https://doi.org/10.62585/pjcj.v4i2.102

Volume and Issues Obtainable at Centeriir.org
Pakistan Journal of Criminal Justice
ISSN: 2958-9363 ISSN (E): 2958-9371
Volume 4, No.1, 2024

Journal Homepage:https://journals.centeriir.org/index.php/pjcl

Cybercrime and Criminal Law in Pakistan: Societal Impact, Major Threats, and Legislative Responses

Muhammad Ahmar Zahid[1] **Aas Muhammad**[2] **Muhammad Aurangzeb Khan Khakwani**[3] **Muhammad Ahmed Maqbool**[4]

[1]BA LLB Hons, Inspector Investigation in Federal Investigation Agency (Ministry of Interior). E-Mail: ahmarzahidchandoor@gmail.com
[2]Assistant Professor, The Department of Law, The Islamia University of Bahawalpur. E-Mail: aas.muhammad@iub.edu.pk
[3]Muhammad Aurangzeb Khan Khakwani, Advocate High Court, Bahawalnagar. E-Mail: ozaib.83@gmail.com
[4]Advocate District Court Bahawalpur. Email: ammych001@gmail.com

ABSTRACT

This article examines the growing threat of cybercrime in Pakistan, highlighting the societal, commercial, and governmental vulnerabilities arising from the heightened dependence on digital technology. It rigorously analyzes the legal framework, including the Prevention of Electronic Crimes Act (PECA) 2016, underscoring its deficiencies in tackling swiftly advancing cyber threats. The article promotes a comprehensive reform initiative, including the enhancement of legislative frameworks, the strengthening of the Federal Investigation Agency's (FIA) enforcement capabilities, and the increase of public awareness. It emphasizes the necessity for coordination among legal, civil society, and technology experts to protect digital rights while reducing cyber dangers. Furthermore, suggestions for enhancing judicial and institutional capability are put forward to establish a more secure digital environment in Pakistan.

Article History: Received: 08-04-2024 **Accepted**: 29-06-2024 **Published**: 30-06-2024
Keywords: Cyber threats, Cyber Laws, Legislative Measures, PECA

Corresponding Author's Email: **ammych001@gmail.com**

doi https://doi.org/10.62585/pjcj.v4i2.102

1. Introduction

The revolutionizing phase of information technology is consequently changing civilizations and their institutions exponentially, creating opportunities and big challenges in the process. One of these emerging concerns that has become pervasive and touches nearly every aspect of society is cybercrime. As technology is woven into the fabric of everyday life, a new frontier of cyber-related events, either directly or indirectly affecting individuals, corporations, and governments, is emerging. While most countries have easily adjusted themselves in this evolving information technology environment, developing countries such as Pakistan have faced more and severe issues because they have remained way behind in their technological advancement. Cyber-crimes and their complexities get a breeding ground due to this lagging factor.

Cyber-crimes were not heard or seen in Pakistan 30 years ago since the common man knew nothing about these hitherto unknown threats (Islam et al., 2019). Today, the internet—useful for many social and commercial purposes—has also made possible a whole range of malicious activities. This has left Pakistan's fast-growing digital infrastructure ever more open to the possibility of cyber-attacks. The criminal justice systems of Pakistan generally deal with crimes, based on both traditional and modern methodologies. The base of the Cr.P.C is largely derived from the Pakistan Penal Code (PPC), which elaborates on all criminal offences, and the Code of Criminal Procedure dwells on the modalities needed to be followed while carrying out an inquiry of a criminal nature and the process involved in launching legal proceedings.

However, the Electronic Transactions Ordinance of 2002 was Pakistan's first legislation aimed at curbing the misuse of information systems and promoting the adoption of e-government technologies (Shaikh et al., 2016). The primary objective was to identify and facilitate the usage of electronic documents and commercial transactions. While the progress made in regulating electronic communications was commendable, it proved insufficient in curbing the increasing prevalence of internet-related crimes. As these cyber-crimes increased, it became clear that we needed complete laws. In 2007, the Prevention of Electronic Crimes Ordinance was made law. Even though it was passed more than once, this law did not provide long-lasting legal answers because it expired. After all, the parliament did not act (Munir, 2010). The Prevention of Electronic Crimes Act was drafted given the escalating cybercrime, which in common terms, is crime happening online—that is to say, any criminal activity conducted through digital means—including hacking, identity theft, and data breaches. Together, these legislations endeavour to address both traditional criminal activities and this rising cybercrime menace in Pakistan. Even after the coming into force of the Prevention of Electronic Crimes Act (PECA) in 2016, the current piece of legislation in Pakistan is too far from having the potential to deter electronic crimes. While PECA is a step in the right direction, it does not fully protect against all the new types of hacking that keep coming up as technology improves. The increasing population of internet users in the country, which crossed over 87 million customers on the broadband list by 2020, further intensifies the need for enhanced cybersecurity protocols (PTA, 2020).

According to the Federal Investigation Agency (FIA), in recent years, it has received more than 29,000 complaints related to cybercrime, and some arrests have also taken place. But apparently, this number is still huge (Yasin, 2021).

Over the past few years, Pakistan's internet industry has grown very quickly. Most of the users are in big cities, which are also important economic hubs. Improvements in computers and internet access have opened up contact and learning options that were previously unimaginable. Still, people and businesses use this infrastructure for illegal operations, showing that Pakistan is not immune to the challenges of online (Islam et al., 2019). While it may be nigh impossible to eliminate cybercrime in cyberspace, there's still much that can be done to reduce its incidence. First, consciousness among users has to be raised over

the risks associated with committing cybercrime. Strict enforcement of laws already in existence should be put into effect.
Besides, the excessive use of digital technology equates to the advent of big data, cloud computing, and artificial intelligence, which has introduced new threats to cybersecurity and, hence, complicating efforts to protect cyberspace. Cybercrime act originating from within Pakistan are also a threat, apart from external agents whose agenda might be to weaken national security. Social media platforms have been utilized by terrorist organizations as a means to disseminate false information. Even nations such as India exploit it to disseminate inaccurate or misleading information about Pakistan. The EU Disinfo Lab has recently uncovered an extensive network of fraudulent websites and media platforms used to tarnish the reputation of Pakistan globally (EU Disinfo Lab, 2020). This underlines the need for stricter and more effectively enforced legislation of this nature. The author has thoroughly examined cyber-crimes, and the pertinent growing difficulties, and has attempted to provide potential remedies to mitigate the problems. Additionally, the author elaborates on the legislative measures that Pakistan has implemented to protect against cyber threats in the following sections.

1.1 Terminologies

Before continuing, it is crucial to establish clear definitions of keywords in cyber studies, namely: Cyber-security, Cyber-threat etc. This will enable a more professional analysis of the topic and facilitate readers' comprehension of these ideas.

Cyber-security refers to the actions and conduct of persons in safeguarding their devices (Zwilling et al., 2020). Cybersecurity principles are held by persons who engage in protective conduct that is positively regarded (Stanton et al., 2005).

Cyber-security awareness refers to the comprehension and awareness of issues linked to information security, including their consequences and the necessary actions to address them (Kim et al., 2019) (Bulgurcu et al., 2009).

Cyber-threat refers to an occurrence in the digital realm that has the potential to result in the loss of valuable resources and negative outcomes (NIST SP 800-160) (Bederna and Szadeczky 2020). As stated by Shad (2019), it refers to the activity that might lead to unauthorized access, extraction, modification, or disruption of the integrity, confidentiality, or availability of an information system or the information stored, processed, or sent via it.

Cyber espionage refers to acquiring classified information without the owner's consent or authority (Bederna and Szadeczky, 2020). Furthermore, as defined by Paterson and Hanley (2020), cyber espionage is the unlawful use of computer networks to collect secret information, especially that held by governmental or organizational institutions.

Cyber-terrorism Cyber-terrorism refers to the use of the Internet by terrorists to carry out violent acts (Hua and Bapna 2013). Cyberattacks that are designed to cause substantial damage with the intention of frightening or coercing a civilian or government population are also classified as such (Platt 2012).

