Cybercrime, Internet and Cybercrime Legislation: A study of Pakistan

[1]Abdul Ghaffar Korai., [2]Abdul Samad. , [3]Ahad Ghaffar, [4]Javed Ahmed, [5]Imtiaz Ahmed Memon.

[1] Assistant Professor Law at Shaheed Zulfiqar Ali Bhutto University of Law Karachi.
[2]Hungarian University of Agriculture and Life Sciences.
[3]Legal Intern at Law Office, Karachi.
[4]Advocate High Court of Sindh.
[5]Deputy Director (Monitoring) Criminal Prosecution Service, Law Department Government of Sindh.

Abstract

The aim of this research is to study cybercrime, internet and cybercrime legislation in context of Pakistan. Pakistan is one of the most dangerous countries in the world when it comes to cybercrime. Cybercrime is a broad word that encompasses computer-assisted criminality. Pakistan has a slew of regulations in place to combat cybercrime, including cyber terrorism and unauthorized access to secure data. We studied the related literature, different laws to prevent it and also the actions we can take to control cybercrime in Pakistan. This article discusses the global perspective and categories of cybercrime as well and also a little analysis of cybercrime impact on economies of different countries.

Keywords: Cybercrime, law, Pakistan, Internet, Legislation

Introduction

The Internet, computers, mobile phones, and other kinds of technology have fundamentally transformed all aspects of human existence in the last several decades, including how we interact, bank, shop, obtain news, and enjoy ourselves (Holt and Bossler 2016). These technological improvements have also provided a plethora of options for crooks to engage in a variety of illicit activities. Because "the criminal uses specific understanding of cyberspace," cybercrime is commonly referred to as cybercrime (Furnell 2002). As a result, cybercrime can be viewed as a broad word that encompasses computer-assisted crime, which involves the use of computers and technology to support tasks such as sending abusive messages. At the same time, computer-centric crimes that are a direct outcome of computer technology and would not exist without it, such as unlawful computer system intrusion, are included in the term cybercrime (Furnell 2002; McGuire and Dowling 2013). Cyberinteraction (e.g., unauthorized system access), online deception/theft (e.g., identity theft, online fraud, digital hacking), online pornography/obscene (e.g., child sexual exploitation material), and cyberbullying (e.g., cyberbullying; cyberterrorism) are all examples of cybercrime (Holt, Bossler, and Seigfried-Spellar 2018; Wall 2001). It is very hard to quantify the number of cybercrimes that occur in most countries throughout the world due to a lack of defined legal definitions and few genuine and trustworthy official statistics (Holt and Bossler 2016). However, while traditional street crime in many forms continues to diminish, data suggests that cybercrime is on the rise (Tcherni et al., 2016).

According to Parker (1998), one of the key worries of the international community is cybercrime, which has developed as a result of the introduction, growth, and usage of information and communication technology. Cybercrime is a well-known form of international crime that has been influenced by the worldwide information and communication technology revolution (Barr & Pease, 1990). Cybercrime differs from traditional crime in four ways: it is simple to learn and implement, it requires low resources in comparison to the potential harm it causes, it can be perpetrated in jurisdictions where it does not exist, and it is usually not evident that it is criminal (Levi, 1998). New types of cybercrime have presented new issues to legislators, law enforcement agencies, and international organizations as a result of this (Madhava & Umarhathab, 2011). This necessitates the establishment of both national and international procedures to monitor the use of ICT in cybercrime. Pakistan has not only worked hard to achieve digitalization in the public sector, but has also taken steps to foster digital prosperity in the commercial sector. IT policies have been introduced in addition to broadband rules in order to foster a digital culture in society. Internet connections and speeds have just doubled.

The government recently opened bidding for 3G and 4G technology, which is expected to revolutionize the telecoms industry. Furthermore, massive sums of money are being allocated to public sector entities for the purpose of computerization and networking. In the country, e-government, e-banking, and e-learning have all exploded. However, no suitable regulation exists to prohibit electronic/cybercrimes or to protect users from electronic fraud, among other things. This is the most

significant impediment to user trust and confidence. In addition to the Pakistan Electronic Crimes Law (2007) and the current Pakistan Electronic Crimes Law (2014), the updated Pakistan Electronic Crimes Regulations (2002) (2008) were promulgated in conformity with the 1973 Constitution and expired six weeks later. In the absence of cyber legislation, cybercriminals like to play with online communities, making it easier for them to become victims, losing not only their privacy, data, and money, but also, in some cases, their lives. It will have a negative impact on their social and familial lives in these conditions (Magalla, 2013).

