15-SRJ-270-35

SIAZGA RESEARCH JOURNAL, 2023
VOL. 02, NO. 04, 273 – 282
DOI: https://doi.org/10.58341/srj.v2i4.35

ISSN(e): 2958-2164
ISSN(p): 0000-0000
DOI: 10.00000/SRJ
Siazga Research Journal
an open access research journal
A Quarterly Research Journal Published By:
Office of Research, Innovation and Commercialization
University of Loralai - Balochistan

Check for updates

Original Article

The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan

Muhammad Iqbal[a], Samar Raza Talpur[b], Amir Manzoor[c*],
Malik Muneeb Abid[d], Nazir Ahmad Shaikh[e] & Sanaullah Abbasi[f]

[a] Bahria University Karachi Campus, Pakistan
[b] Sukkur IBA University, Kandhkot Campus, Pakistan
[c] Karachi School of Business and Leadership
[d] University of Sargodha, Pakistan
[e] SZABIST, Karachi, Pakistan
[f] Federal Investigation Agency (FIA), Pakistan

Copyright © The Author(s). 2023
This is an open-access article distributed under the terms of the Creative Commons Attribute 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

How to cite:
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
https://doi.org/10.58341/srj.v2i4.35

Abstract

Cybercrime (e.g., hacking, phishing, and spreading false news) is a criminal activity performed through computing machines. The frequency of these kinds of activities is increasing at a fast pace around the globe and damaging society with financial losses and trust. Miniaturization of computing and the compulsion of web usage in our daily lives are two significant factors that are becoming more pervasive in a rapid increase of cyber security issues, making it a complex problem to tackle. The detection and prevention of cybercrime is paramount for any lawful country. Cybercrime can occur anywhere at any time, and ultimately, the outcome could be devastating. The availability of cyber laws is the first step towards resolving this issue. Still, unfortunately, Pakistani lawmaker institutions, i.e., the National Assembly and Senate of Pakistan, passed the Cybercrime Act very late, i.e., in 2016. Fighting against Cybercrimes in Pakistan is challenging because we still lack a professional workforce and technology. Pakistan is one of the major victims of this problem. This study mainly focuses on the legislation passed by the Government of Pakistan with the Prevention of Electronic Crimes Act, 2016" followed by analyzing these cyber laws in tackling cybercrime cases.

Keywords: Cybercrime, Cyber laws, Law enforcement, Legislation

1. INTRODUCTION

The growth of the Internet has been incredible for the past two decades, and it has become one of the fastest-growing technologies ever made. There were almost 361 million Internet users in the year 2000, and globally, the current count is nearly 4.574 billion (internetworldstats.com, 2023). According to a study conducted by Statista, a company dealing with business process data management, 48.2% of website traffic globally came from mobile phone devices in November 2018 (Singh & Bakar, 2019). Moreover, users downloaded 178.1 billion mobile applications from their mobile phone devices. Technology convergence also plays a pivotal role in our lives, and in this context, the three C's, i.e., Computers, Content, and Communication, are the main pillars of technology convergence.

Due to this technology convergence, you can see and share the same multimedia content on different digital devices today. With the proliferation of the Internet and mobile phone devices, south Asian countries have shifted drastically towards web platforms. Around 55% of the world's population lives in Asia and for the last decade, the use and popularity of web-based technologies has shown a significant increase. Table 1 presents the statistics about the Internet, Facebook, and cell phone user penetration in South Asian countries.

*Corresponding Author: Amir Manzoor, Karachi School of Business and Leadership
engr.dr.amir@gmail.com

Table 1
Internet penetration and other statistics for South Asian Countries

S.No	Country	Internet Users (Millions)	Penetration (%)	Facebook Users (in millions)	Cell Phone Penetration (in million)
1	Afghanistan	7.34	18.8	3.84	18.8
2	Bangladesh	96.2	58.4	34.71	31.05
3	Bhutan	0.4	51.5	0.41	0.8
4	India	560	40.6	251	345.92
5	Maldives	3.7	68.4	0.37	0.4
6	Nepal	16.2	55.6	10.42	39.3
7	Pakistan	71.61	32.4	37	32.5
8	Srilanka	7.17	33.5	6.43	14.85

The data clearly shows the very high penetration rate of internet users in almost all listed countries, but the figures for Bangladesh, Bhutan, Maldives, and Nepal are impressive. The number of FB and Smartphone users in the region is also increasing quickly, and India, Pakistan, and Bangladesh are the main drivers of this growth.

