International Journal of Human and Society (IJHS)

P-ISSN: 2710-4966	E-ISSN: 2710-4958
Vol. 4. No. 01 (Jan-Mar) 2024	Page 1323-1335

Revamping Cybercrime Laws In Pakistan: A Comparative Analysis Of Pakistan And United Kingdom

Hamaish Khan	Research Officer, Research Center, Supreme Court of Pakistan at Islamabad hamaishkhan010@gmail.com
Syeda Saima Shabbir	Senior Research Officer, Supreme Court of Pakistan at Islamabad. Syeda_saima@yahoo.com
Ashraf Ali	Chairperson, Department of Law, Abdul Wali Khan University, Mardan, KP, Pakistan ashrafali@awkum.edu.pk
Aisha Nayab Qureshi	Lecturer, Department of Political Science, Women University Swabi, KPK, Pakistan aishanayabqureshi@gmail.com

Abstract: *In this modern era the global connectivity has touched the horizon and abolished the digital borders across the globe. All the human beings have easy access to the online social platforms, whereby they interact with fellow beings. Similarly, most of the routine manual work is digitalized and put online. At one side it has advanced the daily business, on the other hand all the activities and data remains at risk of cyber-attacks.*

A criminal act in which an Android device, window device, a network of computer and a computer is used and targeted for an offence act is termed as cybercrime. It also refers to illegal access to social media, email and similar platforms of an individual or other legal entity. Cybercrimes includes fraud of internet and email, fraud of identity, financial theft, theft of data for payment of card, cyber-extortion, cyberstalking, spamming, cyberterrorism, online harassment, child pornography, theft and sale of corporate data, scams of phishing, spoofing of websites, ransomware, malware, hacking of IOT etc.

Pakistan being one of the top populous countries in the world having in use of large internet accessibility. The Prevention of Electronic Crimes Act, 2016 (PECA, 2016) is the relevant law relating to cybercrimes in Pakistan. The United Kingdom is one of the developed countries in the world. Use of internet is backbone of governance system of UK. UK has effected very comprehensive legislation relating to cybercrimes. The main codified cybersecurity laws are the Computer Misuse Act, 1990 (CMA, 1990), while other relevant cybersecurity laws include, the, Police and Justice Act, 2006, Serious Crime Act 2015, Communication Act 2003.

This research article analyzed cybercrime laws and its implementation mechanism with special reference to Pakistan and United Kingdom. Cybercrime laws and implementation mechanisms of the UK are comparatively analyzed with cybersecurity laws and implementation machinery of Pakistan. Major deficiencies are highlighted in cybersecurity laws and its implementation machinery of Pakistan and fruitful suggestions are provided for codification of cybersecurity laws, its effective implementation and eradication of cybercrimes in light of comparison of cybersecurity laws and implementation system of UK.

Keywords: Cybercrimes, PECA, Computer Misuse Act, Pakistan and UK Comparison, FIA, NCA, NCSC.

Introduction

Computers, mobiles phones and other telecommunication devices using internet have reduced the distances between people along the

world and thus, every person anywhere around the globe can have the access to talk and discuss their feelings, enjoy social relations and well as expand professional set up by just adopting the latest version of technology (Daley et al., 2016; Cullen et al., 2017; Daudpota, 2017;Clemons and Banattar, 2018; Dadkhah et al., 2018; Damian, 2019;Smith et al., 2020; Solheid et al., 2020). Today when we put a look around ourselves we find devices and machines everywhere which are the gift of technology and humans are very much dependent on the technology nowadays (Goel, 2016; Dzomira, 2017; Feng et al., 2017; Frensh and Mulyadi, 2018;Ferguson et al., 2019; Johnston and Cooper, 2020; Moe and Kalling, 2020).

By the advent of technology, it has been frequently used in every field of life, due to which the security maintenance, data confidentiality, and privacy have become a challenge. More specifically the security of digital data has become difficult due to the increasing cybercrimes (Goodman, 1997; Holt, et al., 2015; Hashmi et al., 2016; Herald, 2016; Greer, 2017;Hollis, 2017; Hui et al., 2017; Hu et al., 2018;Hasinoff and Krueger, 2020). A cybercrime is said as unethical attempt by the hacker or the computer professional to breach data or misusing the confidential information of an organization or individual. The computer experts of professional make crimes by getting access to the users' confidential data without permission. With the increasing use of technology in almost every field, the number of cybercrimes is becoming uncountable (Intravia et al., 2017; Keyser, 2017; Jiwoong at al., 2018;ladanza et al., 2019; Issac, 2019; Iwasokun, 2019;Kisharwani et al., 2019; Jeffries and Apeh, 2020; Johnson and Manickavasagam, 2020;Kapoor et al., 2020). Another concerning fact is that very few of the cybercrimes are reported worldwide and many of such crimes remain unreported. The experts get access to the companies or big corporations, confidential data, approach to their weakness via either website or other digital platform, and then misuse it (Khan et al., 2010; Kundi et al., 2014; Laeseke et al., 2020).