Literature Review

The lack of a proper definition of the term cybercrime is the primary issue in cybercrime research. Although some jurists have attempted to define the phrase, there is still no agreement on what it means. "Cybercrime is a generic phrase that refers to all criminal actions undertaken through computers, the Internet, cyberspace, and global networks," says one definition. In other terms, it is a crime in which a computer is utilized as a criminal tool or as a criminal target. Because mobile phones are sometimes used to commit crimes, yet the description provided does not include mobile phones, this definition does not encompass many aspects of cybercrime. Dr. Debarati Halder and Dr. K. Jaishankar came up with a reasonable concept that encompasses other current technologies. It is described as a criminal act that destroys the victim's reputation or causes bodily and mental harm to the victim through the use of modern telecommunication networks (chat rooms, emails, alerts, etc.) such as the Internet for individuals or groups with criminal motivations. And groups) as well as mobile phones (SMS/MMS). The word "cybercrime" is also used as a label to describe crime and is a synonym for technological crime, high-tech crime, Internet crime, economic crime, electronic crime, digital crime, and so on. Equipment for computers or information technology. Instead of attempting to comprehend cybercrime as a singular phenomenon, it is preferable to "consider the word as a collection of criminal behaviors, the ‘common ground' of which is the major role played by the Information and Communication Technology Network (TIC) in its committee."

Mobile and cloud computing, e-commerce, and social apps are all transforming the global corporate landscape. Organizations are devising methods to leverage this cutting-edge technology to communicate information and execute online business transactions. Commercial transactions done online accounted for almost 80% of overall transaction volume. To limit the risk of transaction failure and consumer discontent, high-level security standards have been imposed. Cyber security encompasses more than just an organization's local information technology infrastructure; it also includes border networks and information technology infrastructure. The importance of network security in the development and present implementation of essential computing and communication infrastructure cannot be overstated. Improving network security and defending critical digital infrastructure requires a combination of national security and economic development. Strengthening government policies and services also requires making the Internet more secure and protecting Internet users from cyber assaults. Cybercrime prevention must be a part of a national strategy to safeguard information and communication infrastructure as well as cybersecurity. As a result, a holistic approach is required to develop and implement a national cyber security plan. Cybersecurity methods, such as building technical protection measures or teaching people on how to defend themselves from cybercrime, can, for example, aid in the reduction of cybercrime. The basic actors in the fight against cybercrime are these national or individual strategies. To combat cybercrime, a holistic approach is required; technology solutions alone will not suffice to prevent any crime. Cybercrime must be investigated and prosecuted effectively and efficiently by law enforcement agencies.

In the age of terrorism, cyberspace is where organized crime and criminal groups collide; these groups include the Russian Mafia's Internet security, the Internet Tamil Black Tigers, and the Mafia. Cyberterrorism is classified as a type of cybercrime. The first such terrorist strike was on a computer system in Sri Lanka, according to the intelligence service. In less than two weeks, the national insurgents overwhelmed the Sri Lanka Embassy's email system with more than 800 emails in a single day. The following is the wording from the email: "We are the Internet's dark tigers. This is done to obstruct your communications." Because the rebel organization is known for killing individuals, this is a subject of tremendous concern for diplomats. Cybercrime is divided into nine categories under the international community's cybercrime law. Privacy protection, intellectual property damage, criminal/procedural law, Internet economic crime, counterfeiting, online fraud, youth pornography, illegal access, and illegal/harmful content are among the categories. Despite the passage of legislation, certain countries, such as China and Saudi Arabia, have deployed technical Internet filtering measures. The Internet Service Unit (ISU) was created in 2010 by the Kingdom of Saudi Arabia. ISU is in charge of screening network traffic and ensuring that consumers can only access legitimate websites (websites not on the "blacklist").

Global Perspective on Cyber-Crimes

In the digital age, online communication has become the norm (R.S, 2007), and Internet users and governments are more vulnerable to cyber-attacks (Rasch, 1996). Cybercriminals are continuing to develop advanced technology by shifting their attention away from financial data theft and toward business espionage and gaining government data. In light of the growing growth of cybercrime, developing-country governments must work together on a global basis to build efficient threat-control frameworks. Developing countries can grow and expand communication networks as information technology and telecommunications advance, allowing them to construct networks and transmit information more rapidly and conveniently. As a result, cybercrime has expanded globally in recent years, drastically altering the situation, and criminals are now employing more sophisticated equipment to compromise network security. Furthermore, recent malware, spam, company website hacking, and other similar attacks are all stunning and obvious "genius" creations. These infrequent harmful operations have morphed into cybercriminal organizations that move funds through unauthorized network channels.