This fast growth of Internet technologies has also brought new challenges to our lives, and cybercrime is one of the significant threats to everyone who is a part of the Internet. Cybercrime incidents such as identity theft, Cyberstalking, phishing emails Malware etc. are taking place quickly. The convergence of different technologies on the Web also brings unconventional digital threat methods, such as hybrid warfare, which could be used to sabotage the opponent's actions. Globally and especially in Asia, the growth of cybercrime is at an all-time high, costing annually billions of dollars to organizations and individuals. Yeoh et al.(Yeoh et al., 2023) discussed the zero-trust cybersecurity model to replace the traditional perimeter-based security model.

Cybercrime fraud can be defined by the following:

$$\text{Cyber Crime Equation (C\_cr)= Dr+ Op + Rt --------------------(1)}$$

Where Dr denotes the desire of an individual or group, Op and Rt represent the opportunity and rationalization of cyber criminals.

Cybercrimes can happen anytime on the Web because of very lucrative financial opportunities through computers as a target and as a tool(Usman, 2017). In general, economic motives are behind an individual's desire to engage in unlawful or unethical activities, which is valid for cybercriminals. Crimes require opportunity and suitable environmental conditions for corrupt practices, which presents opportunities to cybercriminals for crime. We believe that opportunity has a significant role in committing any cybercrime by potential offenders.

In most cases, the people justify their criminal behavior by psychologically distorting the true intention behind their criminal act. If the cyber-attack is politically motivated in Pakistan, people regard it as a great cause. This kind of defense mechanism is known as rationalization. To share the sternness of cybercrime issue, a well-known cybersecurity company, Malwarebytes (Malwarebytes, 2020), revealed a massive increase in security breaches and reported that more than 200,000 cyberattacks happen daily, which include ransomware, phishing attacks, and malicious scans.

Cybersecurity Ventures(Morgan, 2022), a leading research and IT company reveals that global cybercrime cost is continuously rising, with a 15% increase yearly and reaching around 8 trillion USD by 2023, which was 3 trillion USD in 2015. Worldwide, there is about a 102% increase in crimes involving ransomware in the first half of 2021 compared to the beginning of 2020. A large number of victims of ransomware criminal groups belong to rich countries. Fig.1 reports the countries most attacked by ransomware attacks(Morgan, 2022). Ransomware attacks cost its victims billions (USD) annually.

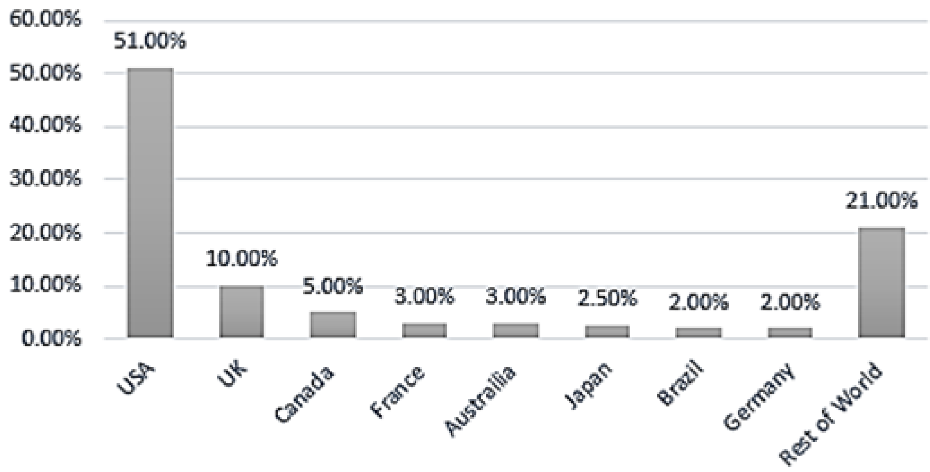

Figure 1: Countries Targeted by Ransomware

Figure 2 depicts the annual damages in billions (USD) due to cyber-attacks. Cyber Security Ventures (Morgan, 2022) revealed in their report that in just two years the world witnessed a 15x time increase in ransomware damages.