Although the governments worldwide and the law enforcement agencies are working too hard to control the increasing number of cybercrimes but still a lot more is required to protect people from such dangerous minds (Mittal, 2012; Marcum and Higgins, 2019). Crime is the plague of society and not matter whatever steps are taken it cannot be stopped but still the governments always take steps for their control by enacting laws according to the nature of the offences (Nel and Burger, 2017; Mohamed, 2019; Kim at el., 2020). Among various companies and organizations working all over the world have complained about such type of criminal activities including 30% loss in copy right agencies, 35% interference into personal information of the organizations, 12% financial loss, 23% harm to the networking statistics and many more (Truyens and Van Eecke, 2016; Van Baak and Hayes, 2018). Pakistan is one of the major users of technology in every field of life. Thus, Pakistan is also fallen prey of cyber attacks. The existing law is not enough to coup with the prevailing circumstances. Hence, there is dire need of revamping of cybercrime law in Pakistan. United Kingdom has comprehensive legislation regarding cybercrimes. Consequently, cybercrime law of Pakistan may be revamped with comparison to United Kingdom.

Statement of the Research Problem

This research article focuses on the existing legislation of cybercrime laws and its implementation mechanism in Pakistan and United Kingdom. Cybersecurity space of the above mentioned countries will be comparatively analyzed. Deficiencies in the cybersecurity laws and implementation system of Pakistan will be highlighted in comparison with that of UK. It will be discussed that what kind of cybercrimes are committed and how it will be curtailed through proper legislation and fruitful implementation.

Significance of the Study

This research study has a great significance and relevancy in the modern digitalized and online world. It will enable the readers to get knowledge about cybercrimes, cybersecurity laws and grievances agencies. The current

cybersecurity laws are analyzed and a comprehensive plan of action has been suggested for a harmonized legislation in the mentioned countries, coupled with its implementation techniques, especially in Pakistan with comparison to UK. Recommendations are given for revamping of cybercrime law of Pakistan. At Policy level, it will also benefit the mentioned countries, especially Pakistan for effective legislation and implementation of cybersecurity laws in a better manner.

Literature Review

The notion 'Cybercrime' initially came into surface in famous science fiction novel "Neuromancer", written by Will Gibson in the year 1985 (Lavigne, 2008). Due to its intermittent use in a variety of contexts, this term gained its entrance in the common lexicon (Jamil, 2006). In addition, Navneet K., stated that a crime is known as any punishable and illegal act by government or industries establishment, out of all of the multifold offences that take place frequently, the most practiced are that which are committed online as cybercrimes,(Navneet, 2018). Cybercrimes are increasing at accelerating momentum across the globe as a result fast growing technology and its use in all walk of daily business ant its vulnerability to online attacks due to weak safeguarding shield. The current implementation strategy, hardware, software and technology adopted by the law enforcement agencies for hunting of hackers, complex investigation and its eradication is outdated and inadequate for curbing novel forms of cybercrimes. Cyber-criminal acts and cyber operations that constitute cyber war has same methods but with different motives and threshold.

For specification of various types of virtual crimes different nomenclature techniques are adopted. The cyber-dependent crime and the cyber enabled-crime are the two explicit terms used by Gordon and Ford for specification of cybercrimes (Gordon, & Ford, 2002). The insertion of malicious and mischievous software, denial of service (DDOS), crimes encompassing hacking are cyber-dependent crimes, which are done by using computer or related window device. Online economic and social networking frauds comes under the category of cyber-enabled crimes, as these are preceding sort of crimes, committed in large scale and severity through internet (McGuire & Dowling,2013). Cybercrimes are further specified into three main categories by Navneet: the cybercrimes against persons (malware, computer sabotage, salami attacks, cyber stalking, cyber-defamation, spamming, phishing, email harassment), cybercrimes against property(logic bomb, Trojan horse, unauthorized intrusion, system hacking, cyber-vandalism, cybersquatting, intellectual property crimes) and cybercrimes against organizations (mail bomb, virus attack, denial attack, password theft, hacking) (Navneet, 2018). Smith categorized cybercrimes as syntactic, semantic and blended (Smith, 2015).

The exclusively technical and self-replicating that the victim unintentionally opens, as mainly noted in ransomware attacks, are the synthetic crimes. Semantic crimes refer to social networking, while amalgamations of both are referred as blended crimes (Huff, Desilets, & Kane, 2010) . Sometime the technique encompasses in the amalgamated crimes enumerate the attacker approaching the victim and presenting an answer to a reasonable issue conclusively suitable that the victim on consent gives permission to financial and personal details to the hacker. In such situation, the attacker sold the personal details obtained from the victim and also use it in order to commit further online fraud. Virtual economies are at the stake of risk of cybercrimes. Victimization through cybercrimes has gained momentum in the last decade, especially in respect to harass online (Jones, Mitchell, &Finkelhor, 2013).

