of hackers that differ in terms of their motive and level of experience. Hackers may engage in hacking activities for many reasons, such as amusement, minor larceny, or seeking retribution. Alternatively, they may be driven by ideological or political motives, either on a domestic or global scale. Regarding their goals, hackers may be

categorized as those who engage in hacking for personal or activist reasons, those who do so for criminal intent, or those who are backed by governmental entities (Usman 2017). Due to its lack of organization and limited impact, hacking poses a far lower danger compared to other more severe cyber threats. However, it is seen as a significant hazard not only because it may greatly disturb those impacted, but also because it can result in more severe cyber threats such as major cybercrime and cyber warfare. Although the operations of the hackers listed above are relevant to Pakistan, the Indian hackers, who are seemingly operating with the support and guidance of the Indian government, provide a significant problem. Since 1998, the Indian hackers have consistently targeted the websites of the Pakistani government and security services, mostly using Denial-of-Service (DoS) assaults (Khan, Raza et al. 2021). Between 1999 and 2008, Indian hackers attacked 1600 Pakistani websites, as reported. The occurrence has increased in frequency and organization after the establishment of the Indian Cyber Army (ICA) consisting of software experts in August 2010. The gang successfully breached the security of around 36 websites in Pakistan, which included the websites of NADRA, National Accountability Bureau (NAB), Pakistan Navy, and the ministries of finance, foreign affairs, and education. In 2013, a Norwegian cybersecurity company disclosed that Indian hackers have been engaged in an espionage operation known as 'Operation Hangover' against Pakistan since 2010. The company said that the hackers specifically targeted high-ranking executives of both business and government organizations (Khan, Raza et al. 2021).

Cybercrime Category	Percentage/Ratio	Platform Use for Attempt of Crime
Financial fraud	23%	Mobile, social media ATM's and online banking
Identity theft	11%	Facebook and other media
Harassment	11%	Mobile Facebook
Hacking	11%	Social media platform

2.4 Cybercrime and Contemporary Challenges

Two significant obstacles in understanding cybercrime activities are a lack of knowledge and a deficient culture of cyber security, both at the individual and corporate levels. There is a lack of skilled and capable personnel available to carry out the security measures. Furthermore, there is no specific regulation regarding email accounts, especially for the military forces, police department, and security staff. Furthermore, there have been reports of cyber-attacks originating not just from terrorist groups but also from a neighboring state that is in opposition with our national interests. Moreover, basic requirements for entering the police force do not include any expertise related to the field of computer science. Consequently, their knowledge of cyber-crime is often lacking (Baezner 2018).

The rapid pace of advancements in cyber technology sometimes outpaces the progress of the government sector. Consequently, they are unable to identify the origin of these cyber offenses. The progress in Research & Development pertaining to ICTs is rather inadequate. The security forces and law enforcement personnel lack the necessary armament to combat sophisticated criminal activity. The existing procedures are insufficient in autonomously determining the accountability of authorities in relation to globally committed crimes. Furthermore, the government's allocation of funds for security measures, namely for the training of law enforcement personnel, security personnel, and ICT detectives, is significantly inadequate compared to other types of crimes (Zahoor, Razi et al. 2020).

2.5 Criminal Justice system in Cybercrime

The genesis of Pakistan's legislative system pertaining to cyberspace may be traced back to the Constitution of Pakistan, 1973, which does not explicitly mention information technology or cyberspace. However, it enumerates the legislation items in the Federal Legislative List, which are specified in the Fourth Schedule of the Constitution. These legislative powers are granted to the Federation in relation to communications, copyright, inventions and designs, international treaties and conventions, the State Bank of Pakistan (including e-banking and e-commerce mechanisms), and insurance law. Regarding criminal matters, the validity of the powers of the Federation in Pakistan is based on articles 142 and 143 of the Constitution (Usman 2017). These articles provide that criminal legislation, criminal process, and the law of evidence are jointly the duty of both the Federation and the Provinces. Utilizing this constitutional framework, the Federation has enacted many legislations pertaining to cyberspace. The primary legislations in question are: The Federal Investigation Act of 1974, the Pakistan Telecommunication Act of 1996, and the Prevention of Electronic Crimes Act of 2016. This outline serves as an introduction to provide fundamental information for any in-depth investigation on the topic; each law is being briefly examined (Razi and Zahoor 2021).

