International Journal of Business and Economic Affairs (IJBEA)
7(1), 10-22 (2022)
DOI: 10.24088/IJBEA-2022-71002
ISSN: 2519-9986

Critical Analysis of Cybercrimes in Pakistan: Legislative Measures and Reforms

Jibran Jamshed [1]*, Waheed Rafique [2], Khurram Baig [3], Waqas Ahmad [4]

[1] Assistant Professor, Department of Law, The Islamia University of Bahawalpur, Bahawalpur, Pakistan
PhD Scholar Gillani Law College, Bahauuddin Zakariya University Multan, Multan, Pakistan

[2, 3] PhD Scholar Gillani Law College, Bahauuddin Zakariya University, Multan, Pakistan

[4] Lecturer Times Institute Multan, Pakistan

Abstract: Cybercrimes are increasing at a rapid pace in Pakistan. The current study explores the issue of cybercrimes in Pakistan. It aims to explore all the legislation dealing with cybercrimes in Pakistan. The study first described the cybercrimes and all those factors that are responsible for the cybercrimes. It explored all the common methods employed by criminals for cybercrimes. The study then critically evaluates the law dealing with cybercrimes in Pakistan. It analyses and evaluates the procedure of Federal Investigation Agency (FIA) which is responsible primarily for dealing with cybercrimes in Pakistan.The Population is selected from Pakistan southern area of total users online devices internet and e-commerce . Where electronically cybercrime is commend. Total sapmle size is 297. To collect data asurevy is adapted. The data will be anlysied via softwre Smart PLS. The findings of this study enhance public awareness and contribute to academic. The results are implacable to further study and useful for researchers and publically well being mission. The main addition of this resaech is to analyse the cyber crime activities that are now a days performed by mny hackerds in all over the world. Mostly in Paksitan So, this is a great advancement in research.

Keywords: Cybercrimes, Reforms, Federal investigation agency, Itelectual property, Legislative measures, Pakistan

Received: 29 October 2021/ Accepted: 19 December 2021/ Published: 23 January 2022

INTRODUCTION

Cybercrime is the most rapidly growing criminal activity on the planet. Any electronic device is used in the commission of a crime, or any electronic device is targeted for the commission of that crime. It's a crime that jeopardizes an individual's safety and financial well-being, as well as national security (Mohiuddin, 2006). Most, but not all, cybercrime is committed by criminals seeking financial gain. Cyber Crime is a broad term that refers to any illegal activity that involves the use of computers, the internet, or the use of a computer as a tool to conduct an offense. Cybercrime, often known as computer-oriented crime, it's the usage of computers for criminal purposes such as committing fraud, dealing with child pornography, and exploiting security and intellectual property (Anderson et al., 2013).

The world's population has surpassed 7.5 billion people. As a result, the internet is used by half of the world's population. In the last year, there has been a 10% growth in internet users, a 21% increase in global social media users, and a nearly 30% increase in mobile social media users. Nearly half of all people now use their mobile to access social media. When we specifically discuss Pakistan, we find that 44 percent of Pakistanis use social media. Now a day, the effective mode of communication is through social media. As the number of people using social media grows, so do the number of issues that arise. People may suffer from physical and emotional issues as a result of their excessive use of social media, according to research. Cybercrime is increasing gradually as a result of excessive usage of social media from majority of those affected with are women and children.

Social Responsibility Theory In the middle of the twentieth century, many of the third world and underdeveloped countries used this concept of the press that was associated with "the commission of the liberty of Press" in the U.S.

*Corresponding author: Jibran Jamshed
†Email: jibran_jamshed@yahoo.com

in 1949. Social Responsibility theory believes in the free flow of information without any censorship on it but at the same time the contents of the media must be mentioned in the public panel and the media organizations or personnel should feel their responsibility towards the society they are living in and should filter their content according to the acceptance level and requirements of the society. It does not believe in external control over media contents but emphasizes that there should be a system of internal accountability. The ownership thence stands exclusive. The concept of social accountability passes the easy "goal" of information reporting to investigative reporting. The speculation helps develop professionalism within the media organizations with the help of establishing a higher standard of professionalism, accuracy, and knowledge. The theory enables:

- Every individual to claim something or express his/her opinion regarding the media.
- Group opinion, customer motion, and work ethics.
- Serious invasion of critical social interests.
- Asad Munir and Ghulam Shabir Page | 90 Global Political Review (GPR)
- Personal ownership of media can ensure better public service besides of government's take over.
- Media ought to feel the social responsibility and if they do not, the government or other organizations will do.

The theory of social responsibility was associated partially to this study to the extent that social media demands social responsibility from both the regulators as well as the users. The study engages different implications and aspects of Social Responsibility Theory and emphasizes intensive knowledge of possible consequences and vulnerability while using the internet especially social media. It further highlights the role of public institutions in setting the guidelines and making policies for better, healthier, and safer use of the internet. Social Learning Theory Bandura (1977) presented the Social Learning Theory after a series of studies proposing that people can learn from each other. They learn through observation and imitation. They also learn through modeling certain models. This learning is also based on their attention, the amount of memory engaged, and motivational factors behind that. He further suggests that human behavior is a product of different influences that include:

- Cognitive influences
- Behavioral influences
- Environmental influences

The theory further highlights some characteristics that help achieve effective modeling. These are:

- Attention
- Retention
- Production
- Motivation Different aspects of Social Learning

Theory relate to the current study such as learning from the society, learning from others, learning about different kinds of cybercrimes from friends, family, social circle, and the internet itself. Awareness and learning are some important components of the current study and social learning theory fits it to a good extent. Awareness of common cybercrimes such as spoofing, hacking, phishing, tormenting, and cyber terrorism is indispensable (Munir, 2018).