Hacking is the act of illicitly obtaining access to information by individuals with hostile intent who use their technological expertise to inflict damage (Bederna and Szadeczky 2020). A more common occurrence in recent years compared to older ones, it may be defined as the attitude and behaviors of a group of persons who are heavily involved in electronic activities, typically including obtaining illicit access (Alsunbul et al., 2015).

1.2 Literature Review

Crime has existed since the inception of human civilization, yet, the advent of contemporary technology has brought about cybercrimes. Cyber-crimes refer to crimes that are perpetrated using computers, either directly or indirectly. Conversely, conventional crimes are crimes that are performed using traditional tactics or procedures. Although there may seem to be no differences between these types of crimes, a thorough analysis reveals that the difference rests in the extent to which the media employed during the commission of the crime is influential. Cybercrime refers to any stage in which cybernetic intermediaries are utilized, while traditional crimes refer to crimes carried out without the assistance of technology means.

In 2018, Fang conducted a study that specifically examined the term "cyber". His research indicates that the term "cyber" is commonly used synonymously with "internet" by the majority of individuals. Nevertheless, "cyber" possesses two inherent attributes: it consists of electronic channels and allows for online communication. In his 2016 paper titled "Is Trident Safe from Cyber Attack?" released by the European Leadership Network, Futter defines cyber as communication conducted through electronic channels.

In his 2012 paper titled “Understanding Cybercrime: Phenomena, Challenges and Legal Response,” Gercke stated that the word 'cybercrime' refers to a range of offences, encompassing both conventional computer crimes and network crimes, when not utilized within the framework of legal agreements. Cybercrime is generally defined as any conduct involving computers or networks that serves as a means, an object, or a location for unlawful activities.

However, The United Nations (UN) concurs that an international definition of cybercrime does not exist. Nevertheless, it provides the following generalization: "Cybercrime encompasses cyber-enabled and cyber-dependent offenses, as well as online child sexual exploitation and abuse, which is classified as a distinct type of criminal activity" (United Nations Office on Drugs and Crime, 2013).

The inception of cyber crime can be traced back to the 1970s when the United States military implemented ARPANET (Advance Research Projects Agency Network). The US Department of defense provided funding for the project to safeguard their military communications; however, the technology developed enabled the reproduction of the initial message, which was subsequently exploited (Islam et al., 2019).

Since it is a novel concept in the field of international relations, the word "cybersecurity" is also rather nebulous. The idea of computer security was floating about in the 1970s, but it wasn't until the late 1980s that serious consideration of the topic was given. Then, in the 1990s, businesses began offering scanning apps. The phrase "cybersecurity" has been used often in cyber literature since the turn of the century, although it has not been properly defined. The word might signify various things to different individuals, say the experts (Akyeşilmen, 2016).

The researcher has included the US Department of Defense's definition for the benefit of our readers. Cybersecurity is defined as the “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” (Department of Military Affairs, 2010).

Cyberspace, coined by William Gibson in his 1984 novel "Neuromancer," now refers to the complete range of computer networks and related activities that occur over computers and their interconnected networks, primarily originating from the internet (Jamil, 2006). Therefore, cyberspace is a digital environment without legal limits where individuals engage with a network of hundreds of thousands, if not millions, of computers and users simultaneously. Consequently, this cyberspace has facilitated the occurrence of cybercrimes (Marvin, 1988).

While, according to Halder & Jaishankar (2011), “cyber-crimes are the offences which are committed by individual and groups against the individuals, groups and organizations having criminal motives to intentionally damage i.e. physical or mental harm to the victim directly or indirectly, who uses telecommunication networks like, chat rooms, emails, notice boards and groups and mobile phones for SMS/MMS." Computer crime, often known as cybercrime, consist of targeting computers and attacking them by infecting them with viruses and spreading malware.

Next, computer as a weapon refers to the use of a computer to engage in conventional criminal activities such as fraud or illicit gambling. Lastly, computer as an accessory refers to the mere act of utilizing a computer to store unlawful or stolen information or data (Mativat & Tremblay, 1997). Nevertheless, there is a lack of consensus over the universally accepted unambiguous definition of cyber-crime (Collin, 1996). Therefore, in a broad sense, it can refer to illicit internet-mediated activities that frequently occur in worldwide electronic networks, whether they are domestic, international, or transnational, without any cyber boundaries. This activity may include fraud, theft, blackmail, forgery, and embezzlement. However, it is notoriously difficult to detect and punish due to the technical complexity and unseen attackers who are located thousands of miles away.

Furthermore, international cyber-crimes pose a significant challenge to both domestic and international law and its adequate enforcement. In many countries, the existing legislation is not specifically designed to address cybercrime. Consequently, criminals are increasingly engaging in internet-based crimes, exploiting the inadequate penalties or the challenges in tracking down the perpetrators.

Concerning the hazards that arise from cyberspace in the context of Pakistan, Ullah et al, in their 2015 paper titled "Pakistan and Cyber Crimes: Problems and Preventions," explained that the problems lie not with the problems themselves, but rather with either the approach or the investigator. A prevalent issue in Pakistan is the lack of enough skills and expertise among investigators to conduct inquiries, collect evidence, ensure its security, and present it in court. Hence, the individual who violated the law is exempt from criminal punishment.

In their 2022 publication titled "Critical analysis of cybercrimes in Pakistan: Legislative measures and reforms," Jamshed et al emphasize that the continuous advancement of technology makes it perpetually difficult to detect electronic crimes. This difficulty arises from the ease of altering data and the potential for anonymous transactions. Given the manipulation of data, the investigation of cybercrimes is far more intricate than that of traditional crimes. Nevertheless, the implementation of contemporary methodologies might effectively decrease the intricacy of digital crime.

In their study titled "Cyber security and challenges faced by Pakistan," Khan et al. observed that while new technology offers convenience, constant evolution, and continuous improvement, contemporary threats are emerging with remarkable frequency. Moreover, users' capacity to cooperate is becoming increasingly arduous. Nevertheless, cybercrime is capable of adapting to these new technologies, so endangering the security and financial stability of a nation.

In his 2020 article titled "Cyber Warfare and Global Power Politics," Firdous explored the ramifications of cyber threats and the approach of international law in addressing them. His results indicate that the issues stemming from these illicit activities have garnered considerable attention, particularly those pertaining to cracking, copyright infringement, graphic sexual content aimed at minors, and child grooming. This phenomenon is commonly known as privacy problems, which arise when hackers or attackers intentionally corrupt or intercept confidential data, either through lawful or unlawful means. The efficiency of the international legal system, which aims to facilitate responsibility for criminal acts through the International Criminal Court (ICC), is impeded by the lack of coordination or contradiction between local laws and international norms.

1.3 Research Questions

1. In light of the rapid development of digital technology, how has society in Pakistan reacted, and how has this affected the growth of online services?
2. Which cyber threats are the most significant in Pakistan, and what difficulties have they engendered, and how is Pakistan specifically addressing these threats and the resulting challenges?
3. What cyber laws has Pakistan passed, and how can these laws be improved to make them more effective against future cyber threats?

1.4 Research Methodology

The study technique for the research thesis will use a doctrinal and qualitative approach to examine the current legislative frameworks, policies, and practices of cybersecurity in Pakistan. This research will conduct a thorough analysis of academic publications, government reports, published books, and past thesis works that are pertinent to cybersecurity concerns and measures in Pakistan.

Conducting doctrinal research will entail a meticulous analysis of policy and legislative documents to comprehend the legal position and actions of the government in response to cyber threats. Concurrently, the qualitative component will concentrate on amalgamating perspectives from prior scholarly works to investigate the practical implementation of these policies and their efficacy in reducing cyber hazards. When used together, these techniques will illuminate Pakistan's present cybersecurity situation and allow us to make well-informed suggestions for how the country may strengthen its defenses.

2. Cyber Expansion in Pakistan

In the early 1990s, Pakistan, a developing nation in the Global South, gained access to the internet. There are now more people using the internet in Pakistan than in any other country (Kemp, 2020). In 2016, internet penetration increased to 17.8% thanks to the country's availability of 2G and 4G technology, and the country's digital economy ranked tenth by UN criteria (Statista, 2020). According to the Pakistan Telecommunication Authority (PTA), “there are 169 million cellular subscribers and a broadband penetration rate of 39.5% with 87 million users (PTA, 2020). “There is now a mobile internet penetration rate of 26% and 54% of the population has access to mobile broadband (GSMA, 2020).