Prevention of electronic crimes is an important aspect that must be deal to resolve the ever increasing issues related to technology and its uses. It is not so far when there was no concept of talking to people living far away from each other (Tim et al., 2017). However, with the passage of time and advancement in technology helped the people to listen the voices of their dear ones for their satisfaction and provided a peace to their hearts. Moving one step ahead,

revolution of internet globalized the world and shringkage of distances occurred (Vertes-Olteanu, 2014;Stefan et al., 2020; Tonellotto, 2020).

Research Methodology

The present study is related to social science that depicts the human behavior and life and thus, can be categorized as the qualitative (use of word and phrases) rather than quantitative (use of numeric digits) (Stauss and Corbin, 1998).

In this research article the Qualitative Research Methodology has been applied. The existing cybersecurity laws, rules and regulations of Pakistan and UK are studied and textually analyzed. Cybercrimes data of NCSC, NCA, UK's National Fraud and Cybercrime Reporting Center, Scotland Yards and all other relevant agencies will be studied, compiled and analyzed. All the relevant technical and legal texts, books and journals are studied in-dept. Interviews of the jurists, prosecutors, relevant law enforcement authorities are conducted. Relevant research papers of the scholars are also analyzed and conclusion is adduced.

Different Kinds of Cybercrimes

Cybercrime refers to any criminal activity that is committed using computers, networks, or digital devices as the primary means of perpetrating the offense. It includes, Hacking and Unauthorized Access, Malware and Ransomware Attacks, Phishing and Social Engineering, Identity Theft and Fraud, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Cyber Espionage and State-Sponsored Attacks, Data Breaches and Information Leaks, Cyberbullying and Online Harassment, Financial Cybercrimes, Cyber Extortion, Child Exploitation, Cyberstalking, Cyberwarfare and Cyber Terrorism, Cyber Smear Campaigns, Data Manipulation and Tampering, Cyberbullying in Gaming, Insider Threats, Carding and Credit Card Fraud, Election Interference, Virtual Currency Theft, Online Scams and Phishing Schemes, Cyber Blackmail, Internet of Things (IoT) Exploitation, Cyber Espionage for Intellectual Property Theft, AI and Deepfake Exploitation, Unlawful Access to Sensitive Research Data.

Cybercrime Laws in Pakistan

Cybercrime laws in Pakistan have evolved over the years to address the growing threats and challenges posed by advancements in technology. The government of Pakistan recognizes the importance of combating cybercrime and has enacted several Acts and regulations to deal with various forms of cyber offenses. Let's delve into the key legislations related to cybercrime in Pakistan:

1. The Pakistan Telecommunication (Re-organization) Act, 1996

The Pakistan Telecommunication (Re-organization) Act, 1996 is an important legislation in Pakistan that addresses various aspects of telecommunications, including provisions related to cyber crimes. The Act was enacted to regulate and reorganize the telecommunication sector in the country and establish the Pakistan Telecommunication Authority (PTA) as the regulatory body for the industry. While the Act does not specifically use the term "cyber crimes," it contains several provisions that can be applied to offenses committed in the digital realm. Sections 31 and 32 are relevant provisions relating to cybercrimes

2. The Electronic Transactions Ordinance (ETO) 2002

The Electronic Transactions Ordinance (ETO) 2002 of Pakistan is a legislation that addresses various aspects of electronic transactions, including cyber crimes. It provides legal recognition and regulatory mechanisms for electronic communications, transactions, and records. The ETO aims to facilitate e-commerce, ensure the security and authentication of electronic transactions, and discourage cyber crimes. Several sections of the ordinance specifically deal with cyber crimes and their corresponding penalties. Sections 34 to 37 are relevant provisions.

3. The Prevention of Electronic Crimes Act, 2016 (PECA)

The Prevention of Electronic Crimes Act, 2016 (PECA) is a legislation enacted by the Government of Pakistan to address various

forms of cybercrime and electronic offenses. PECA was introduced to tackle the growing threats and challenges posed by cybercriminals, protect the rights of individuals in cyberspace, and provide a legal framework for investigating and prosecuting electronic crimes in the country. The Act consists of several sections that define offenses, penalties, and procedures for handling cybercrimes. Sections, 3 to 27 are relevant to cybercrimes.

CYBERCRIME LAWS IN UNITED KIGDOM

Cybercrime has become a significant concern in the digital age, and the United Kingdom has implemented robust laws to address this growing issue. The UK has enacted several legislations and regulations specifically designed to combat cybercrime and protect individuals, businesses, and the overall security of the nation's digital infrastructure. Following is the key legislation on cybercrimes in UK;

1. Computer Misuse Act 1990

The Computer Misuse Act 1990 is a significant law in the United Kingdom that deals with cybercrime and unauthorized access to computer systems. It was enacted to address the growing concerns regarding the misuse of computers and to establish legal consequences for such activities. The act has since been amended and updated to keep up with advancements in technology and the evolving nature of cyber threats.