Many people are unaware that they are committing cybercrime. Cybercrime includes making several posts on Facebook, Instagram, and other social media platforms without verifying them, and then having people share or circulate those posts. According to the Digital Rights Foundation, 51 percent of Pakistani women have experienced psychological maladjustment as a result of internet harassment. According to research, 7 lac 63 thousand 265 URL pornographic material, 31 thousand 963 insulting material, 10 thousand 106 proxy websites, 4 thousand 799 national against, 3 thousand 219 judiciaries against, and roughly 1 thousand websites have been blocked as a result of religion contempt spreading and dishonorable material (Holt etc al., 2017).

Objctive of the Study

These criminal activities or the offense/crime related to the internet is termed as cyber crime. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues

Historical Background

The fact that the "Abacus" was regarded the first form of computer is not surprising. According to the investigation, a pair of crooks hacked “A French Telegraph System” in 1834 and stole financial and market information. It is widely regarded as the first Cyber Attack in history (Skertic, 2021). Then, as time goes on, the number of cases of cybercrime rises. The first spam email was sent and received in 1976, and the first virus was installed in an Apple Computer in 1982 (Welles, 2021).

It was one of the world’s largest cyber heists, an online-era bank robbery that no amount of armed guards, defensively shielded cars, or tightly secured vaults could prevent; it resembled a terroristic attack on the national bank. Hackers stole more than 80 million dollars from Bangladesh’s National Bank, which was regarded as one of the world’s most reputable financial organizations who may have exploded like a bomb (Business and Economy News). The vast majority of the funds have yet to be retrieved; there is no way this could have been accomplished by a few unscrupulous employees.

Cybercrimes in Pakistan

The term "cyber" is short for "computer induced reality." It has to do with electronic connection networks, especially the internet, which is the mother of all media network connectivity. The internet revolves around cyber technology, which includes the progression of information in phones, computers, and computer games, among other things. Our reality was astonished by the internet, which now plays a significant part in the development. Because they have access to online technology, even the automobiles we drive or the television we watch are examples of cyber innovation. Internet access has been available in Pakistan since the nineteenth century. Pakistan Telecom Company Limited began providing access to all cross-country consumers, however cybercrime began to emerge in our culture. When the internet was first introduced, paper work was reduced, and manual business was moved to the internet, and manual business was replaced by computer. However, it is beneficial for people or a blessing, it also has negative consequences, such as instances of deceit, fraud, misrepresentation, and other criminal activities carried out over the internet or computer. There was no usual practice in place at the time, and criminals roamed free (The News).

It’s a crime that usually occur online. Hackers frequently commit cybercrimes by focusing their efforts on computer systems or modern devices. Cybercrime is typically committed by individuals or small groups. However, large crime syndicates use and abuse the internet. These “advanced” cyber criminals invent new ways to commit old crimes in new ways, treating cyber - crimes as a business and framing global criminal networks. Criminal organizations share techniques, schemes, and methods, and they can join forces to release coordinated attacks. They already have an underground production network where cybercriminals can buy and sell hacked information and identities. Cyber Crime is divided into several categories, including Cyberbullying, Hacking, Data Theft, Financial Theft, Money Laundering, Malware, and Electronic Terrorism. As a result, cybercrime is involved in a variety of ways by employing various attack techniques by cybercriminals (Sinrod & Reilly, 2000).

The age ratio in cybercrime varies on the case. According to the FIA Cyber Crime cell, they apprehended a businessman, a sales person or a vegetable seller, so the ratio varies by age. However, the majority of cybercriminals are between the ages of 18 and 28. Some cyber criminals commit social media crimes, while others only seek financial gain, such as hacking ATM pins, forging prize bond notifications, and so on. Finally, some criminals steal people’s personal identification information. Last year, the alleged cyber criminals were 17 years old, associated to 24 years the previous year (Britz, 2009)

Pakistan is engaged in two wars: one against terrorists, and the other against cybercrime and its security. There are over 50 countries that have introduced their cyberspace and cyber security systems. Pakistani intelligence agencies begin striving to safeguard, secure, and keep citizens’ personal data, information, and secrecy from unauthorized access. As a result, Pakistan develops its security policy and begins to raise awareness among individuals through workshops and seminars held at various colleges and universities (McQuade, 2006).