Given the large number of people utilizing information and communication technology, cyberspace has become a new area that presents issues in terms of regulating cybersecurity. Pakistan was worldwide rated 94th according to the 2018 “Global Cyber Security Index Report” (GCI) by the International Telecommunication Union (ITU). Pakistan is among the top five areas with the greatest rates of encountering malware from January to December 2018, with a rate of 18.94%. Pakistan was among the top five nations in terms of crypto-currency mining encounter rates in 2018, with a significant proportion of 1.47 (Microsoft, 2018). In 2019, key Pakistani officials experienced a hacking incident when their mobile phones were compromised over WhatsApp using a specific form of malicious software called 'Pegasus'.

Reports surfaced suggesting that Indian intelligence was using the same software to eavesdrop on attorneys, lawmakers, and others in the country, which further heightened public anxiety over the event. According to Qarar (2018), “the US National Security Agency likewise primarily monitors Pakistan. This extends to the country's banking system as well.” It is also vulnerable to cyberattacks. Most often seen are instances of online payment fraud, hacking, card skimming, and ATM card abuse.

As highlighted by Malik (2019), “Out of a total of 25 million bank accounts, an estimated 8,000 to 10,000 individuals have been targeted and victimized by hackers inside the business.” Pakistani banks incurred significant financial losses as a result of cyberattacks (Iqbal, 2021). The primary obstacle in the present scenario of developing cybersecurity legislation in Pakistan is the successful execution of the laws. The deficient institutional framework in Pakistan poses a significant obstacle to the enforcement of cyber security regulations, along with other imminent issues such as the existence of adversarial intelligence networks and anti-state groups.

2.1 The boom in e-services in Pakistan

Over the last 20 years, e-commerce and e-government have taken off thanks to information and communication technologies, especially the Internet. The use of information and communication technologies (ICTs) is driving nations throughout the globe to rely more and more on cyberspace. According to Khan et al., (2021), "More over four billion people, or 55.1% of the world's population, were online in June 2018, up from 16 million, or 0.4% of the population, in December 1995." Consequently, a state's responsibility to safeguard both its physical and virtual borders is growing. This is particularly true for Pakistan's quickly developing e-government, e-commerce, and e-business sectors because of the country's history of deadly regional conflict, religious extremism, and terrorist activities.

Since gaining independence, Pakistan has seen several challenges to its physical security. However, it now has the additional challenge of safeguarding its increasing use of ICTs by addressing information security vulnerabilities. According to the Pakistan Telecommunication Authority (PTA) figures from February 2019, "over 31% of the population in Pakistan has access to the internet. Pakistan was identified as one of the world's top ten rapidly expanding digital and internet economies in the 2017 Information Economy Report by the United Nations Conference on Trade and Development." The poll indicates that internet access among Pakistanis rose from 3% to 15% during a span of three years (2012-2015).

The exponential expansion of internet access in Pakistan in recent years has been a significant driver behind the advancement of 3G/4G technologies. Currently, 63 million individuals out of 65 million broadband customers utilize 3G or 4G smartphones to access the internet. Public and private organizations in Pakistan are progressively relying on online administration and service systems to function within this rapidly developing nation, as Ahmed elucidates. NADRA, which maintains the national ID database, is the preeminent governmental organization in Pakistan.

As mentioned by Malik (2014), "The NADRA provides access to internet data about Pakistani individuals to many entities, including banks, the Pakistani Election Commission, the Department of Immigration and Passports, mobile networks, and security organizations." This organization. Public enterprises in Pakistan are increasingly using electronic methods to enhance modernization and efficiency in the provision of economic, social, and safety services. In 2014, the National Information Technology Board underwent a name change due to its merger with the Pakistan Computer Bureau. The Pakistan Computer Bureau was first founded as the E-Government Directorate under the IT Ministry in 2002. Information and Communication Technology (ICT) services, such as Automated Teller Machines (ATMs), internet banking, online payments, and virtual stock exchanges, are prevalent in the country's economy due to the presence of Virtual Stock Exchanges (VSEs). E-government services are also offered by other social sectors such as schools, hospitals, and police units. Khyber Pakhtunkhwa. Upgrading military and nuclear arsenals is a prominent feature of growth in the 21st century, and Pakistan is also following this trend. (Ahmed, 2017).

3. Cybersecurity Challenges in Pakistan

With the rise of the internet, cyberspace has the potential to augment and perhaps replace more traditional forms of criminality in today's world. Because malicious actors in today's virtual world may easily attack vital infrastructure, national security is a big concern in this setting. Although cyberspace is important and has many advantages, Pakistan's increasing dependence on it puts the country's national security at risk because of ineffective cybersecurity measures.

As highlighted by Ahmad (2021), "In the 2017 annual report of the Global Cybersecurity Index (GCI), Pakistan occupied the 67th position among 193 nations in terms of cybersecurity commitment." This research indicates that the nation's cybersecurity is positioned at a low global rank due to a dearth of legislative, technological, organizational, capacity management, and collaborative measures. A few instances illustrate the insufficiency of Pakistan's cybersecurity protocols. Based on Snowden revelations, The Guardian published an exposé in March 2013 indicating that the United States National Security Agency has designated Pakistan as its second most-wanted target, following Iran (Rossi, 2014).

The UK intelligence agency, "Government Communications Headquarters" (GCHQ), was accused by Intercept of infiltrating Pakistan's primary communications infrastructure to get unauthorized access to commonly used websites, via the same method. During the latter half of 2015, Microsoft disclosed that Pakistan experienced the highest number of malware attacks (Malik et al., 2022). Subsequently, the Senate Committee on Foreign Affairs of Pakistan uncovered that Pakistan was among the primary nations subjected to foreign espionage (Cassidy, 2013). The cybersecurity situation in Pakistan is concerning due to its susceptibility to cyber assaults and the lack of legislation, policies, and enforcement to combat such threats (Shad, 2019). Due to Pakistan's inadequate cybersecurity measures and general lack of security, the nation is susceptible to four specific types of cyber threats:

I. Organised Cybercrime

The growing digitization of global financial and commercial activities has attracted highly organized and talented criminals to the realm of cybercrime. Cybercriminals use the Dark Market and similar black market networks like Silk Road to conduct a wide range of illicit activities, including the sale and theft of sensitive information (such as passwords, social security numbers, and bank account details) and the trafficking of botnets. The global economy is significantly impacted by the shift of organized crime to the digital domain. According to research by the "Center for Strategic and International Studies" (CSIS)), cybercrime is projected to incur an annual cost of $445 billion to the global economy (Kar & Spanjers, 2017).

International law enforcement agencies have not yet reached a consensus on how to combat cybercrime. With the increasing use of e-banking and e-government services, the incidence of cybercrime is rising in Pakistan. The nation constantly encounters cybercrime, which encompasses activities like account hacking, unlawful cash withdrawals, and money transfers. In 2017, the "National Response Center for Cyber Crimes" (NRCC), which is the cybercrime arm of the Federal Investigation Agency (FIA), received a total of 2019 complaints (Soo, n.d). The grievances may be categorized into three fundamental groups: Out of the total number of instances, 76 percent (1592 cases) were related to social media harassment, defamation, and extortion. Financial fraud accounted for 14 percent (307 cases), threats via telephone accounted for 5 percent (116 cases), and there were 186 occurrences of email hacking. Many crimes remain unreported because of a lack of understanding of cyber rules and a lack of trust in law enforcement. Based on the rating provided, it seems that the financial industry is the most susceptible to significant cybercrime. As highlighted by Nadeem et al., (2023), "Habib Bank Limited (HBL) ATMs were targeted in a highly advanced hack that used skimming devices to breach 579 accounts and pilfer Rs10 million." The bank was subject to cyberattacks in both 2015 and 2016. Computer hacking and phishing/email scams have seen a surge in prevalence in recent years, becoming a prevalent kind of cybercrime. Cybercriminals use these techniques to gain entry into a computer network and pilfer confidential or personal information, enabling them to engage in fraudulent activities.

