Asian Social Studies and
Applied Research (ASSAR)
Published by ASAR Council

Volume 2 Issue 3
August, 2021
ISSN (E): 2709-9229

Critical Analysis of Prevention of Electronic Crimes Act 2016 in Pakistan

IQRA GUL
LLM Scholar, Department of Law
Abdul Wali Khan University Mardan.

ABDUS SAMAD KHAN
Assistant Professor, Department of Law
Abdul Wali Khan University Mardan.
Email: abdus@awkum.edu.pk

SHAISTA NAZNIN
Assistant Professor, Department of Law
Abdul Wali Khan University Mardan.

Abstract

The world lives in a digital age, where the humans' can't imagine to live without the Internet. Technology has become an integral part of our daily lives, and with the significant advancement of technology comes a significant increase in cybercrime. With the introduction of more social media platforms that use millions of data points per second globally, the use of information is growing by the day. These data contain sensitive information such as trade secrets, privacy concerns, and security concerns. The number of electronic crimes is growing by the day, and these cyber crimes can have an impact on an individual, an organization, or even an entire nation. The study intends to investigate various types of electronic crimes occurring in Pakistan and their consequences, authorities working for the implementation of the "Protection of Electronic Crimes Act, 2016" and the steps taken by them in this regard, the role of the "Pakistan Telecommunications Authority" (PTA), and judicial implementation of the "Protection of Electronic Crimes Act, 2016." In addition, the study thoroughly investigates the relevant sections of PECA and provides the best possible solutions and recommendations. Qualitative research was used to study and analyze the impact and challenges caused by cybercrime. For this reason, the interviews with jurists and lawyers, as well as discussions with lawful authorities and members were held to gather the primary data. Finally, the purpose of the "Protection of Electronic Crimes Act, 2016," the powers conferred on the PTA, violations of citizens' constitutional rights, and recommendations to improve the system are discussed.

Key Words: *Electronic Crimes, Cybercrime, Protection of Electronic Crimes Act, 2016.*

Introduction

The world has officially entered the digital age, in which technology is ever-present and pervasive. The advancement of technological innovations makes our daily lives easier. They do, however, make significant contributions to criminality. Cybercrime has become a major issue on a global scale (Benson, 2019). More academics involved in cybercrime prevention and cyber security research are desperately needed (Hollis, 2017). It is also critical to investigate this topic cross-disciplinaryly (Alsayed, 2017). To

understand the impact of cybercrime around the world, we need to look through a variety of lenses, including legal, sociological, and political ones (Jeffries, 2020). The existing literature on cybercrime is primarily from the developed world. Because Asia accounts for half of all internet users, there is a growing need to encourage academics to conduct cyber security and cybercrime research in the Asia Pacific region (Johnston, 2020; Kapoor, 2020).

In academic parlance, there is still no precise and clear definition of cybercrime. It is also known as 'electronic crime,' 'computer crime,' 'computer-related crime,' 'hi-tech crime,' 'technology-enabled crime,' 'e-crime,' or 'cyberspace crime' (Lee, 2019). Aliyu (2018) classified computer crimes into three broad categories based on his research into legislation and common law: crimes in which the computer is used as an instrument of crime, crimes in which the computer is incidental to the offense, and crimes in which the computer is the target of crime. These classifications, while imperfect, help us understand cybercrime. Atlam et al., (2020) advocated a different classification. Using a continuous scale, they classified cybercrime into Type I and Type II offenses. They defined type I cybercrime as crime that is more technical in nature (e.g., hacking), while type II cybercrime is crime that relies more on human contact than technology (e.g. online gambling). However, according to these authors, 'there are likely to be very few events that are purely Type I or Type II; these types represent either end of a continuum' (Chang, 2019). However, advances in artificial intelligence and robotics are rapidly altering the technological landscape. One could argue that these phenomena could give rise to a "Type III" cybercrime perpetrated by self-learning machines.

Hui (2017) also developed a useful classification tool. They classify cybercrime into 'cyber-enabled' crime and 'cyber-dependent' crime. Cyber-enabled crimes are traditional crimes facilitated by the use of computers (Moore, 2014). The range of 'cyber-enabled' crimes is myriad – from white-collar crime, such as fraudulent financial transactions, identity theft, and the theft of electronic information for commercial gain, to drug-trafficking, aberrant voyeuristic activities, harassment, stalking or other threatening behaviors. While these have always been deemed criminal activities, they are now so much easier to pursue with a computer (Kerr, 2018; Keyser, 2017).