The Computer Misuse Act 1990 is a piece of legislation in the United Kingdom that addresses cybercrime and unauthorized access to computer systems. It was enacted to protect computer systems and data from unauthorized access, modification, and misuse. The act defines various offenses and penalties related to computer misuse and provides a legal framework for prosecuting individuals involved in cybercrimes. Its relevant sections are 1 to 3.

2. Police and Justice Act 2006

The Police and Justice Act 2006 is an important legislation in the United Kingdom that addresses various aspects of law enforcement and criminal justice. While it does not specifically focus on cyber crimes, it contains provisions that are relevant to tackling offenses related to cybercrime. Sections 35 to 37,40 and 41 are relevant provisions.

3. Serious Crime Act 2015

The Serious Crime Act 2015 is an important piece of legislation in the United Kingdom that addresses a wide range of serious offenses, including cyber crimes. The act enhances the powers of law enforcement agencies to investigate and prosecute individuals involved in cyber criminal activities. It introduces various provisions aimed at combating cyber offenses and ensuring the security of individuals, businesses, and critical infrastructure in the digital age.

Its relevant sections are 41, 42, 45 and 50.

4. Communication Act 2003

The Communication Act 2003 is legislation in the United Kingdom that addresses various aspects of electronic communication, including the regulation and prevention of cybercrimes. While the Act primarily focuses on the regulation of telecommunications networks and services, it contains provisions that are relevant to tackling cybercrimes. Its relevant sections are 125 to 131.

5. Fraud Act 2006

The Fraud Act 2006 is a significant piece of legislation in the United Kingdom that deals with various types of fraudulent activities, including cybercrimes. This Act was introduced to replace the outdated legislation on fraud and to provide a comprehensive legal framework to tackle fraudulent behavior. The Act outlines specific offenses, provides definitions, and establishes penalties for individuals involved in fraudulent activities, including those conducted through cyberspace. Its relevant sections are 2 to 11.

6. Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) is a comprehensive legislation in the United Kingdom that governs the protection and processing of personal data. It aligns with the

European Union's General Data Protection Regulation (GDPR) and provides a legal framework for data protection in the UK. While the DPA 2018 primarily focuses on data protection, it also contains provisions to address cyber crimes and ensure the security of personal data.

In relation to cyber crimes, the DPA 2018 includes several key provisions that aim to safeguard personal data from unauthorized access, data breaches, and other forms of cyber attacks. These provisions outline the obligations of organizations and individuals who handle personal data, as well as the rights of data subjects. Its relevant sections are 2, 67, chapter 2 and chapter 3.

Deficiencies in Prevention of Electronic Crimes Act, 2016

Major deficiencies in the Prevention of Electronic Crimes Act 2016 of Pakistan are following:

1. **Vague Definitions and Ambiguous Terminology:** The Prevention of Electronic Crimes Act 2016 suffers from several deficiencies in terms of its definitions and use of ambiguous terminology. Many critical terms, such as "cybercrime," "data," and "cyber-terrorism," are either inadequately defined or left open to interpretation. This lack of clarity creates confusion and leaves room for misuse and abuse of the law.
2. **Overbroad and Restrictive Powers:** The Act grants extensive powers to law enforcement agencies, including the authority to conduct surveillance, intercept communications, and seize digital devices without adequate checks and balances. These powers can be easily misused and violate an individual's right to privacy, leading to potential harassment and abuse of power.
3. **Lack of Procedural Safeguards:** One of the significant deficiencies of the Act is the absence of robust procedural safeguards to protect the rights of individuals accused of electronic crimes. The law allows for arbitrary arrests and extended pretrial detention. The absence of stringent safeguards increases the risk of wrongful arrests and undermines the fundamental principles of due process and fair trial.
4. **Lack of Clarity on Offenses and Penalties:** The Act fails to provide a clear and comprehensive list of offenses, leaving room for subjective interpretation. The absence of specific definitions and guidelines can lead to inconsistencies in the application of the law and may result in arbitrary arrests and unfair treatment. Furthermore, the Act imposes disproportionately harsh penalties for certain offenses, which can be disproportionate and unjust.
5. **Inadequate Protection of Freedom of Expression:** The Act contains provisions that can be used to curtail freedom of expression and suppress dissenting voices. Vague provisions on the prohibition of online content that is considered "obscene," "immoral," or "harmful to national security" can be misused to stifle legitimate speech and criticism. The lack of clear boundaries and safeguards for freedom of expression undermines democratic values and restricts the public's right to information.
6. **Insufficient Protection for Whistleblowers and Journalists:** The Act fails to provide adequate protection for whistleblowers and journalists who expose corruption or wrongdoing through digital platforms. The absence of clear provisions to safeguard the anonymity and privacy of whistleblowers can deter individuals from coming forward, thus undermining efforts to combat cybercrimes and promote transparency.
7. **Inadequate International Cooperation:** The Act lacks comprehensive provisions for international cooperation and coordination on cybercrime-related matters. Given the transnational nature of cybercrimes, effective collaboration with international law enforcement agencies is crucial. The absence of robust mechanisms for

cooperation hampers efforts to investigate and prosecute cybercriminals operating across borders.