II. Cyberwarfare

Cyberwarfare refers to state-sponsored cyberattacks that are well-planned, financed, and executed by experts. It is common for governments to launch these types of cyberattacks in pursuit of their political, security, and strategic goals (Beidleman, 2009). The strategic use of cyberspace to complement traditional military operations marks the next phase of warfare. Critical infrastructures are hit first by a "cyber-enabled physical strike," rather than a direct military target.

In 2007, Israel successfully neutralized Syria's air defense systems via a cyber-attack, enabling them to approach Syria's nuclear facility undetected and carry out an unexpected aerial assault (Bar, 2020). It is said that in 2008, Russia strategically used the internet during its confrontation with Georgia about South Ossetia. According to McAfee's 2007 annual report, around 120 nations were engaged in the development of offensive cyber capabilities, which include the manipulation of denial of service attacks and the interruption or degradation of computer and information systems (Firdous, 2020). India has a prominent position on this list, with other notable nations such as the United States, China, Russia, Israel, North Korea, and Iran.

III. Hacking Attacks

The primary cyber danger is hacking, which involves unauthorized access to computer systems to cause harm, disruption, or engaging in illegal activities. Hackers' motives and talents might differ significantly. Hackers may engage in hacking operations as a form of retaliation or as part of their ideological agenda, either at a national or global level (Parikh et al., 2017).

Those who hack for nefarious, political, criminal, or state-sponsored purposes are known as cybercriminals. Because of its fragmented form and limited ramifications, hacking does not represent as great a concern as other significant cyber threats. However, this is a grave issue since it can incite more instances of severe criminal activity and cyber warfare, while also inflicting tremendous suffering upon those who are already susceptible.

IV. Cyberterrorism

Terrorist organizations that are motivated by ideology and politics are increasingly congregating in cyberspace, primarily because it provides them with a convenient environment in which to advance their transnational and local objectives (Nnam et al., 2019).

They have a lot of options when it comes to using cyberspace for recruiting, training, radicalization, propaganda, indoctrination, and communication. They may also steal money, coordinate assaults in the real world, and damage their adversaries' websites and networks by taking advantage of the ungoverned internet. The anonymity, low cost, and global virtual reach that cyberspace affords make it an attractive and practical tool for terrorist agendas. With the help of sectarian groups and the Tehreek-i Taliban Pakistan (TTP), Pakistan saw its worst era of political and religious extremism and terrorism after 9/11 (Basit, 2022).

This is accompanied by ethnic separatism and violence. Terrorist groups in Pakistan mostly use physical assaults to create chaos inside the nation. However, they also utilize online to indoctrinate and recruit members, as well as disseminate their ideology.

In this regard, two considerations stand out. To begin, terrorist groups such as al-Qaeda, Islamic State, and TTP are well-equipped and able to quickly adapt to virtual combat. Second, the TTP is said to have the support of security services that are opposed to Pakistan; this is in addition to their well-known extreme dislike of Pakistan. What this means is that the gang, with help from outside sources, may be able to retaliate against Pakistan via the Internet. If this happens, terrorists may resort to cybercrime to steal money instead of attacking physical facilities, and they can even target key infrastructures (MANZAR et al., 2016).

4. Legislation regarding Cyber Technology in Pakistan

The term “cyber law” refers to the subfield of law that aims to regulate illegal activities that occur in cyberspace or via the use of computer resources. Up to this point, Pakistan's internet laws are as follows.

4.1 The Telegraph Act, 1885

Nonetheless, in light of the emergence of contemporary technologies, this Act has been rendered inadequate. Nevertheless, it remains extant to bolster the authority of provincial and federal governments to encroach upon the privacy rights of the populace. The executive branch exercises unrestrained authority in pursuit of the public good, bypassing judicial oversight. Telegraphs may be seized by the government in the event of a public emergency and to ensure public safety. However, unauthorized entry into telegraph offices and interference with telegraph messages also resulted in the imposition of a penalty (The Telegraph Act, 1885).

4.2 Pakistan Telecommunication (Re-organization) Act, 1996

This legislation mandates that the “Telecommunication Authority or Frequency Allocation Board” must report any unlawful activities related to telecommunications to the court. The court has the authority to issue a search warrant for locations where unlawful activities are taking place. Additionally, the court may take any equipment used for criminal purposes or to conduct investigations related to such activities, (Pakistan Telecommunication Act, 1996).

4.3 National I.T. Policy and Action Plan, 2000

In 2000, the Pakistani government implemented its information technology policy. The primary aim of this policy was to establish legislation about cybercrimes. Following an examination of UNCITRAL Model Laws and consultations with the legal systems of numerous common law and civil countries, this policy was adopted. The policy was developed by the “International Consensus Principles on Electronic Authentication,” which were formulated by the Internet Law and Policy Forum. This decision was made after considering the approaches taken by other nations (Mushtaque et al., 2015). An information technology (I.T.) policy and action plan are developed to enhance the security of personal data and safeguard the integrity of electronic commerce (National I.T. Policy, 2000). This instrument represents an important step toward securing cyberspace.

4.4 Electronic Transaction Ordinance, 2002

The fundamental motivation behind this law was to provide legitimacy to various online transactions. Thanks to this regulation, digital records and signatures are now considered legitimate. In addition, the Electronic Transaction Ordinance of 2002 calls on the federal government to establish regulations to safeguard data and user privacy. But there are a lot of ambiguities in this regulation as well. Numerous offenses that were addressed under the numerous international cyber laws of different nations were disregarded. Also, the laws haven't been updated to keep up with the rapid development of new technology and cybercrimes, therefore they're considered archaic.

4.5 Electronic Crimes Act, 2004

This Act was implemented with the collaboration of the Ministry of Information Technology in compliance with the terms of the Electronic Transactions legislation, 2002. In this Act, the different transgressions associated with the digital realm were established as cyber-crimes. The Act (Electronic Crimes Act, 2004) classified various activities as cybercrimes, “including criminal access, criminal data access, data damage, system damage, electronic fraud, electronic forgery, misuse of devices, misuse of encryption, malicious code, cyberstalking, spamming, spoofing, unauthorized interception, and cyber terrorism.” Therefore, this Act lacked a dedicated enforcement unit. Furthermore, the activities that were made public under this legislation were also lacking clear definitions. The definitions of illegal offenses were too ambiguous to be comprehended. This law was rendered ineffective due to the absence of any enforcement measures and the intricacy of the wording used to describe cybercrimes.

4.6 Cyber Security Council Bill, 2014

According to Mushtaque et al. (2015), “This bill was introduced by Senator Mushahid Hussain Syed on April 14, 2014.” A council to address cyber security challenges on a global and national scale, as well as to develop a strategy and set of rules for the next 10 to 20 years, was proposed in this law. Therefore, the government has not yet passed the Cyber Security Council Bill (2014).

4.7 The Prevention of Electronic Crimes Act, (PECA) 2016

The bill for this Act was ratified by the National Assembly in April 2015 and subsequently voted on by the Senate in August 2017. This legislation was implemented in response to the terrorist assault on Peshawar school. It was included in Pakistan's Government's National Action Plan to address terrorism in the nation. As highlighted by Iqbal et al., (2023), “the Act classifies cyber stalking, cyber spoofing, phishing, cyber harassment, illegal access to an information system or device, illegal access to information or data, illegal interference with an information or data, illegal interference with information system, cyber terrorism, blasphemy, and cyber forgery as cybercrimes.” Nevertheless, the wording used in the Act lacks simplicity and clarity.

Many human rights groups and legal experts argue that the wording of the legislation has to be more precise since it infringes upon privacy and undermines freedom of speech (Prevention of Electronic Crimes legislation, 2016). According to this legislation, anybody who assumes the identity of another individual to engage in fraudulent activities is legally responsible for invading someone's privacy.