Today, the world's population is expected to be over 2 billion Internet users and 5 billion mobile phone users. Every day, around 294 billion emails and 5 billion phone calls are sent (Commonwealth Secretariat, 2002). The convenience of digital networks, on the other hand, comes at a cost. Business organizations and society as a whole are more reliant on computers and Internet-based networks, resulting in an increase in cybercrime and digital attacks around the world. Financial fraud, hacking, obtaining pornographic photos from the Internet, virus attacks, email tracking, and the establishment of websites that promote racial hatred are all examples of cyber-attacks (Herhalt, 2011). The first and most important step in achieving protection is to gain a deeper understanding of the various sorts of risks that business communities and internet consumers encounter. The most common cybercrimes that can impact electronic security decisions are listed below. Prepaid fraud, botnet interpretation, denial of service (DoS) and distributed denial of service (DDoS), domain name renewal scams, false advertising, hacking, theft of laptops or other hardware, identity theft, intellectual property theft, information duplication, phishing, threat software, social media, spam, spyware, and an insecure wireless local area network (WLAN) are among the most common cybercrimes (KPMG, 2013). The first big cybercrime crisis happened in 2000, when a large-scale transmission of computer viruses infected around 45 million computer users throughout the world. Similarly, cybercrime fueled by politics has infiltrated worldwide Internet (Herhalt, 2011).

Experts fear that some government agencies may be utilizing cyber-attacks as a new kind of warfare instead of armed conflict. Stuxnet (a computer virus) was used to carry out stealth attacks on the programmed, according to reports from 2010. Iran's uranium enrichment centrifuges should have been forbidden by Iran's nuclear power plants. Carders Stealing Bank is a major cybercrime in which duplicate cards are used to take cash from ATMs or retailers (Chapman and Smith, 2001). Because of the worldwide character of cybercrime, it can occur not just in the country or region where it originated, but also in other countries or regions. As a result, cybercrime necessitates not just a high level of reaction, but also internationally coordinated control measures. Likewise, methods for detecting and reporting these crimes must necessitate a significant investment of time and money. Enterprise costs have risen dramatically as a result of the need to secure and repair network infrastructure. For example, the annual cost of cybercrime in the United Kingdom is estimated to be 27 billion pounds, or 43 billion dollars in US dollars, and 7 billion pounds, or 9.2 billion pounds in US dollars (11 million US dollars) Intellectual property (IP) theft for espionage purposes. According to reports from the German IT trade group "Bitkom" and the Federal Bureau of Investigation, phishing accounted for almost 70% of the anticipated cost in Germany in 2010, according to the German Criminal Police Agency's 2010 report. In addition, cybercrime's indirect costs include damage to an organization's reputation and a loss of trust among internet users in online transactions (Herhalt, 2011; European Commission, 2003).

The Internet use in Pakistan

Internet connectivity has been available in Pakistan since the mid-1990s. Since then, Pakistan Telecom Co., Ltd. has begun to provide access services across the country via local telephone networks, and cybercrime has become more prevalent in our culture. Pakistan has one of Asia's largest Internet populations. This proportion is growing every day as the government offers computers and Internet to talented students and lowers the cost of accessories and Internet. In the sphere of information technology, 3G and 4G technologies have also ushered in a revolution. Manual business on the Internet is evolving as the number of Internet users grows, reducing paperwork by replacing manual procedures with computers. Although the ability to save time is a boon to society, the Internet and computers are sometimes used for illicit acts such as fraud and deception.

Pakistan and Cybercrime

Pakistan is one of the countries with the most Internet users, having joined in the 1990s. While the Internet makes life easier and saves time, it also leads to theft, fraud, child pornography, blackmail, and other issues. People in Pakistan abuse the Internet, and some of it is used for illicit and illegal purposes (Mohiuddin, 2006). According to statistics, Pakistan has around 7,500,000 Internet users in 2004. We didn't have enough planning or experience to investigate cybercrime within a few years. Criminals are frequently freed without following proper processes. The Federal Bureau of Investigation is in charge of a national cybercrime response centre set up by the government (FIA). It was created with the primary goal of preventing Internet misuse. Cyber security, cyber fraud, technical investigations, and digital forensics are all areas where the agency has experience. In Pakistan, the first cybercrime case occurred in 2003. Five Pakistanis engaged in import and export-related enterprises by providing fraudulent information and abusing credit cards. According to the FIA research, Facebook is used in 65 percent of cybercrimes, including blackmail and harassment of women, the majority of which occur in Karachi. Every day, the Karachi Internet Department receives roughly 20 cybercrime reports. In 2018, approximately 5,500 cybercrime-related offences were reported in Lahore, including harassment, extortion, stalking, invasion of privacy, deception, fraud, and more. The following is a quick rundown of Pakistani cybercrime reports from prior years: Dawn (Dawn, 2018).