The National Security Agency (NSA) has issued a report to Pakistan outlining security flaws in the country and how digital data could be used for unlawful purposes. According to the NSA assessment, the Pakistan Senate defense committee, as well as PIPS and PISA, are responsible for the results of the cyber security restrictions imposed on Pakistan on July 8, 2013. Pakistan is now taking effort to combat cyber threats to the country. Experts are hired from NUST, LUMS, RIPHA, and Pakistan Information Security Association’s online services. In November

2018, 624 customers from 22 banks suffered over $11.7 million in cash as a result of a cyber-attack. According to a verified report from the FIA, the data of 19,865 ATM cards was sold on the dark web. By 2021, the number of vacant cyber security jobs would have more than tripled due to cybercrime (Ramdinmawii, 2014).Extremist activities in Pakistan, are primarily accessed through social media in order to undermine and disrupt the power, sovereignty, uprightness, and credibility of individuals and institutions, necessitating serious action against cyber extremism (Krasna, 1996). The FIA Cyber Crime Wing claimed to have apprehended 16 people who were stealing information from National Identity Cards of old and illiterate men and women via online, mobile phone money transactions, and NADRA, as well as recuperating and recovering thousands of SIM cards. Officials reported that people were denied of millions of rupees by offering online banking, ATM Cards, Benazir Income Support Program (BISP) and many other different schemes, plans and prizes (Rehman, 2021). According to a February (2016) media report, a man named Fahad Bari is accused of harassing women on Facebook and was apprehended by the FIA. The raiding party discovers a startling material on his computer and confiscates it as evidence.

Research Questions

The main focus of this research is on what constitutes cybercrime and how it affects the general public. It will focus on the underlying attacks that lead to the formation of cyber-crime strategies. The strategy will begin with a historical overview of cybercrime, followed by a discussion of its classification and the types of procedural flaws that exist in cybercrime laws. The study tries to identify the most common factors responsible for cybercrimes in Pakistan along with laws and procedures dealing with such crimes.

RESEARCH METHODOLOGY

The research methodology adopted for this research is a synthesis of qualitative and analytical methods. Primary and secondary data is collected for the critical analysis of Pakistan's cybercrime legislation. The principles of cybercrime are explored, and several forms of cybercrime are examined. It can be applied to get in-depth perspectives into an issue or to develop new research topics. According to this study, there are several negative consequences for society as a result of cybercrime, and this is why computers and networking are used as instruments for criminals. The study will analyze various measures that may be implemented to counter these cybercrimes so that individuals can continue to enjoy utilizing technology rather than being prevented from using it. It also examines the laws that are made explicitly for cybercrime and how the laws protect the people and grab the cyber hoodlums, as well as what kinds of obstacles people encounter once they are harassed with in cyber world, and it concludes by providing or recommending safety measures that a consumer can take.

FACTORS RESPONSIBLE FOR THE CYBERCRIMES

As technology become more innovative, it provided new chances for criminals, hackers, and exploiters to use advanced technology for dangerous purposes. Many people are not fully aware of technology, such as how to review websites, use social media, or disclose personal information on public boards. Lack of cognizance allows cyber criminals to penetrate and cause harm in a variety of ways, which may give rise to the commission of Cyber Crime, which is on the emergence due to the following factors: The cost of data breaches continues to rise, having increased by 29% to a normal of $4 million per incident (Singer, 2014). The costs incurred by cyber events can generally be divided into two categories: first-party and third-party losses (Romanosky, 2016). Cybercrime is on the rise, its consequences are taking longer to resolve, and more corporations, entities, and firms are losing money as a result. Current cyber attackers are emerging, from the organizations they choose to misguide to the strategies they utilize and the types of harm they inflict. A year ago, there were an average of 145 security breaches, which gain access to the organization's core network or enterprise linkage. This is 11% more than the number of reported violations in 2017 and nearly 67 percent more than five years ago. Among the various reasons for the rise in the cost of cybercrime are;as

- Cybercriminals are becoming more adept at new Cyber Attack techniques.
- A huge number of new internet users come from countries with weak network security.
- Cybercrime-a-service and other business plans are making it much easier to gather information online.
- Cyber criminals are becoming more financially advanced, enabling the user for them to adapt their operational activities (Wilczek, 2019).

Breach Caused by Mobile Devices

In 2015, mobile phones had an infection rate of less than 1%, so these devices were regarded as safe. Currently, more than three-fifths of IT security experts report that mobile phone devices have either surely or definitely caused a breach in their companies. Which threats to mobile cyber security are emerging as mobile technology continues to advance? Nearly 45 percent of mobile phone owners own smart phones, which have more storage capacity than previous models. Each new mobile device, tablet, laptop, or computer provided an additional opportunity for a cyber-attacker to gain access to someone's personal information. Connecting accusing ports of others can cause malware issues for multiple devices, as many cell phones can be linked to computers to be charged. People are becoming more technically adept as the mobile phone market expands, and they should be educated as technology advances. Proper training should be used to ensure that the company's employees or workers understands cyber security threats and how to avoid them (Fischer, 2014).

Several mobile phone owners believe that by installing antivirus apps on their phones and being extra cautious about the websites they visit, they can protect themselves from malware and other threats. People are using their mobile phones to communicate with families and friends, to negotiate business strategies, and to store all manner of confidential information. As a result, it is not astounding that cyber criminals want to split in and respond in, and this has also become the chief factor for committing Cyber Crime through mobile phone breach.

Embedding Malware into Legitimate Applications

In their quest to steal information, Cybercriminals have incorporated malware into legal programs and are concentrating their efforts on insecure Wi-Fi hotspots, stealing passwords, and more (Leuprecht, 2019). Malware is a tool used to carry out nefarious purposes on the online platform, either by exploiting existing security flaws or by creating new ones (Jang-Jaccard, 2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, Viruses as well as other malware files serve their masters well, while deceitful hoodlums use malware to infect vulnerable frameworks and recruit person's devices towards their own purposes (Wisniewski, 2012). Malware can be inserted on computers by hackers for a variety of reasons, including gaining physical access to the device. Cyber criminals create malicious programs that is installed on some other user's computer without their awareness in order to obtain confidential information or harm the device; they typically commit crimes for financial benefit. Cyber hackers can easily commit Cyber Crime by generating different types of malware such as viruses, spyware, ransomware, and Trojan horses.