Cybercrime is the world's biggest industry when it comes to criminal growth (Öztürk, 2020). Any criminal activity that involves a computer, networked device, or a network is termed a cybercrime (Payn, 2018). Some cybercrimes are performed to create profit for cybercriminals; some cybercrimes are perpetrated directly against computers to harm or disable them, whereas others are using computers or networks to spread malware, illicit information, photos, or other content (Saunders, 2017). The world is seeing an escalation in cybercrimes year by year, both in size and sophistication as the technology is advancing rapidly, and there is a huge need to surmount the challenges that are imposed because of these crimes (Herjavec, 2020; Tonellotto, 2020). The paper presents the details of these crimes' impact and challenges and discusses suggestions to the challenges.

Electronic crimes are taking place worldwide and all the countries are focused on the control of these crimes due to the sensitive nature and rapidly growing rateof these crimes because it is an era of technology and these crimes have the potential of disturbing peace in social lives of the citizens as well it can become a threat to the national security as well. In this regard Pakistan has also enacted laws for the control of electronic crimes. The study mainly focuses on the crimes taking place in Pakistan and their control in the light of laws prevailing in the region.

Objectives of the study

i. To examine the "Prevention of Electronic Crimes Act (PECA) 2016," identify flaws, and make recommendations to the relevant authorities for effective judicial implementation of "PECA, 2016."
ii. ii. My research on this topic is also important because cybercrime is on the rise, with daily reports of electronic crimes disrupting social balance. They endanger society because anyone can be a victim, and computer criminals are constantly attempting to breach security and obtain personal information from individuals for monetary gain.

Research Objectives

i. What are electronic crimes and who are their victims?
ii. What are the laws related to electronic crimes in Pakistan?
iii. What are the international laws for PECA?
iv. What is the reliability of PECA (2016) is efficient enough to deal with electronic crimes?
v. What is the reason behind controversial status of PECA?
vi. What is the role of PTA and powers extended to it by PECA?
vii. What is the aim of PECA and who are the targets?
viii. What are the rudimentary measures that must be taken to improve the existing PECA?

Methodology

The current study is qualitative (using words and phrases) rather than quantitative (using numeric digits) in nature (Strauss and Corbin, 1998). So, this study will be qualitative. Interviews with jurors and lawyers will provide primary data. Secondary sources include Islamic jurisprudence and law books, articles, court decisions, internet searches, and immanent juries' commentaries. Although little research has been done on the PECA, all articles and books related to our study will be sorted out to gain the maximum knowledge to solve the mystery our research plan. Content of the data is in the form of text, as the objects of the study are Interviews and research articles, Books and laws

Primary data source consists of the interviews and detailed discussions by;

i. Interviews with jurist and lawyers
ii. Discussion with lawful authorities and members

Secondary Data

Articles and other publications related to our study that depict the idea of PECA are secondary data sources. The secondary data source will also include other research papers that have reviewed the PECA. Our secondary data sources will include various library works, internet webs, and personal note books. All relevant books and articles will be read several times to grasp the authors' theme. In addition, we will use the library and note-taking to gather information to solve our study's mystery. Various articles that clearly depict our research study will also be read and used for data collection. It helps in collecting and presenting data efficiently.

Literature Review

International Laws of Electronic Crimes

Cybercrime has sparked national and international outrage. Less capita involvement, indistinct approach for demonstrating it is illegal (Hashmi et al., 2016; Hollis, 2017). As a result of the above situation, legislative authorities must deal with and enact strict laws to stop such criminal activities.

G8

G8 consists of eight industrialized nations' leaders: USA, UK, Russia, France, Italy, Japan, Germany and Canada. To combat cybercrime and protect data and systems, the G8 issued a Ministers' Communiqué in 1997. All law enforcement personnel must be trained and equipped to deal with cybercrime, and a point of contact must be available 24/7.

United Nations

In 1990, the UN General Assembly passed a resolution on computer crime. In 2000, the UN General Assembly passed a resolution to combat cybercrime. In 2002, the UN General Assembly passed a second resolution on e-crime.

ITU

The International Telecommunication Union (ITU) is a specialized agency of the United Nations that works on telecommunications and cybersecurity issues. The World Summit on the Information Society was organized by the ITU (WSIS). It was published in 2003, along with the Geneva Declaration and Geneva Plan of Action. On the Internet Society Commitment and Agenda were adopted in 2005.