2.6 The Federal Investigation Agency Act, 1974

The Federal Investigation Agency (FIA) is the primary federal law enforcement agency established by the Federal Investigation Agency Act, 1974. In Pakistan, the Federal Government is responsible for overseeing various police legislation, while the Director General, who has the authority of an Inspector General of Police, is in charge of its administration. The powers vested in members of the FIA are equivalent to those of Provincial Police officials in terms of apprehending individuals and confiscating assets, which they are authorized to execute over the whole territory of Pakistan (Bhatti, Adnan et al. 2021). The field units consist of geographical and functional directorates, each led by police officers holding the rank of Deputy Inspector General of Police. Each directorate is further comprised of police stations. Every police station, including provincial police stations, is overseen by Station House Officers. The SHOs are of equal or higher status than Sub-Inspectors of Police. At the conclusion of the Act, there is a Schedule that enumerates the offenses and laws that come under the jurisdiction of the FIA. The FIA primarily focuses on addressing critical issues such as people smuggling, trafficking in persons, immigration, cybercrimes, official secrets legislation, corporate crimes, money laundering, counter terrorist

funding, and high treason (Haider, Ali et al. 2023).

From the perspective of cybercrimes, it is the primary and only authorized agency responsible for investigating offenses pertaining to computers, the internet, and the illicit use of information technology. The organization has the authority to commence legal proceedings based on extraterritorial jurisdiction in criminal cases, so establishing itself as a significant entity within the country's national security framework, particularly with regard to internal security. The FIA's authority to operate across borders is enhanced by its ability to establish a National Central Bureau (NCB) that exclusively collaborates with INTERPOL, the International Police Organization. With the growing prevalence of the rule of law strategy in combating terrorists and cybercrimes, the FIA's significance as a primary organization in addressing inter-provincial and international organized crime is becoming more prominent (Mukhtar 2018).

2.7 The Prevention of Electronic Crimes Act, 2016

The Prevention of Electronic Crimes Act, 2016 (PECA) is the primary legislation that addresses cybercrimes in Pakistan. It encompasses many behaviors that occur in cyberspace and include digital technologies, making them illegal. Overall, the law has established twenty-three offenses, encompassing activities such as unauthorized access and interference with data, disruption of critical infrastructure, glorification of cybercrimes, cyber terrorism, hate speech online, electronic forgery, electronic fraud, unauthorized use of someone else's identity, unauthorized interception, offenses against the dignity and modesty of individuals, child pornography, cyber stalking, spamming, and spoofing (Haq, Zarkoon et al. 2023). Among these twenty-three offenses, only three offenses are cognizable according to section 43. This implies that legal action can only be taken for these three offenses through a judicial order. In practice, this affects the legal rights of individuals who seek assistance from executive authorities or the police to address their grievances. PECA encompasses not only criminal substantive law, but also procedural and regulatory aspects. Regarding criminal procedure, it specifies that only an authorized investigative agency is permitted to probe cybercrimes. The Prevention of Electronic Crimes Investigation Rules, 2018, which were established under section 51 of the Prevention of Electronic Crimes Act (PECA), provide exclusive authority to the Federal Investigation Agency (FIA) to conduct investigations related to cybercrimes (Akhlaq 2021).