Year	Number of inquiries conducted	Number of Cases Registered	Number of arrests made
2016	514	47	49
2017	1290	207	160
2018	20295	255	209

Emerging Trends and Challenges

The organization's current main focus is on developing measures to secure user identities and sensitive data theft. The world is transitioning to a digital economy, and the majority of information is now available in digital form. Users may believe that ICT social applications that interact with friends and family via a website make them feel safe, but in reality, they make it simpler for hackers to access and steal personal data from users, particularly family users. Although the majority of users seem unconcerned with the privacy of the content and messages they share on social media, this can be problematic. In addition to the numerous advantages of online social media, there are numerous drawbacks. One of the most serious issues with online social media is identity theft. Millions of bogus personal data exist, which are used to manipulate or damage others. The reason for this is that it is very easy and quick to manufacture and generate false personal data using other people's information or photographs, and to steal information using social engineering techniques. Android-based devices will be subjected to increased attacks, although not on a big scale. Tablets running the same operating systems as smartphones, as we all know, will soon be infected with the same virus. Macs are less vulnerable to malware threats than Windows-based systems. The new Windows 8 operating system makes it simple for application developers to create nearly any application for any Windows 8 device. When compared to Android apps, the likelihood of producing dangerous apps increases. Opportunities and problems coexist as a result of the aforementioned technology. The growing usage of online social networks, as well as the privacy and confidentiality of individuals who utilize the aforementioned services, will be a major headache. Many scholars have presented strategies to lessen the hazards to the confidentiality and privacy of groups that previously collected personal information from social media sites (for example, they have more than 800 million views on Facebook, which is one of the most popular online social networks. One). The concept of a Virtual Private Social Network (VPSN) was envisioned as an example of these methods to alleviate privacy threats. VPSN is a symbol for the virtual private network concept seen in online social networks: only friends who are encircled by VPSN may see effective and authentic personal information. Many new applications and devices are in the works, bringing with them new security risks. Everything will be digitized as the company moves toward a paperless economy. They aim to safeguard confidential information as well as the system's physical security. Companies are attempting to replace mobile cloud computing with cutting-edge cloud technology, but many are hesitant to do so due to privacy and availability concerns.

Categories of Cyber Crime

Unauthorized Access:

Entering, teaching, or connecting with a computer, computer system, or computer network's logic, arithmetic, or memory function resources is referred to as access. As a result, any sort of access without the consent of the legal owner or the person in control of the computer, computer system, or computer network is referred to as illegal access.

Hacking & Cracking:

Every act of breaking into a computer and/or network is a hacking act, according to the promise. To attack the target computer, hackers write or use pre-made computer programs. They have a thirst for devastation and take pleasure in it. Some hackers hack for personal financial benefit, such as collecting credit card information, transferring monies from various bank

accounts to your own account, and then withdrawing the proceeds. Hackers can steal or alter data, as well as introduce viruses or worms that harm the system. Controlling someone else's website via hacking into a network server is known as network hijacking.

Cyber Fraud/Online Fraud:

The internet allows people to conduct business efficiently and rapidly. The internet is also an open invitation to scammers, and online fraud is becoming out of control.

Cyber Pornography and Pakistan

"The Internet has given a convenient manner of communication and access to a great amount of information" throughout the last few decades. It is a "useful tool; nevertheless, because of the numerous dangers on the Internet, it may also be destructive to children's well-being." Pornography on the internet should be the largest business on the internet now. This business / industry promotes pornographic sites, online pornographic publications, photos, photographs, books, and writings, as evidenced by the millions of pornographic sites. Despite the fact that pornography is not illegal in many nations, child pornography is nevertheless prohibited in the majority of them. " People's social interactions, learning methodologies, and entertainment choices have all changed as a result of the rapid rise of electronic and computer communications and information exchanges during the last decade. The Internet has given rise to a new form of communication, particularly among young people." E-mails, webpages, instant messaging tools, webcams, chat rooms, and webpages, as well as their social and text messages, are all growing in popularity around the world. There is a "possibility of child maltreatment through internet pornography temptation and cyberspace access to pornography." In fact, the Internet "is swamped with unsuitable materials, such as pornographic content, adult-themed chat rooms, and instant messaging access, where your identity may be misrepresented by others." Because children "are in places where strangers can visit them or where they may be exposed to harmful sexual materials, they require protection and teaching on how to use the Internet safely." To put it another way, "the cost of sexual crimes to minors and society is too high to overlook the dangers of recruiting internet consumers." Pakistan classified and prosecuted child pornography in March 2016. PECA84, which was passed in August 2016, specified a comparable offence and increased the maximum penalties from 700,000 to 5 million rupees, although the imprisonment remains the same as under Pakistani law. As a result, we can clearly deduce that when computers are used to distribute or transmit any type of child pornography, the situation is far more dangerous than when traditional media is employed.