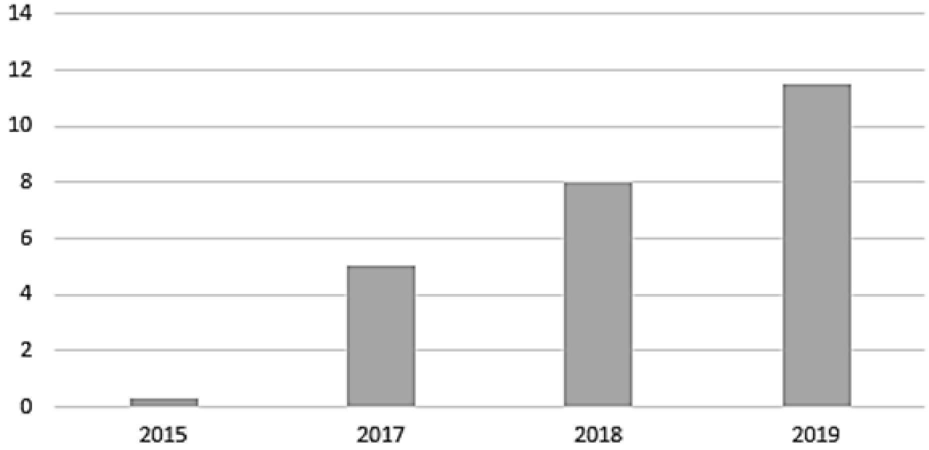

Figure 2: Estimated Damage of Ransomware Worldwide (in billions of US dollars)

Figure 3 provides relevant information about cybercrime damage costs in trillions (USD) to organizations worldwide. Cybersecurity deals with several cyber-attacks such as Malware, ransomware, DoD/DDoS, man-in-the-middle attack, SQL Injection, etc. Cybersecurity is the art of saving confidential information of individuals and organizations from unpasteurized access. Fig. 3 shows the amount of damages in trillion US dollars due to cyber-attacks.

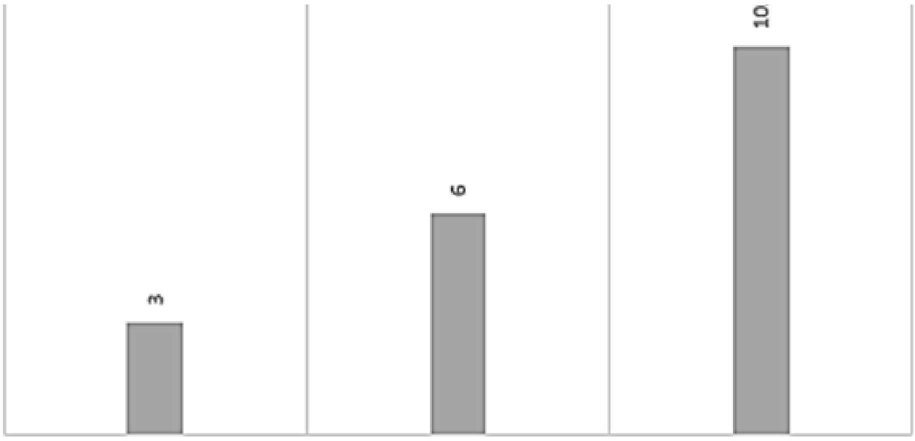

Figure 3: Estimated Cost of Cybercrime Damages (in trillions of US dollars)

For the last decade, Pakistan has witnessed an exponential growth in cybercrimes, especially in financial fraud. In 2020, there were 84,764 registered cybercrime complaints; out of this, 20,218 complaints were of financial fraud. Another important fact about Pakistanis is that most people use social media platforms for cybercrimes. The first half of 2021 saw a 102% increase in cybercrime involving ransomware compared to the beginning of 2020.

The Global Cybersecurity Index (GCI) (ITU, 2021) is an initiative of ITU-T to rank countries to judge their commitments in dealing with cybersecurity issues. GCI is a trusted reference. It has five important pillars, i.e., legal, technical, organizational, capacity development, and cooperation. Pakistan has been trying to curb cybersecurity issues for the past few decades. According to the International Telecommunication Union (ITU), the USA is the most committed country regarding cybersecurity readiness, and Canada received second rank. Pakistan ranks very low in terms of Cyberwellness.

According to the National Response Centre for Cyber Crime (NR3C)-FIA (NRCC, 2023), cybercrime has become a serious threat to the people of Pakistan. It suggests digital device users who don't use computing devices without the compliance of modern security tools. In the Year 2019, NR3C-FIA registered 27,214 cybercrime cases. Moreover, major cases were associated with misuse of Social Network Sites and buying/ selling via fake credit cards. This number is huge as compared to previous figures reported by FIA. In 2018, the total number of registered cases was 19,014; in 2017, the number was 9364; in 2016, there were only 9,075 cases registered by the agency(Shakeel, 2018). A three-year summarized view is shown in Table 2.