8. **Limited Focus on Cybersecurity Measures:** While the Act primarily focuses on criminalizing cyber offenses, it lacks adequate provisions to promote cybersecurity and protect critical information infrastructure. The Act falls short in addressing the need for preventive measures, such as promoting awareness, establishing effective cybersecurity frameworks, and encouraging public-private partnerships to enhance cybersecurity practices.

Thus, the Prevention of Electronic Crimes Act 2016 of Pakistan has significant deficiencies that undermine its effectiveness and potential for misuse. The vague definitions, overbroad powers, lack of procedural safeguards, and inadequate protection of fundamental rights raise concerns about privacy, freedom of expression, and due process. To ensure the proper protection of citizens' rights and effective response to cybercrimes, it is crucial to address these deficiencies and bring the law in line with international standards and best practices.

Need For Revamping of Cybercrime Laws in Pakistan

Cybercrime has emerged as a significant threat in the digital age, and Pakistan, like many other countries, is grappling with the challenges it presents. However, the existing cybercrime laws in Pakistan are outdated and inadequate, necessitating a revamp to effectively combat cyber threats. A comparative analysis with the cybercrime laws of the United Kingdom highlights the pressing need for Pakistan to update its legislation in this area;

Cybercrime Landscape in Pakistan

I. Lack of Greviencess Redressal Forum Adequately

The rapid advancement of technology and widespread internet usage has made Pakistan vulnerable to cybercrimes such as hacking, identity theft, online fraud, and cyberbullying. The current laws in Pakistan fail to adequately address these emerging threats, leaving individuals, businesses, and the overall cybersecurity infrastructure exposed.

II. **Outdated Framework:** Pakistan's primary legislation governing cybercrime is the Prevention of Electronic Crimes Act (PECA) 2016. However, this law fails to encompass various cybercrimes and lacks specific provisions to deal with emerging threats like crypto currency-related crimes, ransomware attacks, and data breaches.

III. **Incomplete Jurisdiction:** The jurisdictional limitations of current laws make it difficult to prosecute cybercriminals effectively. The absence of extraterritorial jurisdiction hampers the investigation and prosecution of cross-border cybercrimes, hindering international cooperation.

IV. **Insufficient Penalties**: The penalties prescribed under the existing legislation are often lenient and fail to act as effective deterrents. Cybercriminals can exploit this weakness, knowing that the consequences for their actions may not be severe enough to discourage them.

V. **Inadequate Procedural Mechanisms:** The procedural mechanisms for investigating and prosecuting cybercrimes in Pakistan need improvement. Law enforcement agencies lack specialized training and resources, resulting in a slow and ineffective response to cyber threats.

VI**. Lack of Specialized Law Enforcement Agency:** There is no specialized law enforcement agency to deal with cyber crimes in Pakistan. The role has been given to the Cyber Crime Unit of FIA, however, which is ineffective.

2. Cybercrime Laws in the United Kingdom in Contrast

The United Kingdom has recognized the importance of robust cybercrime legislation and has taken significant steps to address this issue. The UK's primary legislation, the Computer Misuse Act 1990, has been periodically updated to keep pace with technological advancements and emerging cyber threats.

I. **Comprehensive Scope:** The UK legislation covers a wide range of cybercrimes, including unauthorized access to computer systems, data interference, and the creation and distribution of malware. This broad coverage ensures that new and emerging cybercrimes are adequately addressed.

II. **Extraterritorial Jurisdiction:** The UK laws provide extraterritorial jurisdiction, allowing authorities to investigate and prosecute cybercriminals even if the offenses are committed outside the country. This facilitates international cooperation in combating cybercrime.

III. **Strict Penalties**: The United Kingdom imposes strict penalties for cybercrimes, including imprisonment and hefty fines. These penalties serve as effective deterrents, discouraging potential offenders and protecting the interests of individuals and businesses.

IV. **Specialized Law Enforcement Units:** The UK has established specialized law enforcement units, such as the National Cyber Crime Unit (NCCU), to combat cybercrimes effectively. These units receive specialized training and possess the necessary expertise to investigate and respond to cyber threats promptly.

The comparison with the cybercrime laws of the United Kingdom underscores the urgency for Pakistan to revamp its legislation. By modernizing its cybercrime laws, Pakistan can address the gaps in its legal framework, expand the scope of cybercrimes covered, enhance penalties to deter offenders, establish extraterritorial jurisdiction, and provide law enforcement agencies with specialized training and resources. These measures will strengthen Pakistan's ability to combat cyber threats effectively and protect its citizens, businesses, and national security in the digital age.