Cyber Stalking

Tracking is not a new phenomenon; the powerful have employed various tactics to track the weakest people since the dawn of time, and this strategy has been used to track the weakest people since then. It is defined as "tracking another individual through the Internet, e-mail, or other electronic communication devices." In other words, we can define a project as "one in which the person being harassed must experience reasonable harassment, panic, or suffering as a result of his personal safety or the safety of the person or persons for whom he is responsible." In other words, it refers to tracking another individual via "the Internet, e-mail, or other electronic communication technologies." The similar idea applies to firms in which the largest and most powerful corporations lurk in weaker areas in order to ruin their enterprises and gain market control. The perpetrators of this offence face a sentence of up to three years in prison or a fine of up to one million rupees, or both. Minors face a maximum sentence of five years in prison and a fine of 10 million rupees, or both.

Cybercrime Legislation in Pakistan

The Prevention of Electronic Crimes Act of 2016, which addresses the majority of the charges specified in the Budapest Convention in some way, is the main source of substantive legal provisions.

The Budapest Convention-related procedural authorities are addressed in the Prevention of Electronic Crimes Act; nonetheless, certain powers lack procedural limitations and safeguards.

Substantive law

Unauthorized access to information or data systems (Article 3), unauthorized copying or transmission of data (Article 4), interference with information systems or computer data (Article5), beautification crime (Article 9), cyber terrorism (Article 10), hate speech (Article 11), recruitment, financing, and planning of terrorism (Article 12) are all crimes covered by the Electronic Crime Prevention Act (section 26). The Electronic Crime Prevention Law also establishes a legal framework for the prosecution of offences involving information technology (Article 27).

In addition, pornographic content is covered by criminal law (Article 292), and copyright violation is covered by copyright regulations (Article 66).

Procedural law

Although the Criminal Procedure Law is the fundamental overarching foundation for all computer

crime investigations, the Electronic Crime Prevention Law also includes particular procedural provisions that apply to all cybercrimes, crimes committed with computer systems, and all criminal offences. Investigation. Investigations that necessitate the use of digital evidence.

Article 31 of the Electronic Crime Prevention Law specifies data retention and speedy disclosure powers, search warrants and seizures powers (Article 32), powers to conduct searches and seizures (Article 35), and conditions and conditions linked to searches and seizures. Precautionary measures. (Section 36), as well as data collecting and recording in real time (Section 39).

Safeguards

There are certain general guidelines and precautions in place. The "Electronic Crime Prevention Law," in particular, limits the breadth and duration of the exercise of power (Article 18), as well as the reasons for exercising power and independent oversight to some extent. However, the "Electronic Crime Prevention Law" permits investigators to get data without a court warrant when there is a danger or loophole that the data will be modified, lost, deleted, or restored. 31). Investigators also have the authority to issue blanket orders requiring anybody having decrypted data, equipment, or information systems to provide access to data, equipment, or information systems (Article 35).

Economic Impact of Cybercrime

Cybercriminals continue to develop new attack and evasion strategies by obtaining data from citizens, businesses, and governments through unethical means. Morgan has compiled a list of the top 20 countries with the greatest incidence of cybercrime (Table 1). (Morgan, 2017). Cybercrime has become an obligatory cost in some virtual economies, according to Huff et al (Huff, Desilets, and Kane, 2010). The more experienced and competent hackers in these illegal economies are enriching the cybercrime ecosystem, including the usage of hidden forms of the Internet known as the "dark web," the usage of popular cyber assault tactics (such as malware), and funding through virtual cryptocurrency. Bitcoin, for example, can be used as a platform for digital money laundering. Some of these hackers run their own businesses, while others operate in a similar manner to genuine corporations. Because of their size, these companies are able to hire highly skilled IT personnel (BryanLow 2012). South Africa and China are the two economies with the greatest rates of cybercrime victims. Many governments have developed and implemented cyber warfare strategies in response to the rising complexity and speed of cyber-attacks (Lewis, 2018). According to Porche 2019, a study of the world's top Internet specialists found that China has the most powerful cyber warfare capabilities. In terms of more effective technologies to tackle cybercrime, Russia and the United States tied for second place, while Israel came in third. Despite the apparent effectiveness in tackling cybercrime, according to Poulsen 2018, 66 percent of adult customers in the United States are more concerned about the risk of cybercrime than any physical crime.