The lack of permission for provincial police organizations is expected to undergo revision owing to the widespread occurrence of cybercrimes and the use of digital gadgets in various criminal activities. It is worth mentioning that the PECA has a comprehensive section on precautionary measures, which include the authority of the Federal Government to provide instructions to owners of information systems and the establishment of Computer Emergency Response Team(s) (CERT). The PECA also includes provisions for the issuing of search and seizure warrants and warrants for the disclosure of content data. It also requires service providers to promptly maintain and deliver data and information to authorized police officials. The legislation provides a comprehensive protocol that authorized officers must follow when seizing data (Nashit 2019). The PEC Rules mandate the establishment of a Cybercrime Wing inside the FIA, which must consist of a dedicated division for cybercrime investigations, a department for

forensics, and a section for data and network security. The PEC Rules also provide a framework for cybercrime complaints register to effectively address the grievances of people. Additionally, these Rules include provisions for the instruction of Cyber Wing officers and outline the protocol for transferring cybercrime investigations. The Rules elaborate on the protocol of international collaboration with INTERPOL and on the fundamental principles and ethics that authorized officers must follow while carrying out investigations, particularly in relation to safeguarding victim confidentiality and ensuring witness protection (Akram, Abdullah et al. 2011).

Some Offences and Punishments in Electronic Crimes Act 2016

Offence	Punishments (Years)	Fine (Rs.)
Unofficial access to information system data.	3 months	50,000
Unofficial access to critical infrastructure information system or data.	3	1,000,000
Unofficial copying of critical infrastructure data.	5	5,000,000
Adoration of an offense	7	10,000,000
Cyber terrorism	14	50,000,000
Unofficial use of identity information	3	5,000,000
Unauthorized issuance of sim cards.	3 months	500,000

In terms of cyber security, the current situation in Pakistan not only demonstrates the extent of its susceptibility to cyber-attacks, but also reveals the inadequacy of its preparedness, namely in terms of law, policy, and execution, to effectively address these threats. Given the external and internal security issues, Pakistan's inadequate readiness in cyber security renders it susceptible to a wide range of cyber-attacks (MANZAR, TANVEER et al. 2016).

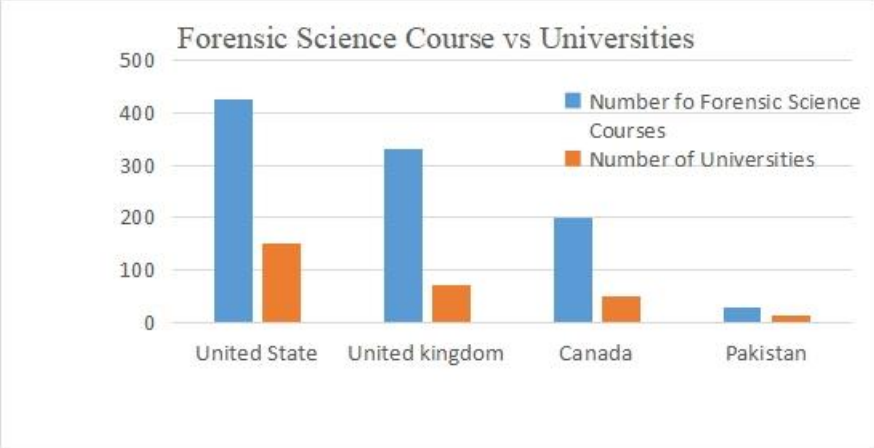
2.8 Serious and Organized Cybercrimes

As financial and commercial activities become more digitalized, organized and competent criminals are more drawn to cybercrime. Black market networks, like Dark Market, are involved in a range of cybercrimes including theft, the purchase and sale of personal data from bank accounts, credit cards, identification numbers, and passwords, as well as the trafficking of botnets. With the transition of traditional organized crime to the digital realm, Cybercrime in Pakistan is on the increase due to the growing popularity of e-banking and e-government. On a regular basis, the nation confronts instances of cybercrime, including a wide spectrum of activities such as unauthorized access to accounts, as well as illicit and unlawful actions like unauthorized cash withdrawals or money transfers (Khan, Raza et al. 2021).