CONCLUSION

To sum up it is inferred that, in today's modern world technology has reshaped day to day routine work and interactions of humans. Internet is used in every field including education, business, banking, health, defense etc. Billions of people are using computers, laptops, android devices, mobile phones and interact with each other online. One hand technology has made life easily, while on the other hand online business, digital transactions and privacy of people are at risk in the hands of cyber criminals. Cybercrimes are increasing day by day across the globe. Pakistan has also been attacked by hackers frequently. In order to combat cybercrimes, various laws have been codified. Prevention of Electronic Crimes Act, 2016 is the main legislation on cybercrimes. However, there are various loopholes in the existing cybercrime laws of Pakistan. On the other hand, United Kingdom has done very comprehensive legislation to combat cybercrimes. In this research paper cybercrime laws of Pakistan and United Kingdom have been discussed in detail. Major deficiencies in cybercrimes laws of Pakistan have been highlighted, including using of ambiguous terminologies, restrictive powers, limited scope, no proper safeguard for witness and whistleblowers, no clarity of offences and its penalties etc. It has been discussed that how cybercrimes laws of Pakistan may be revamped in light of comparison of cybercrimes laws of United Kingdom. It has been suggested that cybercrime laws of Pakistan can be revamped by enhancing cyber incident response, collaboration with international partners, capacity building programs, strengthen data protection laws, improved oversight mechanisms, encryption policies, expedited cybercrime investigation, international cooperation in investigations and public awareness and digital literacy programs.

SUGGESTIONS

Based on previous discussion in research thesis, following are some of practical suggestions for revamping of cyber crime laws in Pakistan;

I. Strengthening Cybersecurity Measures

1. **Establishment of Specialized National Cyber Crime Agency:** There is dire need of establishing a specialized National Cyber Crime Agency for effective implementation of cyber crimes laws and investigation of cyber crimes. Only through a specialized National Cyber Crime Agency, it can

effectively investigate and prosecute cyber criminals, enhance cyber security measures and provide support to both public and private sectors.

2. **Enhancing Cyber Incident Response:** Establish a dedicated national cybersecurity incident response team to effectively handle and respond to cyber incidents promptly. This team should consist of experts from relevant government agencies and the private sector.
3. **Collaboration with International Partners:** Foster stronger collaboration with international cybersecurity organizations and law enforcement agencies to share information, best practices, and intelligence related to cyber threats. This collaboration will help Pakistan stay updated on emerging cyber threats and adopt effective countermeasures.
4. **Capacity Building Programs:** Invest in comprehensive cybersecurity training programs for law enforcement agencies, judges, prosecutors, and relevant stakeholders to enhance their understanding of cybercrime investigation techniques, digital forensics, and legal procedures.

II. **Protection of Digital Privacy and Data Protection**

1. **Strengthen Data Protection Laws:** Introduce comprehensive data protection legislation to safeguard the privacy and personal information of individuals. This legislation should outline clear guidelines for data collection, storage, and processing, and establish penalties for unauthorized access or misuse of personal data.
2. **Improved Oversight Mechanisms:** Establish an independent regulatory body to oversee the implementation and enforcement of data protection laws. This body should be responsible for conducting regular audits, investigating data breaches, and imposing fines or penalties on non-compliant entities.
3. **Encryption Policies:** Promote the use of strong encryption methods to protect sensitive data from unauthorized access. Encourage collaboration between the government and technology companies to develop secure encryption standards that strike a balance between privacy and security.

III. **Strengthening Legal Framework and Law Enforcement Capabilities**

1. **Clear Definitions and Classifications:** Clarify and expand definitions of cybercrimes, including offenses such as hacking, data theft, identity theft, cyberbullying, and online harassment. Clearly classify these offenses and establish appropriate penalties based on the severity of the crime.
2. **Expedited Cybercrime Investigation:** Streamline the process of cybercrime investigation by establishing dedicated cybercrime units within law enforcement agencies. These units should be equipped with the necessary technological resources and trained personnel to conduct swift and efficient investigations.
3. **International Cooperation in Investigations:** Strengthen mechanisms for international cooperation in cybercrime investigations. Develop agreements and protocols with other countries to facilitate the exchange of evidence, extradition of offenders, and joint operations against transnational cybercriminal networks.

IV. **Protection of Freedom of Expression and Digital Rights**

1. **Clear Guidelines for Content Removal:** Establish clear guidelines for the removal of online content to ensure that it is based on valid legal grounds and respects the principles of freedom of expression. Implement a transparent process for content takedown requests, with the involvement of an independent oversight body.
2. **Safeguard Against Online Censorship:** Prohibit arbitrary censorship of online content that may infringe upon the fundamental rights of individuals. Implement mechanisms to challenge and

review decisions regarding content removal or blocking.

3. **Public Awareness and Digital Literacy Programs**: Launch public awareness campaigns and digital literacy programs to educate citizens about their digital rights, responsible online behavior, and the potential risks associated with cybercrime. These programs should target both children and adults and include guidelines on safe internet usage.

By implementing these comprehensive measures, Pakistan can revamp the Prevention of Electronic Crimes Act 2016 (PECA) to effectively address emerging cyber threats, protect digital privacy and data, strengthen the legal framework, and safeguard the fundamental rights of individuals in the digital realm.