Table 2
Summary of Cyber Crimes

Year	Inquiries conducted	Registered cases	Arrests made
2016	514	47	49
2017	1290	207	160
2018	20295	255	209

Source: Shakeel (2018)

However, it can be said that most of the cybercrime cases were not reported by citizens due to a lack of knowledge about cyber laws, the nonprofessional attitude of the police, and the complex judicial system in Pakistan. Moreover, the digital threats are increasing at a fast pace. According to numerous studies, cybercrime's economic and social impact has risen exponentially. Unfortunately, it continuously evolves because cybercrime requires less effort and cost. According to a report compiled jointly by the Center for Strategic and International Studies (CSIS) and McAfee, cybercrime may now cost almost $600 billion, or 0.8% of global GDP(McAfee, 2022). Cybercrimes have had a massive impact on the global economy, and now it has become a challenge for the research community to find appropriate solutions to eliminate this problem. Cybercrime is an unethical activity that mostly takes place via the Internet. Fig. 4 shows the most common cybercrime acts. Broadly, cybercrimes are divided into two categories. Viruses, Malware, and DoS attacks are examples of cybercrimes originating from Networks, whereas phishing emails, cyberstalking and identity theft are some examples of cybercrimes produced through devices.

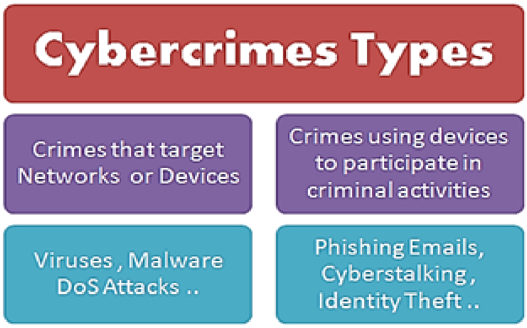
Cybercrimes Types
Crimes that target Networks or Devices
Crimes using devices to participate in criminal activities
Viruses , Malware DoS Attacks ..
Phishing Emails, Cyberstalking , Identity Theft ..

Figure 4: Types of Cyber Crimes

Cyber security is a complex issue for the whole world because every country has its jurisdiction. A global team effort is needed to introduce effective laws locally and internationally. Additionally, there is a need to introduce a uniform and robust security defense technology to fight against cybercrimes. Eesha (Arshad Khan, 2018) discussed the importance of cyber laws to curb this negative phenomenon but not at the cost of citizens' rights.

The research objectives of this study are:

- To highlight the importance of cyber laws in general and PECA in particular
- To emphasize the need for a layer collaborative structure to deal with cyber security issues

The outline of the study is as follows. Section 2 covers the layered model to address cyber security issues. Section 3 presents the significance of cybercrime laws. Cybercrime Prevention and Detection methodology has been discussed in section four, while the tools for crime detection have been discussed in section 5.

2. SYSTEMATIC LAYERED STRUCTURE FOR CYBERCRIMES

Governments need a well-defined collaborative structure to deal with cybercriminals. Such a structure could help to produce an effective cyber security mechanism. Three vertical pillars are Cyber Security Laws, IT tools, and people, while two horizontal pillars are Prosecution and implementation. These pillars are defined as expertise of governance structure. Fig. 5 shows the five-layered model, where each layer's role is significant in cyber security.

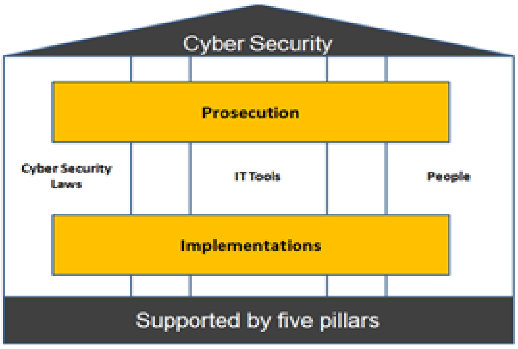

Figure 5: Layered Model of CyberSecurity

Cyber Security Laws

The first pillar of structure is the state's availability of cyber security laws. A well-defined cyber law can help government institutions mitigate cybercrime curses from society. Additionally, it gives knowledge to operate and evaluate the effectiveness of cyber security systems. However, cyber laws need continuous monitoring to update their contents regularly because most cybercrimes appear on web podiums with new threats.