The sending of personal information with the intent to commit fraud, deception, or lying is also considered an invasion of privacy. A similar felony applies to the unlawful acquisition of non-public information by hacking or interception with the intent to conduct a crime, incur a wrongful gain or loss, or get any advantage similar to this. Any information that might compromise national security could be intercepted by law enforcement. In addition, if the court is convinced that there is data or information that is essential for the inquiry, it may grant a search and seizure order to an investigating officer (Arshad, 2016).

The court has the authority to issue a warrant to an individual who has data obtained from a specific communication. This order requires the person to provide the data within seven days if the court deems it necessary for inquiry, as stated in the Prevention of Electronic Crimes Act. Furthermore, the service providers possess the legal power to store data for at least one year, which directly hinders the right to privacy and safeguarding of information. As mentioned by Liaquat et al., (2016) “The Pakistan Telecommunications Authority possesses the authority to eliminate or restrict access to specific information that it deems to be in opposition to the honor of Islam, the national interest, or the security and integrity of Pakistan.” This also includes content that may be harmful to the friendly relations of foreign states, public interest, ethics, morality, and decency.

If the investigating officer can convince the court that the real-time gathering and recording of such data is necessary for evidence, the court has the authority to order it. Additionally, the investigating officer must submit a sworn application for this reason. Additionally, it grants the federal government the authority to distribute the information collected during the inquiry to foreign intelligence services without requiring judicial approval. The federal government has the authority to confiscate and distribute such data, but there is no specific human rights document mentioned to justify these actions (Sherwani, 2018).

Following the enactment of this legislation, many authorities have been authorized to regulate persons and organizations engaged in cybercrimes. The FIA has the authority to regulate conduct in cyberspace.

Allocations will be made for the creation of forensic labs and cybercrime police stations. This Act has a dual purpose, namely safeguarding both persons and the state. Individuals can pursue legal recourse in cases of crimes such as identity or data theft.

4.8 Assessment of Cyber Regulation in Pakistan

As highlighted by Akram et al., (2011), “To recognize and facilitate documents, records, information, communications, and transactions in electronic form, and to provide for the accreditation of certification service providers, Pakistan's Electronic Transactions Ordinance, 2002 (ETO) was the first piece of legislation the country passed addressing cybercrime;” however, it only covered a small subset of all crimes committed online. It was seen as a significant milestone in the process of drafting cybercrime laws. As highlighted by Iqbal (2021), “Cybercrimes such as cyberstalking, cyber fraud, cyber war, data damage, cyber forgery, spoofing, cyberterrorism, and punishments for these offenses were addressed in the ‘Electronic Crimes Act’ that was drafted in 2004 by the Pakistani Ministry of Information and Technology (GOP) in response to the ETO, 2002.”

Over time, the rise and spread of cybercrime in the country made it necessary to pass strict laws on the subject. After that, General Pervez Musharraf, who was president of Pakistan at the time, signed “The Prevention of Electronic Crimes Ordinance, 2007” into law (Munir, 2010). But this law was also just a start; it only dealt with a few of the actual e-crimes.

Following Edward Snowden's disturbing revelations about the “National Security Agency” of the United States engaging in cyber espionage operations in Pakistan, the Chairman of the Senate Committee on Defense and Defense Production put out a “Seven Points Action Plan” to enhance the country's cybersecurity (Senate of Pakistan, 2013). A national cybersecurity agenda was subsequently shaped in part by the Senate Action Plan, which outlined a plan to protect the nation's most vital infrastructure. Even if it was insufficient, as asserted by Iqbal (2021), “the historic National Action Plan (NAP) issued by the GOP at the end of December 2014 to address terrorist activities did have a provision for internet radicalization.”

The GOP's previous actions to address cybercrime were temporary and did not effectively support the judicial system and law enforcement agencies. And then, as mentioned by Iqbal et al., (2023), “Pakistan passed cybersecurity legislation in the lower house of parliament on 11 December 2016. This led to the establishment of the Prevention of Electronic Crimes Act (PECA), in 2016.” The enactment of the act included extensive debates lasting 18 months by legislators, cyber specialists, and industry professionals. However, certain portions of the legislation remain contentious, as will be detailed in the following paragraphs. The provisions contained in the legislation aim to protect against unauthorized access, and interception, and safeguard the transfer of important data and information systems. Additionally, it contains provisions aimed at eliminating cyberterrorism, the promotion of offensive content online, hate speech, electronic fraud, identity theft, cyberstalking, spamming, spoofing, and other related activities. The cyber restrictions in Pakistan are very ineffective, since they may be readily manipulated and bypassed by anybody, even those with little computer literacy (Iqbal, 2021).

5. Factors Impacting Cybersecurity Law Adherence in Pakistan

5.1 Understanding the Context

The majority of nation-states have implemented rules and regulations about cybersecurity since 2014, with a smaller number being added subsequently (Burr, 2015). The task of enacting and enforcing laws and regulations continues to be a significant obstacle for many reasons. One of the key aspects is that cybersecurity rules and regulations need to go via several organizations, including those that are public, semipublic, and private. These institutions have procedures that overlap and hinder their successful execution. Due to these overlaps, the intricate hierarchical structure of the country's administration, and a lack of collaboration across agencies, it is difficult to fully implement and enforce the present regulations. However, the regulation of the information sector is the responsibility of many agencies, whose main function is to ensure that the cybersecurity process is conducted meticulously by all relevant regulations. Typically, they are under the oversight of the "Ministry of Information Technology," however this is not always the case. However, it is worth noting that numerous other ministries, such as the Ministry of Science and the Ministry of Interior, hold substantial power in formulating and executing diverse policies and initiatives about the information technology industry in its entirety (Tene et al., 2017). The level of coordination across all ministries in the security process is notably deficient.

This phenomenon can be observed throughout the policy implementation, legislative, and administrative processes, ultimately resulting in insufficient enforcement and implementation of current laws and regulations (Bikoko et al., 2019). This stance gives rise to further concerns concerning the trajectory of policy formulation within the nation, with a particular focus on cybersecurity. The aforementioned industry has witnessed a remarkable increase in the frequency of cybersecurity vulnerabilities and, consequently, a decline in cybercrime (Rasool, 2015).

These findings, together with policy frameworks inside other ministerial agencies, could have exacerbated the problems. Due to the critical nature of law enforcement in states, a more thorough comprehension of the factors that may influence law enforcement on a regional level necessitates more demographic information (Clark, 2002). When I was younger, I thought a country's development goals were the most crucial part of its system for enforcing laws. Although factors such as the availability of resources, the wealth of the state, and the history of federal programs did not seem to play a significant role in policy formation, there are signs that other factors could become important during the acceptance stage of legislation implementation.

The presence of various factors, such as limited resources, corruption, lack of knowledge, uncertainty regarding law enforcement, a lack of willingness, and low confidence, are impeding the implementation of cybersecurity regulations. Further elaboration on these components is provided below.

5.2 Corruption and Law Implementation

Law enforcement agencies are responsible for supervising and enforcing laws that aim to safeguard those involved in cybercrime, online fraud, and cyberattacks. Corruption significantly undermines the effectiveness of law enforcement in mitigating and preventing cyber security damages (Robbins, 2000). Cybercrime is not a significant concern for law enforcement agencies in many nations, which exacerbates the situation given their limited resources and the presence of numerous other dangers to the legal system. One may argue that no one is ever really hurt by these kinds of crimes (William, 2020). The abuse of official authority for private gain is known as corruption. Forms of corruption include favoritism, embezzlement, bribery, extortion, and the provision of favors in exchange for political contributions. Cybercrime and corrupt conduct often go hand in hand, and cybercrime is often a "door opener" for corrupt activities. Instances of corruption related to cybercrime include bribery for a favorable decision or manipulation of the judicial process, using illicit ways to launder the proceeds of cybercrime and associated corruption, and providing financial support for illegal or unauthorized hacking, ransomware distribution, and denial of service on a global or domestic scale (William, 2020).

As a result of the pervasiveness and sway of corruption, law enforcement initiatives to reduce cybercrime might produce unintended or unanticipated outcomes. Depicting this concept are two fundamental methods by which corruption can undermine the effectiveness of law enforcement.