REFERENCES

Clemons, E.K. and Banattar, J., 2018, January. Regulating online privacy: Some policy guidelines, including guidelines for international harmonization. In Proceedings of the51st Hawaii International Conference on System Sciences.

Cullen, F.T., Wright, J.P., Gendreau, P. and Andrews, D.A., 2017. What correctional treatment can tell us about criminological theory: Implications for social learning theory. In Social learning theory and the explanation of crime (pp. 339-362).

Dadkhah, M., Lagzian, M. and Borchardt, G., 2018. Identity theft in the academic world leads to junk science. Science and engineering ethics, 24(1), pp.287-290.

Daley, M.J., Bolinger, T. and O'neal, H., Google Technology Holdings LLC, 2016. Systems and methods for synchronizing multiple electronic devices. U.S. Patent 9,307,508.

Damian, A.O., Bitdefender IPR Management Ltd, 2019. Systems and methods for detecting online fraud. U.S. Patent 10,171,497.

Daudpota, F., 2017. Pakistan-Understanding Its Law on Electronic Surveillance and Interception. Available at SSRN 2960330.

Dzomira, S., 2017. Plastic Money and Electronic Banking Services Espousal vis-a-viz Financial Identity Theft Fraud Risk Awareness in a Developing Country. Journal of

Feng, X., Asante, A., Short, E. and Abeykoon, I., 2017, November. Cyberstalking Issues. In2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th IntlConf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 373-376). IEEE.

Frensh, W. and Mulyadi, M., 2018. Criminal policy on cyberbullying toward children. In E3SWeb of Conferences (Vol. 52, p. 00050). EDP Sciences.

Goel, S., 2016. Cyber-crime: a growing threat to Indian banking sector. International Journal of Science Technology and Management, 5(12), pp.552-559.

Goodman, M.D., why the police don't care about computer crime, Harvard Journal of Law and Technology, 1997

Gordon & Ford (2002), Cyberterrorism? Computers & Security, 21(7), 636-647.

Greer, Brian. "The Growth of Cybercrime in the United States." Growth (2017).

Hashmi, D., Saleem, A. and Shah, M., 2016. The Protection of Pakistan Ordinance: Limitations and Prospects. Pakistan Journal of History and Culture, No. I (2014).

Hasinoff, A.A. and Krueger, P.M., 2020. Warning: Notifications About Crime on Campus MayHave Unwanted Effects. International Journal of Communication, 14, p.21.

Herald, Surf Safely: Evolution of the cyberspace laws in Pakistan, May 2016

Hollis, M.E., Downey, S., del Carmen, A. and Dobbs, R.R., 2017. The relationship between media portrayals and crime: perceptions of fear of crime among citizens. Crime prevention and community safety, 19(1), pp.46-60.

Holt, T.J., G.W. Burruss, A. M. Bossler., Policing cybercrime and cyberterror, Durham, Nc:Carolina Academic Press, 2015

Hu, X., Rodgers, K. and Lovrich, N.P., 2018. "We Are More Than Crime Fighters": Social Media Images of Police Departments. Police Quarterly, 21(4), pp.544-572.

Hui, K.L., Kim, S.H. and Wang, Q.H., 2017. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. Mis Quarterly, 41(2), p.497.

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

ladanza, E., Luschi, A., Gusinu, R. and Terzaghi, F., 2019, May. Designing a Healthcare Computer Aided Facility Management System: A New Approach. In International Conference on Medical and Biological Engineering (pp. 407-411). Springer, Cham.

Intravia, J., Wolff, K.T., Paez, R. and Gibbs, B.R., 2017. Investigating the relationship between social media consumption and fear of crime: A partial analysis of mostly young adults. Computers in Human Behavior, 77, pp.158-168.

Isaac, L., 2019. Now Boarding All Air Pirates: How Screening Women at Foreign Air Carrier Checkpoints Can Prevent Catastrophe. Available at SSRN 3450908.

Iwasokun, G.B., 2019. Factor Analysis-based Investigation into Financial Crime Related Issues in Nigeria, Global Journal of Computer Science and Technology.

Jamil (2006), Cyber Law, In 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on (pp. 11-14).

Jeffries, S. and Apeh, E., 2020. Standard operating procedures for cybercrime investigations: systematic literature review. In Emerging Cyber Threats and Cognitive Vulnerabilities(pp. 145-162). Academic Press.

Jiwoong, J.A.N.G., Kim, D., HanGyu, C.H.O., Choi, J. and Lim, D., LG Electronics Inc, 2018.Definition of new identifier in wireless access system that supports device to device communication, and transmission method and device using same. U.S. Patent 9,930,706.

Jones, Mitchell, &Finkelhor (2013), Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010). Psychology of violence, 3(1), 53.

John R. Vacca, Computer Forensics: Computer Crime Scene Investigation (second edition), 2002

Johnson, J. and Manickavasagam, B., 2020. Cyber Crimes Against Female Undergraduate Students of Thiruvananthapuram City, Kerala. Our Heritage, 68(1), pp.2604-2612.