The National Response Centre for Cyber Crimes, which is the cybercrime division of the

Federal Investigation Agency (FIA), recorded a total of 2019 complaints in 2017. These complaints may be categorized into three primary groups. Out of the total number of reported cases, 76 percent (1592 cases) were connected to harassment, defamation, and blackmailing via social media. Financial fraud accounted for 14 percent (307 cases), threatening calls accounted for 5 percent (116 cases), and email hacking accounted for 186 cases. It is crucial to emphasize that there are still many unreported occurrences owing to a lack of understanding about cyber laws or a lack of faith in law enforcement institutions (Akhtar 2023). Based on the aforementioned list, it seems that the financial industry is more susceptible to significant cybercrimes. In late 2017, Habib Bank Limited (HBL) had a significant cybercrime incident when skimming devices were used to target their ATM facilities. This led to an unauthorized breach into 579 accounts and a loss of Rs.10 million. In both 2015 and 2016, the bank was targeted by cyber-attacks. It is crucial to emphasize the two prevalent forms of cybercrime that are now increasing in frequency - computer hacking and phishing/email scams. Using these methods, cybercriminals infiltrate a computer network and pilfer personal or private information, allowing them to engage in fraudulent operations (Shad 2019).

2.9 Digital Forensics and Criminal Investigations



At first, when the Prevention of Electronic Crimes Act (PECA) was established in 2016, the only authority to investigate electronic crimes was granted to the Federal Investigation Agency (FIA). However, in order to acknowledge the extensive prevalence of digital evidence in many criminal activities, the Criminal Laws (Amendment) Act of 2023 broadened this jurisdiction. Provincial police are now authorized to file charges pertaining to these offenses under PECA. This alteration shows the growing significance of digital evidence in contemporary criminal proceedings. The 2023 modifications to the Prevention of Electronic Crimes Act (PECA) have included additional offenses in sections 22-A, 22-B, 22-C, and 24-A. These offenses pertain to activities such as online grooming, cyber incitement, and child exploitation (Haque, Abbasi et al. 2023).

Furthermore, the act of encouraging terrorism/extremism, engaging in communication for the purpose of money laundering, and providing financial support for terrorism using modern technologies such as crypto-currency and smart contracts, predominantly relies on electronic

methods. This necessitates the gathering, safeguarding, and analysis of digital evidence through the practice of digital forensics (u Salam, Arif et al. 2022).

2.10 Forensic science courses in developed countries and Pakistan.

Forensic science courses, including those focusing on cybercrime, demonstrate unique characteristics in both developed nations and Pakistan. In affluent nations such as the United States, university programs are often strong and thorough, including specific courses in digital forensics and cybersecurity. These programs emphasize practical skills by include hands-on laboratories and real-world case studies, while also embracing legal issues to equip students for the intricacies of cybercrime investigations. Nevertheless, there might be disparities in the quality of programs between various schools (Shoro, Syed et al. 2020). Well-established courses in the United Kingdom prioritize both technical and legal elements, capitalizing on strong industry contacts to provide students significant real-world experiences. Canada is seeing an increasing focus on cybersecurity education, with programs being designed to correlate with professional qualifications in order to improve practical applicability. Although there are positives, there are also disadvantages, such as the scarcity of specialized programs in some areas. Conversely, Pakistan has implemented many measures to tackle cyber threats, such as establishing the National Response Center for Cyber Crimes (NR3C), implementing the National Cyber Security Policy (NCSP), and enacting the Electronic Crime Bill. The emphasis is placed on prominent public awareness initiatives and partnerships with international organizations. (Haque, Abbasi et al. 2023)

3.0 Cyber Threats and Ethics

The spectrum of cyber threats, including anything from malfeasance to warfare, is very diverse, and their patterns are intricate and hard to delineate. Tracing the path of these crimes is a formidable task. The process of collecting and collaborating delta connected to cyber-crime in order to find the appropriate path is known to include several complications. Cyber hazards may physically affect both the premises and software, which are crucial components of cyber-crime. Therefore, special attention should be paid to software in this regard. Cyber-crime, extremism, and warfare sometimes use vulnerabilities in core technology for their own advantage. The existence of these vulnerabilities is attributed to the fact that they are not deemed unlawful, since they are only software faults that have been disregarded in the discourse around cybersecurity (Shad 2019).