Sr.	Countries	Total Attacks	Sr.	Countries	Total Attacks
01	Canada	**3164**	11	France	**368**
02	India	**2819**	12	China	**366**
03	United Kingdom	**1383**	13	South Africa	**349**
04	Australia	**989**	14	Italy	**291**
05	Mexico	**632**	15	Pakistan	**276**
06	Russian Federation	**594**	16	Netherlands	**266**
07	Brazil	**558**	17	Malaysia	**265**
08	Germany	**466**	18	United Arab Emirates	**259**
09	Philippines	**453**	19	Spain	**248**
10	Japan	**413**	20	Argentina	**238**

Table1. Cyber Attack Rates for the Top 20 Countries (Adopted from Morgan, 2017).

ARTICLE 19 and Digital Rights Foundation Pakistan

Article 19 and the Pakistan Digital Rights Foundation have expressed grave reservations about the planned Electronic Crime Prevention Act ("PEC Act") in Pakistan. The law has a number of provisions that, if adopted, would infringe on people's right to free expression and privacy. We urge Pakistani Senate members to vote no on the bill, and we encourage the Pakistani government to ensure that any new cybercrime legislation adheres to international human rights norms.

Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system:

We are concerned about Article 34 of the Act, which grants the Pakistan Telecommunications Authority ("PTA") extensive "management intelligence" and unprecedented powers to seek the deletion or blocking of "any" internet content without requiring a court judgement. The PTA or "any official authorized on its behalf" can order any service provider to delete or block access to any intelligence if it deems it necessary "for the glory of Islam" or "integrity," and Pakistan's security or national defence "or is based on" friendly relations with foreign countries, public order, dignity, morality, contempt of court, or committing a crime. To put it another way, this clause grants the government complete authority to block access to any information on the Internet that it deems objectionable. The justifications for restricting access to such data go far beyond the legitimate aims outlined in Article 19 of the International Covenant on Civil and Political Rights. "The glory of Islam," "friendly relations with foreign countries," and "dignity" are only a few examples. Furthermore, this section does not effectively allow for the opportunity to appeal or judicial review decisions in any circumstance. Article 34 (2), on the other hand, simply provides that the federal government "may create regulations by which the Agency shall apply policies and processes in line with this Article to monitor and prohibit access and receive complaints." Furthermore, we are concerned with Article 34 (2) and Article 34 (3). Give the government extensive powers to monitor internet information that violates international standards for freedom of expression and privacy using technology like deep packet inspection. In this regard, the four special duties of freedom of speech said in their 2011 joint statement on freedom of expression, "The content filtering system imposed by the government or government-mandated commercial service providers that are not under the authority of end users is a type of pre-censorship." It cannot be used to stifle freedom of expression." In short, Article 34 is overbroad and without adequate safeguards to protect freedom of expression and privacy, which is a violation of international human rights law.

Overbroad offences against misuse of computers and lack of public interest defense:

We found that computer abuse crimes or "hacking" crimes did not include a public interest defense for illegal access to computer system information, programs, or data for lawful reasons, such as investigative or investigative reporting, in our examination of the previous iteration of the bill. These issues are still unresolved. Instead, the majority of earlier computer crimes have been replaced by fewer sections and preventative measures phrased in overly broad language. Section 3 of the Act, for example, makes it illegal for "anyone who deliberately gains unlawful access to any information or data system." The offence carries a maximum sentence of three months in prison or a fine of up to 50,000 rupees, or both. The extent of this offence is exceedingly broad, and therefore breaches international human rights law's legality standards. People who try to access material on government-blocked websites may be prosecuted if the measure passes, because access to that material will not be "approved." Furthermore, the offences in Article 3 are in violation of the 2001 Cybercrime Convention's best practice guidelines. The crime does not, for example, need illegal conduct to violate security measures or have "intent." Obtaining computer data or having other nefarious motives. Article 5 of the Act, which criminalizes interfering with information systems or data but does not require such interference to inflict substantial harm, raises similar issues. The law does not recognize that interest groups can legitimately participate in peaceful "online protests" by seeking to disrupt access to the website without causing any actual harm to the website in the absence of such restrictions or preserving the public interest. For instance, suppose access to a government website is momentarily redirected to an interstitial page with legal information. Worse, Section 4 of the bill makes it illegal to copy or transmit data without permission. We are concerned that Internet service providers may be penalized if they send data without consent, despite the fact that the offence now includes the "intent" criterion. To put it another way, Article 3 plainly imposes certain unspecified licensing obligations. We also found that governments are not required to adopt such sections by the "Cybercrime Convention." We believe it is overbroad and infringes on international human rights law's legality criteria.