5.3 Expertise and Law Enforcement

One of the greatest dangers facing the globe today is cybercrime, which affects not only national security but also economic power and public safety. As highlighted by Firdous et al., (2020), “Law enforcement agencies at all levels have the difficult task of investigating a wide range of cybercrimes and cyberthreats perpetrated by individuals with malicious intent, including hackers, extremists, and state actors.” Law enforcement authorities in charge of cybersecurity must address this problem by providing cybercrime training to competent agency personnel so that they can prevent cyberattacks or identify and bring to justice those guilty of them.

The proliferation of technology and the worldwide accessibility of the internet give rise to novel manifestations of cybercrime daily. As mentioned by Bokhari (2023), “Mike Hulett, director of operations of the National Cyber Crime Unit of the United Kingdom, estimates that nearly half of all reported crimes in the country in 2017 involved cyber activity.” Moreover, approximately 68% of prominent organizations in the United Kingdom have experienced cyber security breaches or attacks. As cybercriminals multiply and refine their techniques, it becomes more difficult for law enforcement to keep up. Research has shown that traditional methods used by law enforcement in investigations may not always work in the digital world (Brener, 2010). For this reason, a fresh strategy backed by a unique set of skills and expertise is needed to combat these technologically complex attacks.

This is of the utmost importance since cybercriminals are known to be technically proficient and to constantly innovate to elude the detection and prosecution of law enforcement (Williams, 2008). To counteract these technologically sophisticated crimes, a fresh approach and specialized knowledge are required. The reason this is so important is that cybercriminals are usually quite tech-savvy, so they're continuously coming up with new methods to evade authorities.

5.4 Public Confidence and Law Enforcement

There are cybercrime centres and an online way to submit complaints, but the crimes themselves are underreported, with the lowest numbers coming from the most common forms of cybercrime, such as bank and credit fraud. Cyberbullying, cyber-harassment, and defamation are the most common types of reported cybercrimes. The new laws passed under PECA are mostly unknown to the general public in Pakistan. The acceptance of filing a formal complaint on the grounds of being bullied online is still extremely foreign and is often seen as an extremely aggressive action to do when the decision to disregard such serious crimes is made and many perpetrators never fall under the jurisdiction of the law. Through a combination of ignorance and reluctance on the part of the public, cybercrime is one of the least reported crimes. FIA data indicate the annual count of cybercrime investigations as follows:

Year	No of Inquires	No. of Registered Cases
2016	514	47
2017	1290	207
2018	20295	255
2019	11389	1071

Additionally disclosed was the fact that a mere 14 convictions were achieved throughout the period of 5 years (2015-2019). This throws doubt on the effectiveness of the PECA. This can evolve into an independent discussion, encompassing both the legal aspects and the effectiveness of the Cyber Crime Wing of FIA in substantiating the indictments against the defendants (Iqbal et al., 2023). Statistical data indicates an increase in the number of investigations initiated, implying that a greater number of instances were reported annually, leading to further investigations against the accused.

Currently, establishing an FIR on cybercrime is more like an online process than the conventional one when one visits the police station and manually registers the FIR. The reporter is not obliged to go and can only submit the complaint from the comfort of their house, hence this online technique is much more efficient than the conventional one. Additionally, the online complaint is immediately registered, and employees from FIA are obligated to take some action on the matter (Jamshed et al., 2022). The downside of this automated system is that individuals frequently lack confidence in the existence of certain services, such as an online FIR for cybercrime, and are unsure of how to operate the system. A significant number of individuals are utilizing social media and internet services, but they are illiterate enough to use sensitive reporting systems and write in detail.

Another problem is that there are a lot of spam complaints on the system. You can take legal action against the spammers, but the system ends up being full of spam. It's safe to say that cybercrime laws aren't being used even half of what they're supposed to be. This is mostly because most people aren't aware of them or can't read or write them. Another problem that comes up a lot is that most people don't know what they're doing that is illegal under cybercrime laws. You could say that both the public and FIA which is in charge of cybercrime, need to work together to close the gaps between them so that more crimes are reported and the law is followed correctly and effectively.

6: Cyber Security Strategy of Pakistan

There are now several threats to data and information in cyberspace. Security measures must be put in place to prevent unauthorized access to the data stored on communication networks and the internet. Data protection procedures must be regulated by each nation. It is possible to implement the different approaches in this respect. To further identify the perpetrators of the crimes, laboratories and investigative methods may be used (Usman, 2017). When it comes to protecting personal information, Pakistan has two options. Digital Crime Response Centre is one such entity. The Senate Defense Committee of Pakistan is the other (Awan & Memon, 2016).

6.1 National Response Centre for Cyber-crime (NR3C)

As highlighted by Awan and Memon (2016), “Pakistan has created the National Response Center for Cyber-crime (NR3C) to effectively monitor, trace, and apprehend cybercriminals to maintain control and combat cybercrime.” NR3C offers education, training, and awareness programs to both people and companies to effectively manage and prevent cybercrimes via the use of security measures. Additionally, Pakistan collaborates with international institutions and organizations to effectively manage and combat crimes originating from its territory.

For the goal of educating people in the cyber realm, it organizes trainings, workshops, and seminars. Researchers in Pakistan discovered that new risks to data privacy emerged with technological improvements. The increasing reliance on digital technology has led to an increase in cybercrime, which is why this center was established to address the growing need for regulating cyberspace. This facility handles both public and private complaints. Because of this, the PECA is the sole statute against which this facility is actively combating crime.

6.2 Pakistan’s Senate Defense Committee to Design the Cyber Security Strategy of Pakistan

Following the disclosure by Edward Snowden, it has been revealed that the U.S. National Security Agency (NSA) has conducted surveillance on Pakistan. Pakistan's passive approach towards formulating a cyber security strategy for national security is a perilous position. Snowden disclosed that the United States engaged in surveillance on Pakistan's National Telecommunication Corporation (NTC), which serves as a critical communication conduit (Lyon, 2014). This channel serves as a means of communication between the military and civilian administrations. According to Snowden, it has been alleged that the NSA engaged in surveillance activities in Pakistan using a technology called SECONDDATE.

This program hacked into the FOXACID server in Pakistan and retrieved all the data that was needed. Awan and Memon (2016) believe that "around 13.5 billion pieces of data, including phone conversations, faxes, and emails, have been compromised." The "Pakistan Information Security Association" (PISA) met with Senator Mushahid Hussain Syed, who was the committee chairman at the time, to discuss the creation of a cyber security plan. This meeting resolved several topics. It was proposed that the budget be set aside for cyber defense, as it is vital to safeguard Pakistan against cyberattacks.

6.3 Critical Information Infrastructure Protection

The "Critical Information Infrastructure" (CII) of a nation is the paramount asset of that country. The whole economy and social system rely on the framework of this infrastructure. If this system is breached, it will pose a significant risk to the existence of a nation. Pakistan does not have a dedicated government department responsible for the protection of any specific (CII). None of the key infrastructure is designated as the foremost infrastructure. Pakistan does not have a roster of Confidential Informants (C.I.s). According to PECA, 2016, anybody who disrupts key information infrastructures will be held responsible for committing a crime. Furthermore, any interferences, alterations, damages, or unauthorized copying of vital information infrastructures are subject to increased penalties. Moreover, it is also linked to cyberterrorism. (Awan & Memon, 2016).

6.4 Why there is a need to Enhance Cyber Security Regulations?

The preceding discussion has shown that Pakistan is making an effort to satisfy the global demand for digital services. Staying current in the realm of digital technology is essential in this day and age. It has examined several forms of cybercrime involving money and people, including advance-fee scams, bank fraud, distributed denial of service attacks (DDoS), software piracy, email bombing, online spoofing, and electronic communications. The need for Pakistan to guarantee digital security on all fronts has been brought to light. Cybercriminals pose a significant danger to Pakistani national security, in contrast to more developed nations. As with many other developing nations, cybercrime is a serious issue in Pakistan. The primary obstacles to effectively managing these criminal activities include the ineffective reactive defense system, scarcity of e-forensic inquiry, lack of skilled personnel, and incongruity between local legislation and international norms. Pakistan should formulate a comprehensive set of cyber laws that may enhance the security measures for safeguarding national and financial interests. Due to the cross-border character of cybercrimes, criminals have more opportunities to carry out these threats (Kundi et al., 2014). Based on a study, there are around 10 to 15 daily reports of cybercrimes including activities such as unlawful money transfers, password cracking, account hacking, salami attacks, and internet spoofing (Zaheer, 2018,).