Unauthorized Product Exploitation

Hackers prefer to take advantage of unauthorized products through weak security systems in the corporate web (Umlauf, 2018). Illegal access or faulty data can be easily exploited by hackers, potentially leading to the commission of a cybercrime. Data is reported as a commodity by both legitimate and illegitimate actors, both online and offline. As a result, data is the prime purpose of cybercriminals. Unlawful data is also essential in the commission of multiple Cyber Crimes, owing to the fact that it is not fully secured and can be illegitimately accessed and acquired. Information breaches have occurred as a result of lost or stolen flash drives and other devices (computers, laptops, and cell phones), a weak framework and information security, unauthorized access to data, or distribution have all resulted in data breaches (Atta Ul Haq, 2021). As a result, the misuse of unauthorized products or insecure data, information etc. may result in an increase in the ratio of Cyber Crime.

Servers of Zombie

Zombie processors that are deemed unsafe or are not updated provide additional ways to gain access to networks, which is also contributing to an increase in cyber - crime. In computing system, a zombie is a computer connected to a network that has been compromised by a cyber-attack. It is frequently used vaguely for malicious purposes. Zombies are frequently used in denial-of-service (DDoS) attacks, which refer to the penetration of websites caused by a large number of systems accessing them at the same time. Because multiple users are sending requests to the server that hosts the web browser at the same time, the processor crashes, restricting access to the authentic user. Spam is also sent using zombie servers. In 2005, it was estimated that zombie computers sent between 50 and 80 percent of all malware in circulation. This technique is beneficial to cyber criminals because it empowers them to keep a keep away from detection. Mariposa, a criminal platform with control over approximately 13 million

computers, was brought down in Spain in 2010 by the Telematics Crime Brigade of the Spanish Civil Guard, and the perpetrators were apprehended. They previously had data from 800,000 people from 180 countries (Schneider, 2012).

Vulnerabilities are not fixed in Time

According to one study, it takes an average of 193 days for a patch to be implemented to fix an issue, even when the patch is available. It's a simple place for hackers to break in and cause havoc. With the growing reliance on online services and infrastructure and systems, proper patch management and methods are more important than ever. While trying to patch a system can take a few hours, previous attacks have shown that failing to patch a system with the most current security updates can be more expensive (Allodi, 2013). Hackers are fascinated by security flaws, also known as security errors. A software vulnerability is a flaw in the operating system's security. Hackers can exploit security flaws by writing code that targets the vulnerability. The code is distributed as part of malicious software. A hacker can infect your computer with no action on your aspect other than accessing a bogus website, playing contaminated media, or opening any breached message. What happened after that? Malware can steal information stored on your device or allow a hacker to acquire control of your computer, tablet, mobile phone, and other devices, scrambling your information and documents (Gkantsidis, 2006). Personal data, information, and documents of this nature become valuable to malicious hackers, who exploit them in a variety of ways, and are a significant reason for the rise in cybercrime.

Clicking Passcode

Clicking responses by users without verifying it are also contributing to an increase in cybercrime. Many web pages you open and the server requests a password or says click the below icon, if you press or show a response without checking it, your information, web, or device may crash.

Sharing Personal Information

Although most men and women had sent their private information to others, or as most adult humans in relationships start sharing their nude pictures, which is both humiliating and a source of cybercrime.

Social Media Apps

As technology advances, everything becomes an online system, and all manual systems become online systems, giving hackers and cyber criminals an edge in carrying out their malicious intentions. If you want to transfer funds, pay bills, go shopping, get food etc, it has a specific app that the generation utilizes.

Filing a Complaint with the FIA

The procedure for filing a complaint with the FIA cybercrime cell is as follows:

- You might even go physically to the FIA cybercrime cell.
- You may contact FIA via email.
- You can also call the helpline number 9911
- However, the complainant must visit the FIA at least once for confirmation.

The online application system is extremely slow. The majority of people come to FIA when they are hopeless. It will take 30 to 60 days to begin the proper procedure for any complaint. A person may identify within the same day, or it may recognize within a month. The FIA also requires complainants to fill out an online complaint registration form (Usman, 2017).

Why don't People Complain in the FIA?

There are numerous reasons why people do not complain in FIA:

- Many people did not file complaints with the FIA because they were unaware of the situation.
- 70% of women are afraid of posting their images online because they can be misused.

Some people refuse to leave because they believe that if they do, more exploitation will occur. When photos and data become public and spread between friends, relatives, the colony, and so on, more abuse occurs. They become quiet for their own sake. 95% of people did not file a complaint with FIA;

- some because of more abuse,
- some because they were afraid of the response, and
- some because their family would not allow them

MAJOR ONLINE ACTIVITIES

People with internet connection in Pakistan account for 10 to 16 percent of the total population involved in these significant online activities (Bashir & Shahzad, 2021).