Globally, the government's role is crucial in countering cybercrimes by introducing and implementing efficient cyber laws. Moreover, the role of cyber enforcement agencies is also very significant to prosecute cybercrimes in such a way as to ensure severe punishment of the executors. American "Computer Fraud and Abuse Act (CFAA)-1986", European "Union's General Data Protection Regulation (GDPR)" and California Consumer Privacy Act of 2018 (CCPA), Indian "IT Act 2000" and Bangladesh's "The Information and Communication Technology (ICT) Act, 2006" are some excellent examples set by different countries to address this issue. Pakistan introduced its first legal framework to cover digital threats in 2002 through the Electronic Transactions Ordinance, but it only covers a few cybercrimes. The current cyber act, i.e., Pakistan Electronic Crimes Prevention (PECA), was enacted in 2016(Government of Pakistan, 2023). Even though the PECA was introduced very late in Pakistan, its preamble states that the scope of this law is extensive to address cybercrimes. However, critics from different corner of society call it a controversial draft because they believe this bill restrict some fundamental rights of the citizen guaranteed in the constitution of Pakistan.

IT Tools

The second pillar of the cyber Security structure is Information technology tools. Using appropriate software and hardware tools can help identify cybercriminals and their allies. In addition to using these sophisticated tools, people can protect themselves by following some standard best practices, such as the use of strong passwords, applying strict social media settings, applying software updates, Do not download any application from an unknown source before surfing on the website check the legitimacy of it, always use VPN connection for Wi-Fi connectivity, etc.

People

The third pillar of the cyber security structure is a professional workforce. Without the support of the right people, an effective security system cannot run. A trained and professional team is vital for an effective security system. Moreover, the team must get training before accessing the security systems.

Additionally, they must be educated about the consequences and risks of not complying with the standard operating procedures.

Prosecution

On the Internet, there is no physical appearance of offenders. It is challenging for cyber law enforcement agencies to track and identify exact culprits. In cybercrime investigation, there is no need for physical analysis, but to reach culprits, the prosecutors need sophisticated hardware/software tools.

Implementation

To fight against cybercrimes, the government of Pakistan has continually updated laws through legislation. However, the role of the judiciary and law enforcement agencies is very significant in reducing criminal activities in the country. Through proper implementation of laws and by giving severe punishments to perpetrators, we could be able to provide a cybercrime-free society.

3. GENERAL INTRODUCTION OF PAKISTAN ELECTRONIC CRIMES PREVENTION (PECA)

Cybercrime is any crime committed through a computer, organized gadget, or a system. A cybercrime (for example, extortion, robbery, or dispersion of child pornography) is perpetrated utilizing a PC. Various countries have embraced multiple techniques to fight cybercrimes. A country with a higher rate of cybercrime cannot prosper or develop. Laws are rules that bind all people living in a community. Laws protect our general safety and ensure our rights as citizens against abuses by other people, organizations, and the government itself. A brief history of cybercrime laws introduced by the federal government of Pakistan is shown in Fig. 6.

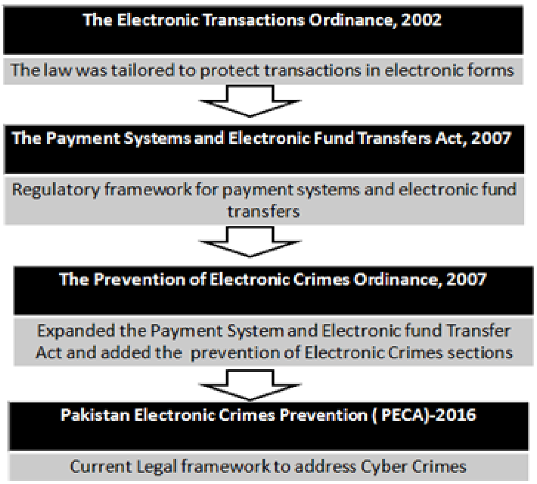
The Electronic Transactions Ordinance, 2002
The law was tailored to protect transactions in electronic forms
The Payment Systems and Electronic Fund Transfers Act, 2007
Regulatory framework for payment systems and electronic fund transfers
The Prevention of Electronic Crimes Ordinance, 2007
Expanded the Payment System and Electronic fund Transfer Act and added the prevention of Electronic Crimes sections
Pakistan Electronic Crimes Prevention (PECA)-2016
Current Legal framework to address Cyber Crimes