Perform a search Examine the significance of technology in the context of deep fake. The researcher discussed the creation of fake pornography through the use of dark technology, specifically deep fake videos. These videos are being employed to defame and ruin the online reputation of individuals, posing significant challenges in addressing these malicious actions. This resulted in several issues for celebrities, particularly concerning their privacy, which raises a significant ethical dilemma about cyber technology (Jamshed, Rafique et al. 2022). This prompts contemplation on the fundamental cause of human transgression and behavior: is it inherent nature or is it shaped by cultural influences, often referred to as nurture. Is it necessary to address the topic of developing cyber ethics in response to obtaining knowledge on individuals who harm others via the use of cyber technology, with the aim of implementing these ethics to avoid cybercrimes (Sharf, Akhtar et al. 2020).

Al-Fasfus (2020) performed research that highlights the significant influence of debt, free cash flow, and viability on the dividend payout ratio within the Jordanian banking sector. The research by Trong and Nguyen (2020) demonstrates the significant influence of improved stock liquidity on a company's decision-making regarding dividend allocation. Furthermore, there is a correlation between higher dividend payments and less volatility in cash flow. Based on the research conducted by Rochmah and Ardianto (2020), a positive association has been shown between free cash flow and dividend premiums, particularly when accounting for the dividend payout ratio. Nevertheless, it is crucial to acknowledge that alterations in cash flow might have an adverse impact on dividend disbursements, particularly for companies characterized by regular cash flow trends.

Papadopoulos and Charalambidis (2007) performed an empirical investigation on the distribution of dividends among a sample of 72 businesses that were publicly traded on the Athens Stock Exchange. The researchers' results demonstrated that cash flow emerged as the primary determinant in the decision-making process pertaining to dividend distributions. The definite establishment of the link between size, capital structure, leverage, profitability, and liquidity remain inconclusive. In Pakistan, Hussain and Usman (2013) did research to analyze the dividend payments of 320 corporations that were listed on the Karachi Stock Exchange. The study's results indicated that the main determinants of dividend disbursements were the present profits and past dividends of these enterprises. The ability of prosperous businesses to consistently create profits and sustain profitability has enabled the generation of favorable cash flows, hence enabling the payout of larger dividends.

Fairchild (2010) emphasizes the importance of proficient management communication in the context of changes in dividend policy, suggesting that it might potentially mitigate negative investor perceptions. The free cash flow hypothesis and signaling theory are both used by the author to analyze the dividend policy. The investigation provides evidence that dividend payments function as favorable indicators for investors, whereas reductions in dividends convey unfavorable indicators. Furthermore, dividend payments are seen as signs of future success and serve as a means to resolve concerns pertaining to the surplus availability of cash flow. The results indicate a negative association between the presence of unrestricted cash and the allocation of dividends.

3.0 Methodology

Research approach employed in this study combined both qualitative and quantitative research designs to comprehensively investigate the multifaceted landscape of cybersecurity in the perspective of Pakistan. This comprehensive approach aimed to provide a nuanced understanding of the complex interplay between technology, governance, international relations within the realm of cybersecurity in Pakistan and legislation. Qualitative research component convoluted an in-depth exploration of historical, socio-economic, and technological factors that shaped Pakistan's susceptibility to cyber terrorizations. This was attained through a thorough literature review, which examined scholarly articles, policy frameworks, and case studies related to cybercrimes in Pakistan.

On the quantitative research front, the study employed statistical analysis to investigate the

trends and patterns of cybercrimes in Pakistan. Crime rate data, including reported cases and arrests, were collected for different years to identify temporal trends. The research also delved into the impact of technology on the advancement of cyber criminology by analyzing data on internet usage, social media engagement, and technological advancements. Inclusive research method incorporated both content analysis and case study analysis. Content analysis was applied to examine textual data from legal documents, policy frameworks, and relevant literature to discern patterns and themes related to cybersecurity in Pakistan. Case study analysis involved an in-depth examination of specific cybercrime incidents, focusing on the modus operandi, challenges faced, and outcomes of these cases.