Council of Europe

The Council of Europe is a 47-nation international organization dedicated to advancing human rights and democracy. The first international cybercrime convention, the Convention on Cybercrime, was drafted by the Council of Europe in 2001 and signed by its 46 members. But only 25 countries ratified it later. [8] That includes harmonizing cybercrime classification, empowering law enforcement, and facilitating international cooperation.

Asia-Pacific Economic Cooperation (APEC)

APEC is an international forum promoting free trade and practical economic cooperation in the Asia-Pacific region. APEC published a Cybersecurity Strategy in 2002, which was included in the Shanghai Declaration. • Legal developments; • Information sharing; • Security and technical guidelines; • Public awareness; • Education.

OECD

The OECD is a 34-country international economic organization founded in 1961 to promote economic development and global trade. The ICCP Committee established an Expert Group in 1990 to draft

information security guidelines, which were finalized in 1992 and adopted by the OECD Council. A Security Culture: Guidelines for the Security of Information Systems and Networks, OECD, 2002.

European Union

Improving Information Infrastructure Security and Combating Computer-Related Crime was the title of a 2001 European Commission communication. In 2002, the EU proposed a "Framework Decision on Cyber Attacks." However, the Framework Decision focuses on harmonizing substantive criminal law provisions aimed at protecting infrastructure elements.

Commonwealth

The Commonwealth of Nations published a model law on cybercrime in 2002 to help harmonise legislation and foster international cooperation. The model law was written to comply with the Cybercrime Convention.

ECOWAS

The Economic Community of West African States (ECOWAS) was founded in 1975. Since its adoption in 2009, ECOWAS has established a legal framework for member states that includes both substantive and procedural criminal law.

GCC

At a 2007 conference, the Arab League and the GCC recommended a joint approach that takes international standards into account.

Electronic Laws in Pakistan

As previously stated, cybercrime is the most dangerous type of crime, or we can say it is the modernized form of criminal activity, requiring extensive experience and tactics in the field of electronics and computers. It is the government's duty to keep society free of criminals. In order to achieve this, laws must be enacted that require criminals to be prosecuted (Khan and Daniyal, 2018). While electronic/cybercrimes have existed for many years, due to their sensitive and technical nature, laws relating to counter-cybercrime have only recently been enacted, and various governments in various countries have formed technical teams (Greer, 2017; Haq, 2019). While laws have been enacted to keep up with the advancement of new technologies and electronic devices, the same need to be illuminated for further improvements (Kesharwani et al., 2019; Kapoor et al., 2020).

Electronic Laws of 2002 and 2007

Governments are working to improve their citizens' and lands' privacy (Demetis, 2019). Ensuring certificate security for service providers was made possible by the 2002 "Electronic Transactions Ordinance" (Johnston and Cooper, 2020). It was the government's first attempt to modernize and control electronic crimes in the country until the "Prevention of Electronic Crimes Act" was passed. An increase in electronic crimes prompted President Obama to issue the "Prevention of Electronic Crimes Ordinance, 2007", (Burnes et al., 2020). Finding a precise solution requires first identifying an entity's role (Billah, 2018). These cases provide an indication of Pakistan's cybercrime rate. A report on cyber crime in Pakistan shows 1290 reported inquiries, 207 cases, and 160 arrests in 2017 and 2295 in 2018. (Ahmed, 2020).

Prevention of Electronic Crimes Act, 2016

This new law criminalizes speech and gives authorities' unchecked power to restrict and prosecute (Turban et al., 2018). As a result of the 2014 terrorist attack on Peshawar's Army Public School, the government's 12-point "National Action Plan" justified these sections (Sunhare and Shaikh, 2019).

Pakistan Telecommunication Authority (PTA)

Previously, the PTA launched a campaign against unregistered phones in Pakistan, sending text messages to all sim card holders (Shakir, 2015). This year, PTA has focused on blasphemy and other cybercrimes. Unauthorized electronic media use was also required to be reported via text message (Saleem Ullah , 2019). Section 37 of the PECA allows the PTA to block/remove online content, limiting Article 19's right to free expression. The PTA has a history of censorship and platform blocking (Riaz and Amjad, 2019). Article 19 is enforced by the government authority receiving directives from the Ministry of Information Technology and Telecommunications (ztürk et al., 2020). PTA now has legislative and judicial authority (Patil et al., 2020).