Pakistan has made several rules to fight these crimes. But these rules aren't enough to stop crooks from breaking the law online. To make the online world safe from dangers, not much progress has been made in this area (Rasool, 2015). Even though Pakistan has signed several international agreements, the country's government has not yet made internet rules that are in line with international law.

7. Conclusion and Recommendations

7.1 Conclusion

In Conclusion, the swift progress in the realm of information and communication technology has not only significantly transformed both the public and commercial sectors in Pakistan but has also led to a very alarming proliferation of cybercrime. Owing to its intangible character, cybercrime is the fastest-increasing kind of criminal activity in society. Individuals and the general public are not immune to the negative effects of digital technology. The security and integrity of information and data are very vulnerable in cyberspace. Offenders may access both an individual's mobile phone and an organization's computer. States are also vulnerable to intervention by cyber weapons.

The magnitude of this criminal menace is significantly impacting both personal and commercial transactions and therefore, the state by the same measure. With the increasing displacement of transactions and contact into cyberspace, their security continues to be profoundly susceptible. Despite some implementation of cybersecurity measures, the legislative framework of Pakistan, as outlined in the Prevention of Electronic Crimes Act (PECA) 2016, is deemed inadequate in effectively addressing the rapidly evolving cyber threats.

While the Federal Investigation Agency has historically been the exclusive body responsible for managing cybercrime, there is a growing sense of urgency for a comprehensive revision in the PECA 2016. Its various legal requirements and other enforcement complexities have been plagued by a lack of coherence and clarity. The Act requires exhaustive consideration by attorneys, civil society, and technological experts to achieve an optimal equilibrium in safeguarding digital rights and reducing cyber risks. The objective of the reform should be to enhance the public appeal of PECA and address fundamental concerns like freedom of speech, privacy, and data security. Therefore, the implementation of regulations for digital content should be grounded on a distinct framework that is autonomous and distinguishes cybercrime. It should prioritize the evaluation of the overall strengthening of Section 37 in relation to the banning of online material, in order to enhance these fundamental rights.

In addition, the government should enhance the law enforcement capabilities of the FIA by providing contemporary technological training coupled with a dedicated cyber forensic laboratory. Advancement of judicial competence in prosecuting cybercrime is necessary and might be facilitated by the establishment of a technical judicial advisory council. To achieve practical effectiveness in handling cybercrime cases, it is necessary to establish an autonomous judicial division that can direct its complete focus and concentration towards handling such cases, therefore allowing the courts to handle more grave offenses. Effective implementation of cybersecurity measures can only be guaranteed by widespread public knowledge and active involvement.

In order to enhance understanding of their respective responsibilities, the FIA and the PTA should conduct comprehensive campaigns addressing cybercrime reporting and the pertinent legislation. Moreover, the FIA must improve its reporting system by offering available hotline numbers 24/7 and simplifying the online procedures to encourage prompt and efficient reporting by the general public. The cybersecurity policy of Pakistan must be more explicit in terms of enhancing institutional capacity and strengthening legislative clarity, therefore enabling more involvement of the population. Through implementing such reform, it is possible to provide effective solutions to the socioeconomic consequences and significant risks presented by cybercrime, therefore establishing a more secure digital environment for the population.

7.2 Recommendations:

Based on the aforementioned study, the below suggestions are suggested for enhancing the legislative framework about cybersecurity and data privacy in Pakistan:

1. Cybersecurity and data privacy are important issues, and the government should start efforts to get the word out. Training programs for commercial companies, government employees, and police departments are one example.

2. Government spending on technical expertise and resource development should prioritize the recruitment of trained personnel and the provision of necessary tools and resources to the police force. As a result, the PTA and other government entities will be better able to uphold the cybersecurity and data privacy regulatory framework.

3. To guarantee a thorough and efficient legislative framework for data privacy and cybersecurity, the government should examine it and make necessary improvements. Some examples of this include tougher punishments for infractions, broader legal protections to account for emerging technology and risks, and enhanced safeguards for individuals' private data.

4. To make sure the cybersecurity and data privacy laws are implemented, the government should enhance cooperation between various government entities and interested parties. To fight cybercrimes, it is important to coordinate efforts, share information and intelligence, and define clear roles and duties.

5. To better address cybersecurity and data privacy concerns, Pakistan should collaborate with other countries. Cooperation may take many forms, including the exchange of intelligence and information, joint R&D projects, and coordinated efforts to fight transnational cybercrimes.

6. To prepare for any data breaches or cybersecurity incidents, the government should create a nationwide incident response strategy. Some examples of this include making sure everyone knows their part, outlining how to respond to incidents, and testing and updating the plan often.

7. Pakistan needs more qualified people to work in cybersecurity and data privacy, and the government should do more to encourage this. Among these measures might be the dissemination of information about available cybersecurity and data privacy jobs, as well as educational and training programs designed to attract qualified individuals to these sectors.

Pakistan may enhance the protection of its citizens' personal information and critical infrastructure from cybercriminals by implementing these recommendations, which would strengthen the country's cybersecurity and data privacy legislation and its ability to enforce them.

Funding
This article was not supported by any funding from public, commercial, or not-for-profit sectors.

Conflict of Interest/ Disclosures
The authors have disclosed that there are no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

References

Ahmad, T. (2021). E-Government in Bangladesh: Development and Present State. *International Journal of Social Science and Human Research*, *4*(01).

Ahmed, A. (2017). "Pakistan Among Top 10 Economies in Terms of its Internet Users," Dawn, October 4, 2017, https://www.dawn.com/news/1361586

Akram, M. M. U., & Abdullah, M. T. (2011). effective Enforcement Of Cyber Laws In Pakistan. *International Journal Of Science And Technology*, 1-15.

Akyeşilmen, N. (2016). Cyber Security and Human Rights: Need for a paradigm shift. Cyberpolitik Journal, 1(1), 32-55.

Alsunbul, Saad, Phu Dung Le, and Jeferson Tan. 2015. Deterring hacking strategies via targeting scanning properties. International Journal of Network Security and Its Applications 7 (4): 1–30.

Anderson, R., Barton, C., Rainer, B., Clayton, R., Ga, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the Changing Cost of Cybercrime. Workshop on the Economics of Information Security (WEIS).

Arshad Khan, E. (2018). The prevention of electronic crimes act 2016: An analysis. *LUMS LJ*, *5*, 117.

Bar, S. (2020). Israeli strategic deterrence doctrine and practice. *Comparative Strategy*, *39*(4), 321-353.

Basit, A. (2022). Af-Pak: One Year Since the Taliban's Return to Power. *Counter Terrorist Trends & Analysis*, *14*(4).

Bederna, Z., Szadeczky, T. 2020. Cyber espionage through Botnets. Security Journal 33: 43–62.

Beidleman, S. W. (2009). *Defining and deterring cyber war* (p. 0040). Carlisle: US Army War College.

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.

Bolger, P. C., & Walters, G. D. (2019). The relationship between police procedural justice, police legitimacy, and people's willingness to cooperate with law enforcement: A meta-analysis. *Journal of criminal justice*, *60*, 93-99.

Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. Bloomsbury Publishing USA.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8(1).

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2009. Roles of information security awareness and perceived fairness in information security policy compliance. AMCIS 2009 Proceedings, p. 419.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32*(5), 477-493.

Burr, R. (2015). To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. In *Washington, DC: 114th United States Congress*.

Cassidy, J. (2013). Why Edward Snowden is a hero. The New Yorker, 10.

Clark, G. (2002). The geography of law. In *New Models in Geography-Vol 1* (pp. 355-385). Routledge.

Collin, B. (1996). The future of cyber terrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, Denning, D. E. (2001). Cyberwarriors: Activists and terrorists turn to cyberspace. Harvard International Review, XXIII (2): 70-75.