Cyber-Crime Issues and Legislation: Pakistani Context

Cybercrime is one of the world's most serious issues. Almost every country, whether established and developing, has taken drastic legal measures to tackle the menace of cybercrime. They enacted legislation to combat cybercriminals. However, developing countries, like Pakistan, are among the unfortunate few countries with a nascent cybercrime law. We won't have to deal with nearly as much cybercrime here. In fact, Pakistan is currently dealing with a variety of cybercrimes, including online cash transfer crimes, online pornography, illegal commodities trafficking, online gambling, intellectual property crimes, e-mail spoofing, online tracking, forgery, unauthorized access, and so on. Access to computer networks, electronic data theft, virus/worm attacks, logic bombs, Trojan horse attacks, Internet time theft, password cracking, buffer overflows, and other methods are used. It was primarily linked to cybercrime filed by women in 2013. According to Pakistan's most recent cybercrime data analysis, software piracy costs the country more than $315 billion each year (Pakistan Observer).

The war on malware cost the United States $500 billion in 2014. (The News International, 2014). Pakistan is one of the leading countries in terms of cybercrime, despite the fact that it has a number of laws in place to combat it. According to an inquiry, 10 to 15 incidences of account hacking are reported every day, with potentially dangerous outcomes such as illegal and unauthorized financial transfers and withdrawals from consumers' bank accounts. With the exponential development of mobile phone use and Internet accessibility, it is clear that cybercrime in Pakistan is constantly expanding (Kundi et al., 2008). These crooks have been discovered to exploit cutting-edge technology in their crimes (financial affairs, information theft, and sometimes even terrorism). Pakistan has established the National Cybercrime Response Center (NR3C) to monitor, track, and catch cybercriminals in order to prevent and battle them. All local and international cybercriminal organizations in Pakistan can contact NR3C through a single point of contact. He also conducts security-related training and education for government, semi-government, and private sector companies, as well as seminars and workshops to teach users how to protect their information resources from cyber-attacks and information leaks, and how to safeguard their systems. These dangers (Jamil, 2006). However, in 1996, Pakistan established the Electronic Transactions Act, which was followed by the 2008 Electronic Transactions Regulations, which were both signed by former Pakistani President Pervez Musharraf. The Electronic Crime Prevention Regulations (CEEC) 2007 was promulgated by the General Husband (Rtd) in December 2007, however it expired in 2010. These offences, according to the legislation, are examined directly by the Pakistan FBI and entail account fraud, internet fraud, access to protected data, system damage, and so on. There are 21 articles in all. Article 6 of the law states that if a criminal manipulates any private, security, or public information or system, or utilizes such information in an illegal manner, he will be sentenced to two years in prison. Penalties and fines. a large sum (Jamil, 2006). In addition, on January 17, 2007, the Federal Cabinet adopted the 2007 Electronic Crime Prevention Act.

For 17 forms of cybercrimes, including cyber terrorism, website hacking, and illicit access to secure data, the 2007 Electronic Crime Prevention Act imposes punishments ranging from six months to death (Jamil, 2006). It also includes cyber terrorism, criminal access, criminal data access, electronic fraud for data corruption, electronic forgery, illegal code access, inappropriate use of encryption, code abuse, network tracking, and guidance. Crimes involving sensitive electronic crimes have harsh punishments (Kundi et al., 2012). For cybercriminals who commit crimes involving sensitive electronic systems, the legislation proposes a maximum sentence of execution or life imprisonment. In addition to the aforementioned legislation, the government has filed to the Cabinet a new bill called the 2014 Electronic Crime Prevention Act, which provides some harsh penalties for cybercrime; nonetheless, it is faulty in that it allows all offences to be chargeable (Jamil, 2006). The draught law, on the other hand, will address cyber terrorism, unauthorized interception, unlawful access to information systems and programs or data, illegal interference with programs or data, electronic forgery, identity theft, and women's safety.

Conclusion

The study's conclusion is that the Internet, computers, mobile phones, and other types of technology have revolutionized every area of human life. Cybercrime is a broad word that encompasses computer-assisted criminality. In most nations around the world, estimating the quantity of cybercrimes is nearly impossible. Pakistan is one of the leading countries in terms of cybercrime, despite the fact that it has a number of laws in place to combat it. Cybercrime is on the rise in Pakistan, thanks to the exponential surge in mobile phone use and Internet accessibility. Cybercriminals are monitored, tracked, and apprehended by the National Cybercrime Response Center (NR3C). On January 17, 2007, the Federal Cabinet passed the 2007 Electronic Crime Prevention Act. Cybercrimes, including as cyber terrorism, website hacking, and unauthorized access to secure data, are punishable by the law, with punishments ranging from six months to death.