Online Social Networking

Nowadays, social networking is quite popular among individuals. You may communicate with a variety of persons and social friends at the same time. If you'd like to go anywhere with a friend, send him a text, develop a plan, and set a meeting time. Things require a short effort to communicate messages, thoughts, and information with each other using social networking through social media, but might also lead to individuals engaging in cybercrime. You have no clue whether he is the original person who is behind the ID and maybe there is a fraudulent person who creates an ID using your friend's name and converses with you, stealing any personal details from you or if he steals any personal information from you, he may use it against you later. As a result, excessive social networking has negative consequences. It is crucial to keep one's data safe and secure, or to make one's account or ID secret (Van Zyl, 2009).

Internet Banking

It's a mechanism in the banking sector that allows customers to conduct monetary operations using a computerized system, an electronic system, or the internet (Williamson, 2006).

Internet Surfing

The term "internet surfing" refers to the process of using the internet or connecting via it. This is where we look for the items, materials, or information that we require. We utilised Google Chrome, YouTube, or other social networking applications to go from one page to the next and access several websites for our personal usage (Lavin, 1999).. However, it also has a number of negative consequences. For example, if we provide our private details, contact information, email address, or any further information required by the online platform, anyone can use it against ourselves. It also includes cybercrime, and individuals are going to blackmail us.

Online Shopping

Online shopping has also been popular in recent years. Many individuals find it difficult to go from their homes to the mall. As a result, it is more easy for people to purchase online or have their desired item delivered to their home. It enables clients to make online purchases of services or products (Lavnikovich & Parkhanovich, 2015). Cybercriminals, on the other hand, attack various internet websites to get data from customers and subsequently steal their ATM or credit card pin.

Online Education

People have gained through online education since it saves them time in getting dressed and going to any institution, and they can simply study their chosen education at home (Larreamendy, 2006). The online education system has been greatly expanded during COVID-19. They receive their education via Zoom, webcast, Skype, or another kind of online learning. You can also acquire an education from any foreign university. Because several foreign nations allow students to get online education from the comfort of their own homes, many students are taking advantage of this opportunity.

Online Auction

It's a public occasion when products or property are auctioned off to the highest bidder. It's essentially a method for selling something at the greatest possible price. An online auction is one that takes place via the internet. The internet allows a large number of people to participate in many auctions with a single tap (Yen, 2008). If you wish to engage in online auction on many of these websites, you must first register, after which you may bid and purchase or sell items to the highest bidder. Cyber hackers, on the other hand, hack websites and acquire data or information from buyers and sellers.

Audio and Video Communication

Communication is the transmission of facts and information between two or more persons. Data also includes photographs, messages, videos, and audios; in essence, communication refers to the process that occurs between the sender and the recipient. Visual communication refers to everything that can be seen, anything that is conspicuous, and any picture. Any communication that takes place through your sound, such as audio messaging, is referred to as audio communication, and exchanging any type of data via telephony is also included. In video communication, you can see the other individual's face and then convey any data, knowledge, or other items to them. However, online activities such as audio or video communication have a number of drawbacks, such as expensive equipment, complex technology may be uncomfortable for people at times (Hinde, 1972).

Entertainment

The term "entertainment" refers to an activity or a sort of action that attracts the attention of a group of individuals or provides delight and pleasure. Public attention may be captured in a variety of ways, depending on their interests. It also includes a variety of online activities such as playing computer games, watching movies, or using multiple social media apps, reading books, or searching for websites based on one's preferences.

Map Direction/GPS

People utilize map sharing as an online activity to communicate their locations with others. If you want to travel somewhere but don't know where it is, you may easily use your mobile's location services to add the location where you want to go. If you wish to invite somebody to your location, you may easily use location settings on your phone, tablet, or computer and communicate your current position. GPS and MAP directions Navigation is a simple and fast map route with a variety of features. By employing GPS navigation and travels, you can now simply obtain traffic alerts and monitor routes with the use of a GPS tracker (Li & Zhijian, 2010).

Information Sharing

The interchange or information sharing across organizations, persons, and technology is referred to as information sharing. In some cases, information can be delivered in the form of:

- By sharing data with various people by sharing any image or video on Facebook or any other platform.
- By providing information with organizations by sharing any photo or video on Facebook or some other platform.
- By allowing applications to share data via IP addresses on a publicly available network.

It's an online activity in which anybody may communicate any sort of information, data, programs, documents, or viewpoints with others (Savolainen, 2017).

Medical Assistance

Medical attendants are often employed by doctors' offices or other medical care providers. They collaborate closely with high-level medical professionals to ensure that everything is in order, to keep track of the patient's medical history, and to prepare blood for the labs. People may now obtain medical help through various internet platforms as technology advances. According to research, the market for mobile health webpages was valued at $8 billion in 2018 and is expected to grow to $111.1 billion by 2025. Every other day, new applications arise that claim to improve your physical and mental well-being (Lupton, 2014).

Online Games

An online game is a type of computer games which can be played through the internet or another network. These online games drew participants of all ages, countries, and vocations using a number of techniques. Several studies have found that playing too many online games creates physical damage as well as increased worry and depression in gamers. According to studies, many teenagers who are hooked to online gaming have elevated heart rates and blood pressure as a result of the thrill and tension they experience (Taylor, 2009).