Department of Defence.(2010). Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

EU Disinfo Lab. (2020, December 9). Indian chronicles: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15- year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

Fang, B. (2018). Cyberspace Sovereignty (3rd ed.). Springer, Beijing.

Firdous, M. A. (2020). Cyber Warfare and Global Power Politics. *CISS Insight Journal*, *8*(1), P71-93.

Futter, A. 2016, 'Is Trident Safe from Cyber Attack?', European Leadership Network, vol. 1, .

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry. International Food and Agribusiness Management Review, 21(3). https://doi.org/10.22434/IFAMR2017.0045

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

GSMA. (2020). Pakistan: Progressing towards a fully-fledged digital economy. https://www.gsma.com/asia-pacific/wp-content/uploads/2020/06/24253-Pakistan-report-updatesLR.pdf

Guinchard, A. (2011). Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy. Journal of Strategic Security, 4(2). https://doi.org/10.5038/1944- 0472.4.2.5

Halder, D. (2014). Information technology act and cyber terrorism: A critical review, Academia.edu, [Online]

Hiscox Cyber Readiness Report 2019. (2019). Network Security, 2019(5). https://doi.org/10.1016/s1353-4858(19)30057-1

Hua, Jian, and Sanjay Bapna. 2013. The economic impact of cyber terrorism. The Journal of Strategic Information Systems 22 (2): 175–186.

Hundley, R., Anderson, R. H., Arquilla, J., & Molander, R. C. (1995). Security in Cyberspace: Challenges for Society: Proceedings of an International Conference. https://www.rand.org/pubs/conf_proceedings/CF128.html

Iqbal, M., Talpur, S. R., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan. *Siazga Research Journal*, *2*(4), 273-282.

Iqbal, Z. (2021). Cyber Threats to Pakistan's Digital Landscape. Sustainable Development in a Digital Society, Lahore. https://sdpi.org/sdpiweb/publications/files/SDC-Anthology-2020.pdf

Iqbal, Z. 2019, 'Cyber Threats in Pakistan's Digital Landscape', Presentation, 22nd Sustainable Development Conference, Sustainable Development Policy Institute, Islamabad, Pakistan, .

Islam Z., Khan, M. A., & Zubair M. (2019). Cybercrime and Pakistan. Global Political Review, 4(2),

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.

Kar, D., & Spanjers, J. (2017). Transnational crime and the developing world. *Global Financial Integrity*, 53-59.

Karakus, O., McGarrell, E. F., & Basibuyuk, O. (2011). Public satisfaction with law enforcement in Turkey. *Policing: An International Journal of Police Strategies & Management*, *34*(2), 304-325.

Kemp, S. (2020). Digital 2020. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2020-pakistan

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

Kim, Eyong B. 2014. Recommendations for information security awareness training for college students. Information Management & Computer Security 22 (1): 115–126.

Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital Revolution, CyberCrimes And Cyber Legislation : A Challenge To Governments In Developing Countries. Journal of Information Engineering and Applications, 4(4), 61–71.

Liaquat, S., Qaisrani, A., & Khokhar, E. N. (2016). Freedom of Expression in Pakistan: A myth or a reality.

LJ Bikoko, T. G., Tchamba, J. C., & Ndubisi Okonta, F. (2019). A comprehensive review of failure and collapse of buildings/structures. *International Journal of Civil Engineering and Technology*, *10*(3).

Malik R. (2019, October 25). Cyber security challenges and solutions for banks, national institutions — II. The News.

Malik, T. (2014). Technology in the service of development: The NADRA story. *Center for Global Development*.

Malik, Z. U. A., Xing, H. M., Malik, S., Shahzad, T., Zheng, M., & Fatima, H. (2022). Cyber security situation in Pakistan: A critical analysis. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *19*(1), 23-32.

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

Mativat, F., & Tremblay, P. (1997). Counter-feiting credit cards, British Journal of Criminology, 37(2): 165- 83.

Mbinjama-Gamatham, A., & Olivier, B. (2020). 'Dark technology', aggressiveness and the question of cyber-ethics. Acta Academica, 52(1). https://doi.org/10.18820/24150479/aa52i1/1

Munir, M. A. (2010). Electronic crimes ordinance: an overview of its preamble and extent. *Pakistan Journal of Criminology*, *2*(1), 189-202.

Munir, M. A. (2010). Electronic Crimes Ordinance: An Overview of Its Preamble and Extent. Pakistan Journal of Criminology, 2(1), 189- 202. http://www.pjcriminology.com/wp-content/uploads/2019/01/14-5.pdf

Nadeem, M. A., Hashmi, S., & Khan, M. A. (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.

Nnam, M. U., Ajah, B. O., Arua, C. C., Okechukwu, G. P., & Okorie, C. O. (2019). The War must be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria. *International Journal of Cyber Criminology*, *13*(2).

Parikh, T. P., & Patel, A. R. (2017). Cyber security: Study on attack, threat, vulnerability. *2017 International Journal of Research in Modern Engineering and Emerging Technology*.

Paterson, Thomas, and Lauren Hanley. 2020. Political warfare in the digital age: Cyber subversion, information operations and 'Deep Fakes.' Australian Journal of International Afairs 74 (4): 439–4

Platt, Victor. 2012. "Still the fre-proof house? An analysis of Canada's cyber security strategy. International Journal 67 (1): 155–167.

PTA. (2020). Telecom indicators. Pakistan Telecommunication Authority. https://www.pta.gov.pk/en/telecom-indicators

Qarar, S. (2018). 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head. Dawn.

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. International Scientific Online Journal, 12, 21-34.

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal*, *12*, 21-34.

Robbins, P. (2000). The rotten institution: corruption in natural resource management. *Political Geography*, *19*(4), 423-443.

Rossi, A. (2014). *Sharing Secrets: Optimizing International Intelligence Cooperation to Counter Terrorism & Rising Threats* (Doctoral dissertation, Johns Hopkins University).

Senate of Pakistan. (2013). Report of the Senate Committee on Defence and Defence Production (6). https://www.senate.gov.pk/uploads/documents/1378101374_113.pdf

Shad, Muhammad Riaz. 2019. Cyber threat landscape and readiness challenge of Pakistan. Strategic Studies 39 (1): 1–19.

Shaikh, A. Z., Shah, U. L., & Wijekuruppu, C. (2016). Public service delivery and e-governance: The case of Pakistan. *International Journal for infonomics*, *9*(2), 1161-1170.

Soo, A. B., Zia, A., Sadiq, E., Raja, F. A., Suddle, S., Gul, I., ... & Salahuddin, Z. THE NAP TRACKER THE NAP TRACKER THE NAP TRACKER.

Stanton, Jefrey M., Kathryn R. Stam, Paul Mastrangelo, and Jefrey Jolton. 2005. Analysis of end user security behaviors. Computers & Security 24 (2): 124–133.

Statista. (2020). Pakistan: Internet penetration rate 2017. Statista. https://www.statista.com/statistics/765487/internet-penetration-rate-pakistan/

Tene, C. B., Omer, S., & Mempouo, B. (2017). Towards a coherent implementation of safe building laws and regulations in Cameroon: law, governance and institutional imperatives. *Journal of Sustainable Development Law and Policy (The)*, *8*(2), 87-109.

Ullah, S., Amir, M., Khan, M., Asmat, H., & Habib, K. (2015, November). Pakistan and cyber crimes: Problems and preventions. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-6). IEEE.

United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime. United Nations. https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Williams, D. A. (2019). Understanding effects of corruption on law enforcement and environmental crime. *U4 Anti-Corruption Resource Centre. Retrieved June*, *3*, 2020.

Williams, L. Y. (2008, March). Catch me if you can: a taxonomically structured approach to cybercrime. In *The Forum on Public Policy* (pp. 28-30).

Yasin M. (2021). Cyber Security and Cybercrime in a Digital Society. In Sustainable Development in a Digital Society (pp. 33-43). Sang-e-Meel publications

Zaheer, L. (2018). New media technologies and Youth in Pakistan. Journal of the Research Society of Pakistan, 1(55), 107–114

Zwilling, Moti, Galit Klien, Du.šan Lesjak, Lukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. 2020. Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems 62: 1–16.