Analysis of PECA 2016

The "Prevention of Electronic Crimes Act, 2016" is not Pakistan's first electronic law. Between 2002 and 2007, the country enacted laws to combat online threats to the public and the land, but they were never approved by parliament (Isaac, 2019). The "Prevention of Electronic Crimes Act, 2016" was signed into law on August 18, 2016, but it drew a lot of criticism for severely restricting citizens' rights to expression and privacy (Hasinoff and Krueger, 2020). The country requires a strong electronic law, but the general public's rights must be considered so that the law does not infringe on citizens' constitutional rights (Moe and Kallin, 2020). A law to prevent electronic crimes was passed in Pakistan on August 11, 2016. It is, in my opinion, one of the most hotly debated laws in the country's history (Dadkhah et al., 2018). In PECA, the authors tried to keep the legislative process secret and avoided consultations at every stage.

Intervention with Fundamental Rights

Article 4 of the Constitution guarantees equal treatment for all citizens (Beshears, 2019; Atlam et al., 2020). It means that if a citizen's fundamental or constitutional rights are violated, there must be a legal basis for the violation. Similarly, Pakistan's Article 10-A guarantees citizens a fair trial, but only for criminal charges (Al Mutawa et al., 2016). The judiciary is regarded as the constitution's savior or guardian. The doctrine of due process was first discussed in the case of Begum Shorish Kashmiri (Tsukahara et al., 2019;). The court debated the definition of "law" and confirmed that everyone has a constitutional/basic right to be tried fairly. The term "law" was used broadly to refer to anything that should be consistent with the judicial principles established by the superior courts (Sueishi et al., 2017). This means that Article 2 of the 1962 constitution should be interpreted "according to accepted forms of legal process," and thus "as comprehensive as the American due process clause" (Shadmanfaat et al., 2019). In this case, due process was expanded from procedural to substantive. Thus, due process protections in Pakistan ensure adherence to the ethical spirit of the law, which means a law must uphold citizens' liberties and rights (Saragih and Siahaan, 2016).

Threat to Privacy of Citizens

In light of section 31, 32, and 42 under PECA, 2016 a similar set of provisions in PECA are intended to give government agencies access to citizens' private data or prevent citizens from accessing government data (Mittal and Sharma, 2017). Non-authorized access to any information system and/or data is a crime under many provisions of the PECA. The "Pakistan Telecommunications Authority" (PTA) and other law enforcement agencies are granted access to citizens' private data while citizens' access to government data is restricted (Khalid, 2019). The Act allows ISPs to retain data, sell data to foreign entities, and force citizens to hand over personal information.

Freedom of Speech

PECA has faced a lot of criticism for violating the fundamental rights of freedom of speech under Article 19 of the Constitution. Freedom of speech and press are fundamental rights that signify the cornerstones of democratic institutions (Gürkaynak et al., 2013; Harrigan, 2017). However, such freedom as per section 37 under PECA, 2016 is subject to reasonable restrictions that may be imposed by law. While, there can be no absolute test for reasonableness of restrictions imposed by law, as a general rule of thumb, it is for the courts to decide whether, under the given circumstances, a restriction is reasonable or not.

Conclusion

To summarize, the current era is highly technological, resulting in massive data exchange. People's lives have been made easier thanks to online marketing, banking and transactions, but online criminals have compromised people's privacy. Many small and large businesses do not know how to properly protect sensitive data, allowing criminals to invade their privacy and steal personal information. A wide range of crimes can be committed using computers, including white-collar, violent (murder and terrorism), counterintelligence (espionage), counterfeiting, and drug trafficking. For example, the average bank robbery netted $6,900, while computer crimes netted $900,000. The Internet has made it much easier for criminals to access their targets, with much lower risks than traditional crimes. One can hack into a bank or company website from anywhere and transfer millions of dollars to a fictitious account, effectively robbing the bank without risking being shot while fleeing. Recognizing the sensitivity of electronic crimes, many countries have developed laws to protect their citizens. The main goal of the Act is not being met due to gaps in the Act's provisions, and there is still much to be added in the Act's provisions for more efficient working and judicial implementation, which has been heavily criticized due to its diverted drafting.

Recommendations

Introducing Biometric System for Sim Cards

SIM cards in Pakistan are now biometric. After biometric verification of the customer, the PTA has issued strict instructions to service providers. Through a digital device, this system connects to the NADRA, which confirms the thumb impression of the person requesting the sim card issuance (Mittal and Sharma, 2017; Mills et al., 2019). This feature was added to help prevent identity theft and fraudulent SIM card use. It used to be that criminals would buy SIM cards with made-up names and addresses, making it difficult for authorities to track down the real culprits (Kundi et al., 2014; Khalid, 2019; Kumari, 2020). Sim cards will not be issued to anyone with a fake identity or no biometrics after the new rules come into effect. A customer's sim card can only be accessed by the user if it is destroyed or lost (Isaac, 2019; Kashyap and Kalyan, 2019; Kapoor et al., 2020).