Furthermore, the study employed a comparative analysis of cybercrime data over the years, with a focus on identifying key challenges faced by law enforcement agencies in combating cybercrimes. This analysis included the examination of the numbers of inquiries conducted, registered cases, and arrests made, as well as the trends in types of cybercrimes reported. Through this combined qualitative and quantitative research design, the study aimed to illuminate the intricate nexus between technology, governance, and international relations in the realm of cybersecurity within Pakistan. The exploration sought to contribute valuable insights that went beyond technical features, providing a holistic view of the challenges and opportunities in the evolving paradigm of cybersecurity.

4.0 Results

The objective of this research is to surpass the examination of technical elements and instead embrace a comprehensive perspective that encompasses wider parts of the cybersecurity debate. The investigation aims to acquire comprehensive information about cybercrime in Pakistan, comprehend the relationship between the criminal justice system and cybercrime, pinpoint significant problems in combatting cybercrime, and investigate the influence of technology on the evolution of cybercrime. The literature study explores the news culture in Pakistan, emphasizing the difficulties caused by the widespread use of social media platforms and the consequent spread of false information. Furthermore, it investigates the worldwide roots of cybercrime, with particular emphasis on the rise of "tricksters" in the United States and the following development of cyber dangers. The cybercrime section in Pakistan offers comprehensive insights into the inception of the Internet during the 1990s and its subsequent use for criminal activities. The formation of the National Cybercrime Response Centre by the government, which operates under the Federal Investigation Agency (FIA), and its responsibility for overseeing cyber security, fraud, and technical inquiries.

The focus is on digital forensics and methodologies. The text presents documented instances of cybercrime from various regions of Pakistan over the years, emphasizing the need of establishing a dedicated cybercrime court due to the rising frequency of such offenses. The report examines the existing difficulties in countering cybercrime, specifically highlighting the issues of insufficient knowledge and inadequate cyber security practices among individuals and organizations. The text emphasized the shortage of skilled professionals to carry out security protocols and the absence of explicit guidelines pertaining to email accounts, particularly within

the defense and law enforcement domains.

The rapid rate of technical progress, surpassing government advancements, has been recognized as a significant obstacle, alongside the want for augmented financing and research in information and communications technology (ICT). This section examines the role of the criminal justice system in combating cybercrime, specifically focusing on the legal framework derived from the Constitution of Pakistan. It includes significant legislations such as the Federal Investigation Agency Act, 1974, Pakistan Telecommunications Act, 1996, and the Prevention of Electronic Crimes Act, 2016. This text emphasizes the significance of the FIA, particularly its crime cell network, and provides an outline of the Electronic Crime Investigation Rules 2018. This text provides a detailed overview of the crimes and corresponding punishments outlined in the Prevention of Electronic Crimes Act 2016. It emphasizes the legal actions taken to address and counteract cyber threats. The Criminal Investigations and Digital Forensics Report offers a comprehensive summary of the developing legal structures, including the revisions made to the Criminal Law (Amendment) Act 2023.

The report highlighted the enhanced jurisdiction of provincial law enforcement agencies in documenting instances of cybercrimes and added additional criminal charges under the Prevention of Electronic Crimes Act (PECA), such as online grooming and child exploitation. Recognizes the significance of digital forensics in the acquisition, safeguarding, and analysis of digital evidence, which is essential in contemporary criminal investigations. This study examines the distinguishing features of forensic science courses, with a particular focus on those pertaining to cybercrime, in industrialized nations and Pakistan. Developed countries place a high importance on practical skills and the incorporation of legal elements. In Pakistan, initiatives like the National Cyber Crime Response Centre and the Electronic Crime Bill have been established to address cyber threats. These efforts primarily focus on raising public awareness through campaigns and collaborating with international organizations. The research emphasizes the continuous endeavours to enhance the regulatory framework and enhance the overall cybersecurity infrastructure in Pakistan.