Figure 6: History of Cyber Laws in Pakistan

The Electronic Transaction Ordinance (ETO) of 2002 was the first IT legislation introduced by lawmakers. ETO was the first legal framework that supported e-commerce, electronic documentation, electronic records, electronic signatures, Forensic evidence, etc. There were 43 sections in this ordinance. The ETO was considered the first step towards dealing with cyber threats. In 2007, "The Payment Systems and Electronic Funds Transfer Act" was formed to deal with new challenges of electronic crimes faced by citizens of Pakistan. The bill deals with cyber terrorism, data damage, electronic fraud, electronic forgery, cyber stalking, cyber spamming, unauthorized access to code, etc. Moreover, this bill also gives executive powers to the FIA for investigating and framing charges against cyber criminals. This bill covers 21 cyber issues. However, this bill faced criticism from civil society because they believe it gives maximum powers to cybercrime regulators, i.e., FIA, to mystify and entrap innocent people.

The President of Pakistan promulgated the Prevention of Electronic Crimes Ordinance 2007 to give legal coverage of some existing cybercrimes. Unfortunately, these ordinances were not tabled in the parliament and lapsed after 120 days from its enactment. In 2016, the parliament passed PECA, but it was also criticized by civil society because they thought it restricted the freedom of speech assured in the constitution of Pakistan. Moreover, loopholes in PECA supported the corrupt bureaucratic system. Additionally, this law did not cover many existing cybercrimes. However, PECA has somehow become a viable medium in achieving a good social change in the nation, because now public in large understand that the Laws exist and they could be convicted by doing unfair means on the Web. In this way, we revive our conviction that law has been crucial in presenting changes in the cultural structure and connections and keeps on being so. Table 3 depicts the summary of significant clauses of PECA.

Table 3
Major Clauses of PECA-2016

S.No	Section	Cyber Crime	Years in Prison	Financial Penalty (in PKR)
1	3	Unsanctioned access to system or data	3 Months	50,000
2	4	Unsanctioned copying or transfer of data	6 Months	100,000
3	5	Interference with system or data	2 Years	500,000
4	6	Unsanctioned access to critical system or data	3 Years	1 Million
5	7	Unsanctioned copying or transfer of critical data	5 Years	5 Million
6	8	Interference with critical system or data	7 Years	10 Million
7	9	Deification of an offense	7 Years	10 Million
8	10	Cyberterrorism (Threat)	7 Years	10 Million
9	10A	Hate Speech	7 Years	10 Million
10	10B	Recruitment, funding, and planning of terrorism	7 Years	PKR 10 Million
11	11(1)	Forgery using electronic means	3 Years	PKR 250,000
12	11(2)	Forgery (using electronic means) with critical system or data	7 Years	PKR 5 Million
13	12	Fraud using electronic means	2 Years	PKR 10 Million
14	13	Developing, getting access to, or supplying devices to be used in crime.	6 Months	PKR 50,000
15	14	Unsanctioned use of identitification information.	3 Years	PKR 5 Million
16	15	Illegally issue mobile SIM card	3 Years	PKR 0.5 Million
17	16	Interfering with communication devices	3 Years	PKR 1 Million
18	17	Unsanctioned Intervention	2 Years	PKR 0.5 Million
19	18	Crimes against dignity of a natural person	3 Years	PKR 1 Million
20	19	Crimes against the modesty of a natural person/minor	5 Years	PKR 5 Million
21	19A	Child pornography	7 Years	PKR 5 Million
22	20	Malicious code	2 Years	PKR 1 million
23	21	Cyberstalking	3 Years	PKR 1 Million
24	22	Spamming	3 Months	PKR 50,000
25	23	Spoofing	3 Years	PKR 50,000

4. CYBERCRIME PREVENTION AND DETECTION

The digital forensic process is a critical element in catching culprits of cybercrimes. This process has five steps, as shown in Fig. 7.

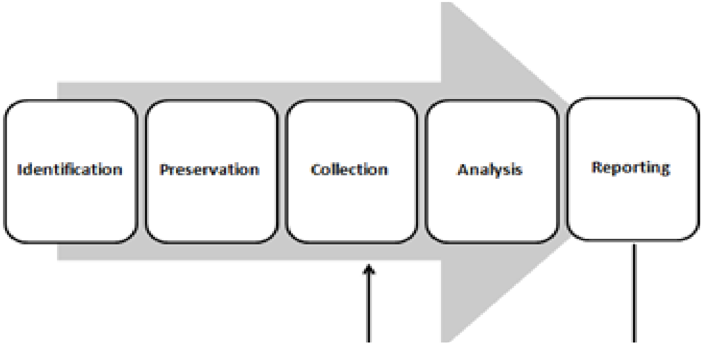

Figure. 7: General model of Digital Forensic Process

Below is a brief explanation of each step

Identification: The first step towards digital forensics is to identify relevant sources of crime, i.e., evidence/information (devices). It is also essential to know about key custodians and the location of data.