Johnston, D.A. and Cooper III, C.D., Level 3 Communications LLC, 2020. System and method for voice security in a telecommunications network. U.S. Patent 10,536,468.

Kapoor, P., Singh, P.K. and Cherukuri, A.K., 2020. Crime Data Set Analysis Using FormalConcept Analysis (FCA): A Survey. In Advances in Data Sciences, Security and Applications (pp. 15-31). Springer, Singapore.

Kesharwani, S., Sarkar, M.P. and Oberoi, S., 2019. Growing Threat of Cyber Crime in Indian Banking Sector. CYBERNOMICS, 1(4), pp.19-22.

Keyser, M., 2017. The Council of Europe Convention on Cybercrime. In Computer Crime (pp.131-170).Routledge.

Khan, A., Wiil, U.K. and Memon, N., 2010,

May. Digital forensics and crime investigation: Legal issues in prosecution at national level. In 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic engineering (pp. 133-140).IEEE.

Kim, S., Chang, Y., Wong, S.F. and Park, M.C., 2020. Customer resistance to churn in a mature mobile telecommunications market. International Journal of Mobile Communications,18(1), pp.41-66.

Kundi, G.M., Nawaz, A., Akhtar, R. and MPhil Student, I.E.R., 2014. Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries.

Journal of Information Engineering and Applications, 4(4), pp.61-71.

Laeseke, P., Schiller, J., Letschert, J. and Llanos, S.D., 2020. Theories, Vectors, and Computer Models: Marine Invasion Science in the Anthropocene. In YOUMARES 9-The Oceans:Our Research, Our Future (pp. 195-209). Springer, Cham.

Lavigne (2008),Mirrorshade Women: Feminism and Cyberpunk at the Turn of the Twenty-first Century, Doctoral dissertation, McGill University, Montreal, Canada.

Marcum, C.D. and Higgins, G.E., 2019. Cybercrime. In Handbook on Crime and Deviance (pp.459-475). Springer, Cham.

McGuire & Dowling (2013), Cyber-crime: A review of the evidence, Summary of key findings and implications, Home Office Research report, 75.

Mittal, S., 2012.A Strategic Roadmap for Prevention of Drug Trafficking through Internet. The Indian Journal of Criminology and Criminalistics (ISSN 09704345), 33(2), pp.86-95.

Moe, J. and Kallin, H., Unwired Planet LLC, 2020. Self configuration and optimization of cell neighbors in wireless telecommunications. U.S. Patent 10,536,883.

Mohamed, S., 2019. Identity Crime in the Digital Age: Malaysian and Mauritanian Legal Frameworks. International Journal of Law, Government, and Communication, 4(15),pp.154-165.

Navneet (2018),Introduction of cybercrime and its types, International Research Journal of Computer Science, 5(8), 435-439.

Nel, W. and Burger, A., 2017.Proving Cybercriminals' Possession of Stolen Credit Card Detailson Compromised POS Devices. In ICMLG 2017 5th International Conference on Management Leadership and Governance (p. 254).Academic Conferences and publishing limited..

Smith, T.D., Barth, M.K., Vongseng, S. and Zimmel, S.C., CommScope Technologies LLC,2020. Telecommunications cabinet with connector storage. U.S. Patent Application16/504,894.

Smith, Cheung & Lau (2015), Introduction: Cybercrime Risks and Responses—Eastern and Western Perspectives, In Cybercrime Risks and Responses (pp. 1-9). London: Palgrave Macmillan.

Solheid, J.J., Conroy, J. W., Mertesdorf, D.R., Holmberg, M., Smith, T.D., Douglas, J.B., Barnes,K.M., Holmquist, M.E., Tinucci, T.C. and Walters, C.S., CommScope Technologies LLC, 2020. Telecommunications connection cabinet. U.S. Patent 10,527,809.

Stefan, P., Traub, J., Hennersperger, C., Esposito, M. and Navab, N., 2020. Challenges in Computer Assisted Interventions: Challenges in design, development, evaluation, and clinical deployment of Computer Assisted Intervention solutions. In Handbook of Medical Image Computing and Computer Assisted Intervention (pp. 979-1012).Academic Press.

Tim, Y., Pan, S.L., Bahri, S. and Fauzi, A., 2017. Digitally enabled crime-fighting communities: Harnessing the boundary spanning competence of social media for

civic engagement. Information & Management, 54(2), pp. 177-188.

Tonellotto, M., 2020. Crime and Victimization in Cyberspace: A Socio-Criminological Approach to Cybercrime. In Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support (pp. 248-264). IGI Global.

Truyens, M. and Van Eecke, P., 2016. Liability of domain name registries: Don't shoot the messenger. Computer law & security review, 32(2), pp.327-344.

Van Baak, C. and Hayes, B.E., 2018. Correlates of cyberstalking victimization and perpetration among college students. Violence and victims, 33(6), pp.1036-1054.

Vertes-Olteanu, A., 2014.Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. JE-Eur. Crim. L., p.84.