IBFT Fraud

Inter Bank Fraud Transfer (IBFT) is a type of fraud that occurs between banks. It's a type of fraud or burglaries that involves using internet applications to illegally remove money from a bank account or shift that money to another bank for malevolent or financial reasons. . Internet banking via online applications is becoming more popular since it is utilized for account information, bill payment, money sending and receiving, and passwords for safeguarding any transaction conducted by the user. You can certainly fall into the trap of a Cyber Criminal due to a simple misunderstanding or a small bit of ignorance. A small error or omission may cause problems on your hard-earned investing assets.

"Lottery Fraud" is also on the increase as a result of online activities. It's a scam in which you're told you've won the jackpot by email, Facebook, Messenger, or texts. Most people respond by sharing their ID card number, private information, and debit or credit card details with the people on the other side. There's also a well-known web scam in which a female claims to be a Nigerian princess who wants to get married you and is sending you $1 million in cash gold in exchange for customs taxes.

Mobile Devices (3G or 4G) Contribution

As modern technology such as 3G or 4G mobile devices grow more common among people, their inappropriate usage has become a contributing reason for the rise in cybercrime. That is to say, the harmful use of mobile devices is also a major factor. As a result, young people's knowledge is critical in this respect. The issue now is, what part will parents play in this? We should not deny our generation of technology; if we do, we will gradually lose touch with the rest of the world. Mobile technologies such as 3G and 4G have ushered in a major shift in the IT industry.

Cyber Laws in Pakistan

Cyber laws that have been enacted in Pakistan do not just address online or computer crime. These regulations cover all aspects of computers and networks. The Government of Pakistan established the "National Response Center for Cyber Crime," which is overseen by the Federal Investigation Agency and performs functions such as locating cyber criminals, investigating cyber-crimes, and attempting to reduce negative internet usage. NR3C possesses complete mastery of digital forensics, system security audits, technical research, examinations, and training. Since its establishment, the unit has been involved in the capacity work of officials from the police, security, court, prosecutors, and other government associations (Rehman, 2020).

The first IT-related legislation enacted by national legislators was titled "The Electronic Transaction Ordinance (ETO), 2002." It creates the foundation for a complete legal system. The Electronic Transaction Ordinance, 2002 is beneficial for accommodating the acknowledgment and assistance of files, documents, data, communications, and relations in an electronic structure, authorization of confirming expert organizations, and difficulties related to and auxiliary to these (Zafar, 2017).

On August 11, 2016, Pakistan's National Assembly approved the "Prevention of Electronic Crimes Act, 2016," which prohibits cybercrime. The act is also amended by the Senate. In August of 2016, the president provided his approval for this law. The act's goal is to prevent unauthorized or unlawful activities with regard to the information technology. The national legislature passed the Prevention of Electronic Crimes Act (PECA) to provide a thorough legal framework for identifying various types of electronic breaches, as well as procedures for investigating, prosecuting, and resolving electronic crimes.

It is the first case under the country's new Cyber Crime Law under which a special court of Pakistan sentenced a man to five years of rigorous jail for uploading derogatory information or material on social media.

In 2017, Sajid Ali, a prominent Shia Sect member, was convicted by the Special Court for Cyber Crime for spreading "discourteous, blasphemous, and derogatory" content on Facebook. Ali, a resident of Bahawalnagar,

was sentenced under Section 11 of the Prevention of Electronic Crimes Act 2016 and Section 298-A (related to derogatory statements against the Holy Prophet and their Companions) of the Pakistan Penal Code, which deals with the use of derogatory statements against Islamic holy personalities. The case was shifted to the FIA Cyber Crime unit in Lahore due to a jurisdiction issue. The FIA prosecutor called 12 witnesses, including the FIA Assistant Director, who presented his analytical report, in which the majority of the witness statements appeared against Ali. It is the first conviction in the nation under the new Cyber Crime Law, which was approved on accusations of publishing blasphemous information on social media against the Holy Prophet's companions. Following this judgement, the court further instructed the government to educate the public regarding cybercrime, particularly blasphemous content. Pakistan has a history of harsh penalties for anyone guilty of blasphemy.

Supreme Court of Pakistan on the Cyber Crimes

The very first cybercrime case in the Supreme Court was reported by the US Consulate in Karachi on May 14, 2003, thus the Superior Court issued a notice to the Deputy Attorney Journal. Former federal minister Syed Iqbal Haider appeared in court on behalf of Iftikhar and Khurram, who are both reportedly tangled in this case. The bench during the hearing included Chief Justice Sheikh Riaz Ahmad, Justice Muhammad Nawaz Abbasi, and Justice Mian Muhammad Ajmal. According to Iqbal Haider, the US embassy in Karachi complained to the federal investigative agency that some Pakistanis are involved in importing products from America and other nations by abusing credit cards. He further claimed that the consulate traced about 5 people involved in this case, as well as their mobile phone numbers, and reported this information to the FIA in order to initiate legal action against these people under Sections 420, 411, 468, 471, and 477(a). According to the consulate, these individuals are also involved in World Wide Cyber Crime, whose costs around $3 million. The matter was also heard in the Special Court over banking offences, but the bail was dismissed both the trial court and the Sindh High Court. The Supreme Court then heard the bail application, which has been adjourned until a future date. While clarifying the scam, Iqbal stated that it has been claimed that these Pakistanis obtained stolen credit card payment slips in order to purchase additional products over the internet and subsequently used them for other objectives (Khan, 2020).