Preservation: In this step, the incident scene is captured by retrieving visual images of the scene along with all electronically stored information. All pieces of evidence are documented so that the incident should be reported as crime actions have been executed in sequence.

- Collection: In this step, the digital information must be stored in such a format that it must be understood by available forensic tools. Moreover, the removal of electronic devices that/were used in cybercrime is very important.
- Analysis: The analysis must process and analyze data to reach a conclusion about digital crime cases. All pieces of evidence must be thoroughly investigated so as to draw a conclusion of the case.
- Reporting: Finally, the reporting phase comes, where comprehensive reports must be compiled. The produced reports must be in compliance of approved methodologies and standards followed worldwide.

The arrow from the reporting phase towards the collection phase indicates that reported evidence is iterative and reproducible. Computer forensic investigation is growing, and its usage is pivotal in law enforcement and legal entities. In Computer forensic investigation, investigators track digital activity through digitally stored information, which leads to physical evidence of unlawful activity.

5. ISSUES

Cybercrime is a complex and diverse phenomenon that is expanding at a fast pace in Pakistan. Unfortunately, Pakistan did not address this issue seriously because, until PECA 2016, we had no proper legislation on cybercrimes. To combat this severe issue much still has to be done by all stakeholders. The following issues create hurdles to tackling cybercrimes in Pakistan.

Legislation against Cybercrime

The PECA 2016 laws are not sufficient to completely handle cybercriminals and protect Pakistan's cyberspace. For instance, PECA 2016 only penalizes unauthorized access, spoofing, Interference, hacking, etc., and does not provide penalties to those who harass others and share abusive material on social media. For example, if the objectionable video content is not removed within one hour in the European Union, the platform publishing the content must pay a huge fine.

Public Awareness

The biggest challenge in Pakistan is that the general public is not educated on the devastating effects of cybercrimes. The public at large, and especially the youth of Pakistan, must understand the consequences of the violation of cyberspace in Pakistan. In this regard, Pakistan has to establish cybersecurity education working group(s) within national and provisional levels to educate students at elementary, middle, and high school levels.

Weak Prosecution

Sophisticated Prosecution is the first step towards punishing cyber criminals. Unfortunately, Pakistan does not meet the required legal and Prosecution expertise. Our argument is supported by the results of Table 2, where there is a huge gap between inquiries conducted and arrests made. The National Response Centre for Cyber Crime (NR3C) is facing considerable evidential and procedural challenges to address this issue, indirectly affecting Prosecution's success rate.

Lack of Information Sharing and Coordination among the Stakeholders

A good prosecution requires collaboration and transparency from various law enforcement agencies and other stakeholders. With different organizational structures. It is challenging for prosecutors to bring practical conclusions in cases due to a lack of information sharing and coordination among various departments.

Lack of Proper Training of Law Enforcers

The state of cybercrime and cyber criminals and the nature of law enforcement keeps changing. At present, investigators are facing multiple challenges, especially in keeping themselves updated with complex technologies to help curb cybercrimes from cyberspace.

6. TOOLS FOR CRIME DETECTION

The role of forensic sciences is very significant in detecting serious cybercrimes. Fingerprint identification technology is considered to be the first significant achievement in identifying individual crimes. However, with the advent of Information Technology, numerous cybercrime detection tools have been used to curb internet crimes. Accurate crime pattern detection is challenging for these Software/Hardware tools to investigate criminal motives and behavior. The detected patterns can be helpful for investigators to predict, anticipate, and prevent cybercrimes. The automated tools do not have 100% capability to predict the cybercrimes. Therefore, most cyber analysts use manual processing to detect specific patterns of cybercrime(s) performed by an individual or group of people. Most of the crime detection tools can perform memory forensic analysis, hard drive forensic analysis, cell phone forensics, and forensic image exploration (Okutan, 2019).