Discussion and Conclusion

Ultimately, the cybersecurity environment in Pakistan is complex and diverse, characterized by the convergence of technology, government, and international connections. The country's historical context, influenced by the consequences of colonial control and the difficulties presented by social instability and high crime rates, provides a foundation for a thorough examination of cybercrimes in the nation. This research highlights the changing nature of cyber threats and their significant influence on political stability, underlining the need for strong cybersecurity measures. Although violent crime has decreased, Pakistan continues to struggle with a significant overall crime rate, which is worsened by factors such as poverty and corruption. The paper explores the complexities of cybercrimes in Pakistan, emphasizing the usage of the internet for activities such as harassment, fraud, and identity theft. The Criminal Justice system, as delineated by the Federal Investigation Agency Act and the Prevention of Electronic Crimes Act,

assumes a crucial function in dealing with cybercrimes, with an emphasis on inquiry, deterrence, and global collaboration. Nevertheless, the report highlights obstacles such as limited knowledge, inadequate cyber security practices, and the need for a highly skilled staff. This article examines the influence of technology on the progress of cyber criminology, highlighting the inherent weaknesses present in the digital domain. The rise of sinister technologies, such as deep fake videos, gives rise to ethical problems and calls for the creation of a comprehensive framework for cyber ethics. The report emphasizes the need for proactive steps in Pakistan to protect the stability, credibility, and integrity of political institutions in the face of changing cyber threats, as the country deals with the complex intersection of technology, governance, and foreign relations.

7.0 Implication the study

This research has significant ramifications as it provides insight into the intricate cybersecurity environment within the socio-political dynamics of Pakistan. The report emphasizes the immediate need for extensive adjustments and advancements in Pakistan's criminal and judicial system in order to successfully counteract the escalating surge of cybercrime. It is essential to develop dedicated cybercrime courts and enhance the quantity of proficient cybercrime professionals to guarantee the prosecution of offenders and the administration of justice. Furthermore, studies provide evidence that taking a proactive stance towards cybersecurity education and awareness, both on an individual and organizational level, is a crucial technique for reducing the impact of cyber-attacks. Enhancing the capabilities of law enforcement authorities, particularly in the fields of digital forensics and cybercrime, is crucial in order to proactively combat the increasing cyber threats.

Moreover, the research underscores the significance of global cooperation and teamwork in addressing the transnational aspect of cybercrime. In light of documented instances of government-backed hacking and cyber espionage, it is imperative to use diplomatic and collaborative initiatives to establish a unified stance against cyber threats. The report emphasizes the need of regularly revising laws and regulations to align with the continually changing landscape of cyber risks and technology. Policymakers should prioritize the ongoing enhancement of the regulatory framework and invest sufficient resources to establish a resilient cyber security infrastructure. In essence, this study highlights the need for a thorough and proactive strategy that encompasses legal, educational, and technical components in order to successfully fight cybercrime and safeguard the digital environment.

8.0 Limitation of the study

Aside from the useful discoveries, it was crucial to acknowledge the constraints linked to this research. The research was confined to the particular circumstances of Pakistan, hence the findings may not be immediately relevant other nations with distinct sociopolitical frameworks and varying degrees of technical advancement. The suggestions and findings of this research are based on the intricate nature of Pakistan's cyber security environment, which may restrict their applicability to the wider global context. Moreover, the dynamic and ever-changing landscape of cyber security implies that there may have been advancements since the data collection of the research, potentially impacting the present condition of cyber security in Pakistan. Thus, a

considerable amount of time has elapsed. The accuracy and trustworthiness of the findings depend on the accessibility and precision of the data sources used. However, this research does not include the possible hazards associated with underreporting, varying data collecting techniques, or the absence of complete datasets. It was crucial to comprehend these constraints in order to evaluate the study findings and influence future research endeavors in the ever-evolving realm of cyber security.

Mudasar Ali Nadeem: Problem Identification and Model Devolpement,
Sumaira Hashmi: Supervision and Drafting
Muhammad Abbas Khan: Literature search, Methodology

Conflict of Interests/Disclosures

The authors declared no potential conflicts of interest in this article's research,authorship, and/or publication.

References

Akhlaq, M. J. P. S. J. o. L. (2021). Cybercrime In Pakistan: A Study Of The Law Dealing With Cybercrimes In Pakistan.