SUGGESTIONS AND RECOMMENDATIONS

We will prevent cybercrime in the future by raising public awareness. According to research, many people are unaware that they are committing Cyber Crime. The major method of preventing cybercrime is to hold seminars in multiple locations, including as schools, colleges, and universities, and to educate people, particularly adults, about unlawful information on the internet. Cybercrime is a constant threat. You may assume that the only type of Cyber Crime to be concerned about is hackers stealing your financial information, but this may not be the fact. They serve considerably more than simply financial objectives. Cybercrime is on the ascent, with new threats emerging every year. Most children and adults who use mobile, laptops, or social media applications are unaware of the type of website they are visiting. Even during their studies, kids who are given access to fraudulent websites may enter their email, login, or other personal information that cybercriminals may exploit. Parents and instructors should educate their students or children how to use the internet, how to protect themselves, and what sort of information they should share on social media. Proper lessons on cybercrime awareness should be given to learners when explaining its laws or highlighting the methods in which they can protect their information from cyber hackers. Seminars and workshops should be held at the college and universities.

People used to believe that their devices didn't require any kind of security mechanism, however nowadays it only takes 4 to 5 minutes to hack into someone's phone or computer. It is critical to use strong or complex credentials everywhere in order to protect our personal information from cyber criminals. If you post personal information on the internet, you should set your account to private, and you should not add somebody to your list of friends if you do not know them personally. Most people believe that if their phone or laptop is seized, there is no need for them to be concerned because the device contains a complex password, and the finder would not be able to access it without the password. However, it is alarming for them because the entire data can be recovered or approached in the hands of hackers or malicious hackers. People should use complex passwords wherever or whenever they access any social media platform, device, or disc, for example. Don't just enter a password when opening any device; nowadays, individuals should protect their confidential information as much as possible. Many fraudulent or false editing applications created by programmers may modify images in a variety of ways. So, while

technology advances and makes users' lives easier, it also creates issues for people that don't understand how to use it properly.

CONCLUSION

Cybercrime is a type of crime that targets any electronic media. For a long time, cybercrime has been on the increase. As people progressively do business and live their lives on the internet, a growing number of cyber criminals use the internet to obtain information or data. Cybercrime is on the rise, and cybercriminals are prospering by targeting people, selling hacked data, improving schemes, and so on. For cyber criminals, the phrase "crime doesn't pay" has become a mockery. Cybercrime is becoming more terrible than at any other moment in history, and the reasons are obvious: it is extremely profitable and indisputably less hazardous. We won't be able to stop them unless we figure out how to raise the threat and decrease the perception of cybercrime. In this day and age, if you have access to Wi-Fi or any other online connection, and you own a recent smartphone, smart TV, or some other type of smart device with a probable internet association - you are weak. When cybercrime crosses geographical boundaries, the entire world becomes a major court. Because of the global nature of the internet, it is unclear which court would have exclusive jurisdiction to try the lawsuit. The litigation procedure and legal systems in many countries varies and may be extremely costly, threatening to drive many lawful organizations into obscurity. There is substantial dispute about the validity of judgements made by courts of one jurisdiction on a global scale, and punishments are questionable. We can prevent ourselves from cybercrime by taking preventive measures and protecting our personal data from cyber criminals by utilizing a full service network security, using strong passwords, keeping your software up to date, teaching your children about the internet, and knowing what to do if you become a sufferer. In any situation, if cyber criminals steal your identities by hacking your private information, you should call the banks where the theft occurred, set up fraud alerts, obtain your credit reports, and report this fraudulent activity to the FTC.

FUTURE RESEARCH DIRECTIONS

The cybercrime legislations need to be upgraded in line with modern development in the field of ICT, especially in Pakistan and KSA. The UAE model of anti-cybercrime may be considered as role model, and electronic crime laws may be revised, especially in Pakistan.

Awareness may be made to Pakistani citizens about the preventive measures from electronic crime. Special care should be made while using social networking website, personal information such as passwords, codes, locker numbers, and photographs would not be disclosed to strangers. The underused computer systems must be protected with updated antivirus. Care shall be made in checking E-mails, only known E-mail shall be checked and others may be ignored. Try to avoid using credit card online and security firewalls must be installed in offices to avoid unauthorized access

In Pakistan, cyberlaws shall be made according to international best practices and norms. The use of computer system is increasing day by day in our routine life, and social networking sites make it more attractive for whole community use. There is a need to introduce a subject about the cyberlaws and cybercrime with every master or bachelor degree to create awareness among the community. In Pakistan, universities did not have any separate department about the cyber security and cyberlaws, and none is offering any program in this field. There is a need to revise the curricula at the university level according to the modern needs. A guide book about the cyberlaws and cybercrimes with explanations should be made available to the public for the purpose of awareness. Training programs must be started for executives and judges about cybercrimes. There is a need to conduct an empirical study to find the actual impact of cybercrimes on the economy, citizens, banks, government institutions and their functionalities, and to the IT professionals.