References

Barr, R. & Pease, K. (1990). Crime placement, displacement, and deflection", in: M. Tonry & N. Morris (eds), Crime and Justice: A Review of Research, 12(3): 12-23, University of Chicago Press, Chicago.

Bryan-Low, C. (2012). Hackers-for-hire are easy to find. Wall Street J. 2012.

Commonwealth Secretariat (2002, October). Model law on computer and computer related crime, [Online] available at: http//: commonwealth.live.poptech.coop/shared_asp_files/uploadfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf , (March 30, 2014).

Chapman, A., & Smith, R.G. (2001). Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice, 2: 189, Australian Institute of Criminology, Canberra.

Chaudhry, Y. (2011). A country without cyber-law: Pakistan, [Online] available at: http://propakistani.pk/2011/01/10/a-country-without-cyber-law-pakistan/10,june 2011/, (March 30, 2014).

Furnell, S. 2002. Cyber Crime: Vandalizing the Information Society. London: Addison Wesley.

Grabosky, P. 2001. "Virtual Criminality: Old Wine in New Bottles?" Social & Legal Studies 10: 243–249. doi:10.1177/ a017405.

Herhalt, J. (2011). Cyber-crime-A growing challenge for governments, KPMG Issues Monitor, 8: 1-24, [Online} available at: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf, (March 26, 2014).

Holt, T. J., and A. M. Bossler. 2016. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series. New York: Routledge.

Holt, T. J., A. M. Bossler, and K. C. Seigfried-Spellar. 2018. Cybercrime and Digital Forensics: An Introduction. 2nd ed. New York: Routledge.

Huff, R., Desilets, C., & Kane, J. (2010). National public survey on white-collar crime. Rockville: National WhiteCollar Crime Ctr.

Jamil, Z. (2006). Cyber Law, Presented at the 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, 2006, Jamil and Jamil Law Associates, Islamabad, Pakistan, [Online] available at: http://jamilandjamil.com/wpcontent/uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf, (March 26, 2014).

KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.

Levi, M. (1998). Organized plastic fraud: Enterprise criminals and the side-stepping of fraud prevention, The Howard Journal, 37(4): 423-38.

Lewis, J. (2018). Economic Impact of Cybercrime, No Slowing Down. McAfee

Madhava S.S.P., & Umarhathab, S. (Eds.), (2011). Information Technology Act and cyber terrorism: A critical review. Cyber Crime and Digital Disorder, Tirunelveli, India: Publications Division, Manonmaniam Sundaranar University.

Magalla, A. (2013). Security, prevention and detection of cyber-crimes in Tanzania, Doctoral Thesis, Tumaini University Iringa University College, [Online] available at: http://www.academia.edu/3471542/the_introduction_to_cybercrime_security_prevention_and_detection_of _cybercrime_in_tanzania, (March 26, 2014).

McGuire, M., and S. Dowling. 2013. "Cybercrime: A Review of the Evidence." Home Office Research Study. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf.

Porche, I.R. (2019). Fighting and winning the Undeclared Cyberwar. The Rand Blog. June 24. 2019. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclaredcyber-war.html.

Poulsen, K.P. (2018). The Decades' 10 most dastardly cybercrimes. Retrieved August 25, 2020 from: https://www.wired.com/2009/12/yecybercrimes/.

Rasch, M.D. (1996). Criminal law and the internet, in the internet and business: A Lawyer's guide to

the emerging legal issues, International Judicial Review, 3(1): 1-17.

R.S. (2007). Pakistan's Cyber Crime Bill 2007: Cyber Crime, Cyber law, e-Governance, hacking and Pakistan, January 20, 2007, [Online] available at: http://southasiaict4d.wordpress.com/2007/01/20/pakistans-cyber-crime-bill-2007/ (March 26, 2014).

Tcherni, M., A. Davies, G. Lopes, and A. Lizotte. 2016. "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" Justice Quarterly 33: 890–911. doi:10.1080/07418825.2014.994658.

Wall, D. S. 1998. "Catching Cybercriminals: Policing the Internet." International Review of Law, Computers & Technology 12: 201–218. doi:10.1080/13600869855397.

Wall, D. S. 2001. "Cybercrimes and the Internet." In Crime and the Internet, edited by D. S. Wall, 1–17. New York: Routledge.