Akhtar, S. J. A. a. S. (2023). Assessing the Cybercrime Legislation in Pakistan: a Comparative Study of European Union and Pakistani Cybercrime Laws.

Akram, M. M. U., Abdullah, M. T. J. I. J. O. S., & Technology. (2011). effective Enforcement Of Cyber Laws In Pakistan. 1-15.

Ali, A., Malik, A. K., Ahmed, M., Raza, B., & Ilyas, M. J. I. J. A. C. S. A. (2019). Privacy concerns in online social networks: A users' perspective. *10*(10).

Ashraf, A., König, C. J., Javed, M., & Mustafa, M. (2023). " Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan. Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023),

Baezner, M. (2018). *Regional rivalry between India-Pakistan: tit-for-tat in cyberspace*.

Baker, E. W. J. I. T. f. D. (2014). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. *20*(2), 122-139.

Bhatti, S. H., Adnan, S. M., Khaliq, A. J. J. o. E. M., & Sciences, S. (2021). Cybercrimes and Role of Law Enforcement Agencies: A Critical Analysis. *2*(1), 79-89.

Haider, W., Ali, A., Zubair, M. J. J. o. E. R., & Review, S. S. (2023). Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan. *3*(2), 48-54.

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

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

Jamshed, J., Rafique, W., Baig, K., Ahmad, W. J. I. J. o. B., & Affairs, E. (2022). Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms. *7*(1), 10-22.

Kabay, M. J. C. s. h. (2012). History of computer crime. 2.1-2.41.

Khan, M. D. J. P. J. o. C. (2019). The Decade of Criminology. *11*(2), I-V.

Khan, M. F., Raza, A., & Naseer, N. J. P. J. o. I. A. (2021). Cyber security and challenges faced by Pakistan. *4*(4).

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

LA VALORACIÓN, D. L. P. E., ÁMBITO, E., & CIVIL, D. E. I. (2021). LAW, STATE and TELECOMMUNICATIONS.

MANZAR, U., TANVEER, S., & JAMAL, S. (2016). The incidence of cybercrime in pakistan.

Mukhtar, A. J. J. o. C. A. (2018). Money laundering, terror financing and FATF: Implications for Pakistan. *3*(1), 27-56.

Nashit, M. J. D. J. (2019). Global Cybercrimes, Associated Laws and Befitting Policies for Pakistan. *22*(10), 46-54.

Rasool, S. J. I. s. o. j. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *12*, 21-34.

Razi, N., & Zahoor, R. J. R. d. D., Estado e Telecomunicações. (2021). Analyzing the Cyberspace Laws to Protect Data Privacy in Pakistan. *13*(2).

Saleem, H., Jan, J., Areej, A. J. S., Law, & Review, P. (2022). Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges. *1*(1), 11-24.

Shad, M. R. J. S. S. (2019). Cyber threat landscape and readiness challenge of Pakistan. *39*(1), 1-19.

Sharf, A., Akhtar, S., Sharf, S., & Asif, M. J. I. J. o. M. R. (2020). Ethical Issues of Cyberstalking and Personal Privacy in Pakistan: A Literature Survey. *1*(2), 357-362.

Shoro, S., Syed, F. M. S., & Mânica, S. J. F. S. I. R. (2020). Awareness and importance of forensic odontology amongst faculty members and students of dental institutes in Pakistan. *2*, 100116.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime* (Vol. 2). NYU Press.

u Salam, M. H., Arif, S. M. W. K., Rathore, S. A. J. A. o. H., & Sciences, S. (2022). An Appraisal on Digital Forensic and Computer Tools involved in Investigation process: The Case of Pakistan. *3*(3), 223-230.

Usman, M. J. I. L. R. (2017). cyber crime: Pakistani perspective. *1*(03), 18-40.

Zahoor, R., Razi, N. J. P. R. J. o. A., & Humanities. (2020). Cyber-crimes and cyber laws of Pakistan: An overview. *2*(2), 133-143.