REFERENCES

Allodi, L., Shim, W., & Massacci, F. (2013). Quantitative assessment of risk reduction with cybercrime black market monitoring. In *2013 IEEE Security and Privacy Workshops*. https://doi.org/10.1109/SPW.2013.16

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy*. Springer, Berlin, Heidelberg.

https://doi.org/10.1007/978-3-642-39498-0_12

Atta Ul Haq, Q. (2021). Cyber crime and their restriction through laws and techniques for protecting security issues and privacy threats. In *Security Issues and Privacy Threats in Smart Ubiquitous Computing*. Springer, Singapore. https://doi.org/10.1007/978-981-33-4996-4_3

Bashir, S., & Shahzad, F. (2021). Federal investigation agency against the crime of book piracy in Pakistan. *Library Philosophy and Practice* (e-journal). 5034.

Britz, M. (2009). *Computer forensics and cyber crime: An introduction,* (2nd ed). London, UK: Pearson Education India.

Fischer, E. A. (2014). *Cybersecurity issues and challenges: In brief*. Retreived from https://www.everycrsreport.com/files/20141216_R43831_acbefaafacb64f97fd77df976c469127afdd9308.pdf

Gkantsidis, C., Karagiannis, T., & VojnoviC, M. (2006, August). Planet scale software updates. In *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. Pisa, Italy. https://doi.org/10.1145/1151659.1159961

Hinde, R. A., & Hinde, R. A. (Eds.). (1972). *Non-verbal communication*. Cambridge, UK: Cambridge University Press.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. England, UK: Routledge. https://doi.org/10.4324/9781315296975

Khan, A., Khwaja, A., & Jawed, A. (2020). Navigating Civic Spaces During a Pandemic: Pakistan Report. Retreived from https://bit.ly/3tBZjSp

Larreamendy-Joerns, J., & Leinhardt, G. (2006). Going the distance with online education. *Review of Educational Research, 76*(4), 567-605. https://doi.org/10.3102/00346543076004567

Lavin, M., Marvin, K., Mclarney, A., Nola, V., & Scott, L. (1999). Sensation seeking and collegiate vulnerability to Internet dependence. *CyberPsychology & Behavior, 2*(5), 425-430. https://doi.org/10.1089/cpb.1999.2.425

Lavnikovich, A., & Parkhanovich, Y. (2015). The Alibaba phenomenon.Retreived from https://bit.ly/3D8J2Yk

Leuprecht, C. (2019). Mitigating cyber risk across the financial sector. *Governing Cyberspace during a Crisis in Trust, 64*.

Lupton, D. (2014). Apps as artefacts: Towards a critical perspective on mobile health and medical apps. *Societies, 4*(4), 606-622. https://doi.org/10.3390/soc4040606

Li, H., & Zhijian, L. (2010, December). The study and implementation of mobile GPS navigation system based on Google Maps. In *2010 International Conference on Computer and Information Application* (pp. 87-90). IEEE. https://doi.org/10.1109/ICCIA.2010.6141544

McQuade, S. C. (2006). *Understanding and managing cybercrime. Boston*. London, UK: Pearson/Allyn and Bacon.

Mohiuddin, Z. (2006). *Cyber Laws in Pakistan: A Situational analysis and Way Forward.* Retrieved from https://nanopdf.com/download/cyber-laws-in-pakistan-supreme-court-of-pakistan_pdf.

Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A study on the cyber-crime and cyber criminals: A global problem. *International Journal of Web Technology, 3*, 172-179.

Rehman, T. U. (2020). International cooperation and legal response to cybercrime in Pakistan. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 424-434). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch029

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Savolainen, R. (2017). Information sharing and knowledge sharing as communicative activities. *Information Research: An International Electronic Journal, 22*(3).

Sinrod, E. J., & Reilly, W. P. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. *Santa Clara Computer & High Tech. LJ, 16*, 177.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford, UK: Oxford university press.

Skertic, J. (2021). *Cybersecurity Legislation and Ransomware Attacks in the United States, 2015–2019* (Doctoral dissertation). Old Dominion University, Norfolk, Virginia.

Taylor, T. L. (2009). *Play between worlds: Exploring online game culture*. Cambridge, MA: Mit Press.

Usman, M. (2017). Cyber crime: Pakistani perspective. *Islamabad Law Review, 1*(03), 18-40.

Umlauf, M. G., & Mochizuki, Y. (2018). Predatory publishing and cybercrime targeting academics. *International Journal of Nursing Practice, 24*, e12656. https://doi.org/10.1111/ijn.12656

Van Zyl, A. S. (2009). The impact of Social Networking 2.0 on organisations. *The Electronic Library 27*(6), 906-918.

Wells, R. M. (2021). *Identifying trends associated with cyber-crime in healthcare industries* (Doctoral dissertation). Northcentral University, San Diego, California.

Williamson, G. D., & Money–America's, G. E. (2006). *Enhanced authentication in online banking (Doctoral dissertation)*. Utica College, New York, NY.

Wilczek, M. (2019). *Cybercrime is increasing and more costly for organizations.* Retrieved from https://zd.net/36xGgQu

Wisniewski, C. (2012). *Exposing the Money Behind the Malware*. Technical report, Shopos.

Yen, C. H., & Lu, H. P. (2008). Factors influencing online auction repurchase intention. *Internet Research, 18*(1), 7-25. https://doi.org/10.1108/10662240810849568

Zafar, A. (2017). *Analyzing hybrid optimization for energy management in smart grid (Doctoral dissertation)*. COMSATS University, Islamabad, Pakistan.