The following is a list and brief description of the most widely used forensic tools

- ProDiscover Forensic is a popular cyber security application that allows you to generate forensic reports for legal requirements. It protects evidence and can be retrieved from the computer Disk. ProDiscover is a proprietary Software widely used by law enforcement organizations. This tool is designed for Windows, MAC, and Linux File systems. This tool creates a copy of all suspected files of HDD to keep evidence.
- EnCase©, is a widely acceptable digital investigation application. This tool helps the forensic practitioners to dig out required evidence from computers and cell phones. Through his tool, you can unlock encrypted pieces of evidence. It also offers flexible reporting options.
- Sleuth Kit (+Autopsy) is a Windows-based forensic tool that helps forensic investigators retrieve crime evidence from computer systems and mobile devices. The tool also extracts the data from call logs, contacts, SMS, etc. The tool kit is specially designed to examine the email's metadata.
- Paladin is considered one of the most effective forensic tools available today. This toolkit is classified into 33 different categories. Paladin can help forensic investigators to catch different cybercrimes such as data leaks, unauthorized access, spyware, Malware, and weak passwords.
- CAINE (Computer Aided Investigative Environment) provides an interactive graphical user interface (GUI) to perform various digital forensic activities. This application is designed to address three forensic activities i.e., Database, memory, and Network. It is a live distribution Software and does not need any installation on a computing system. It can be carried out on USB/PEN drives.
- AccessData, a multinational software company, developed FTK Imager and is very popular in the cyber security industry. This software offers extensive features, such as results presented in graphs, and offers a wizard-driven approach to detect digital crimes.

7. DISCUSSION & CONCLUSION

With the tens of thousands of cybercrimes emerging and evolving daily, it would be incorrect to say that it is possible to eradicate cybercrime completely. Even if agencies and lawmaker bodies take all necessary actions to prevent it, it is nearly impossible to completely and fully prevent these incidents. Furthermore, especially in developing countries like Pakistan, which have other major problems and economic deficiencies, cybercrime and the implementation of its laws is not the most crucial problem that the state wants to deal with. Hence, not much importance is usually given to an issue that is most prevalent and equally important in terms of national security and the well-being of the citizens. Furthermore, since Pakistan is a nuclear state and it has a significant geopolitical position in the region, various internal and external security threats have arisen during the last decade concerning cyber security.

Pakistan is part of the league of countries with proper laws and legal framework regarding cyber laws protecting its citizens and promoting safe Internet use. However, the lack of implementation of these laws gives rise to these crimes and encouragement to such criminals. Hence, enforcement and amendment of laws that are already in place is most important. Another important step that the government of Pakistan can potentially take is the sensitization to the phenomenon of cybercrimes. The government should establish awareness programs regarding anti-cybercrime-related activities. Trained personnel with knowledge of internet and computer crimes should guide people, especially those involved in IT-related fields, to not only detect unlawful activity but also indulge in ethical internet usage. However, in line with all of this, it is also important that during enforcement of these laws, people's privacy, freedom of speech, and rights of citizens are not compromised. Hence, lawmaker bodies should keep in mind that Pakistan is a democratic state, and safeguarding citizens' rights is the government's utmost responsibility.

Competing Interests

The authors did not declare any competing interest.

References

Arshad Khan, E. (2018). The prevention of electronic crimes act 2016: An analysis. LUMS LJ, 5, 117. Government of Pakistan. (2023). The Prevention of Electronic Crimes Act, 2016.

https://na.gov.pk/uploads/documents/1470910659_707.pdf

internetworldstats.com. (2023, September 30). Internet Growth Statistics 1995 to 2023—The Global Village Online.

https://www.internetworldstats.com/emarketing.htm

ITU. (2021). Global Cybersecurity Index (GCI) 2018.

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Malwarebytes. (2020). State of Malware-Online.

https://resources. malwarebytes .com /files /2019 /01 /Malwarebytes -Labs -2019 -State -of -Malware -Report -2 .pdf

McAfee. (2022). The Economic Impact of Cybercrime—No Slowing Down.

https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Morgan, S. (2022, October 13). Cybercrime To Cost The World 8 Trillion Annually In 2023. Cybercrime Magazine.

https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

NRCC. (2023, September 30). National Response Centre For Cyber Crime.

https://www.nr3c.gov.pk/cybercrime.html

Okutan, A. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287–294. Shakeel, Q. (2018, October 23). Cybercrime reports hit a record high in 2018: FIA - Pakistan—DAWN.COM

https://www.dawn.com/news/1440854

Singh, M. M., & Bakar, A. A. (2019). A systemic cybercrime stakeholders architectural model. Procedia Computer Science, 161, 1147–1155.

Usman, M. (2017). cyber crime: Pakistani perspective. Islamabad Law Review, 1(03), 18–40.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computers & Security, 133, 103412.