Registration of Mobile Phones

The issue was that mobile phone sellers used to import mobile phones in bulk from various countries and bring them into the country without going through any registration process (Alsayed and Bilgrami, 2017; Todd, 2018). It was difficult for authorities to track and find out the mobile phone used during a criminal activity without registering the IMEI numbers of the cell phones, so the PTA began blocking unregistered mobile devices and issued new directions for registration of mobile phones at the airport, which also helped in generating taxes (Daley et al., 2016; Smith et al., 2020; Solheid et al., 2020).

Screening Data of Social Media Apps

Due to the new policies on sim card issuance and registration, cyber criminals found it increasingly difficult to hide and carry on their previous activities. So they started using WhatsApp and other social media apps for group chats, exploiting another social media flaw (Turban et al., 2018; Tsakalidis et al., 2019). PTA began monitoring and screening social media data to learn more about criminals and their activities. The public believes that such screening of social media data compromises user privacy and makes everything available to agencies and authorities (Vayansky and Kumar, 2018). The general public has no privacy, and whatever they share with their loved ones is screened, in violation of the Constitution's right to privacy. Another aspect is that the music will not be faced by a single person or group, but by all citizens (Benson et al., 2019).

Online Complaints System

PTA has implemented an online complaint system that allows users to report issues via the internet or mobile phones. This system is intended to make it easy for citizens, especially women, to report harassment, blackmail, and other issues (Saragih and Siahaan, 2016; Kapoor et al., 2020). Complaints about blasphemy, obnoxious calls, and other issues can also be made online (PTA). Due to the fear of being caught, blackmailers and obnoxious callers have decreased (Singh and Singh, 2017; Tsukahara, 2019). Women feel safer using social media and other electronic media than in the past.

References

Ahmed, S. R. (2020). *Preventing Identity Crime: Identity Theft and Identity Fraud: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity Crime*. BRILL.

Al Mutawa, N., Bryce, J., Franqueira, V. N., & Marrington, A. (2016). Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis. *Digital investigation*, *16*, S96-S103.

Aliyu, U.L., 2018. Computer Crime. Editorial Board, p.28.

Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *Int. J. Of Emerg. Techn. and Adv. Activ*, *7*(1), 109-115.

Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. (2020). Security, cybercrime and digital forensics for IoT. In *Principles of internet of things (IoT) ecosystem: Insight paradigm* (pp. 551-577). Springer, Cham.

Beshears, M. L. (2017). Effectiveness of police social media use. *American Journal of Criminal Justice*, *42*(3), 489-501.

Billah, M. M. (2018). Sufficiency of Omani Laws to Suppress Cybercrimes in Light of the un Comprehensive Study on Cybercrimes. *Arab Law Quarterly*, *32*(2), 158-184.

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive medicine reports*, *17*, 101058.

Chang, L. Y. C. (2019). Criminological perspectives on cybercrime: risk, routine activity, and cybercrime. In *Research Handbook on Transnational Crime*. Edward Elgar Publishing.

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

Darian-Smith, K. (2020). Children, comforts and intercultural exchanges for Australians in both world wars. *Cultural and Social History*, *17*(5), 697-713.

Demetis, D. S. (2020). Breaking bad online: A synthesis of the darker sides of social networking sites. *European Management Journal*, *38*(1), 33-44.

Greer, B. (2017). The Growth of Cybercrime in the United States. *Growth*.

Gürkaynak, G., Yılmaz, İ., & Durlu, D. (2013). Understanding search engines: A legal perspective on liability in the Internet law vista. *Computer Law & Security Review*, *29*(1), 40-47.

Haq, U., & Atta, Q. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network & Information Security*, *11*(1).

Harrigan, M. (2017). Privacy Versus Justice: Amazon's First Amendment Battle in the Cloud. *W. St. UL Rev.*, *45*, 91.

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

Hasinoff, A. A., & Krueger, P. M. (2020). Warning: Notifications about crime on campus may have unwanted effects. *International Journal of Communication*, *14*, 21.

Hollis, M. E., Downey, S., Del Carmen, A., & 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), 46-60.

Haggag, O., Haggag, S., Grundy, J., & Abdelrazek, M. (2021, May). COVID-19 vs Social Media Apps: Does Privacy Really Matter?. In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)* (pp. 48-57). IEEE.

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

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

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

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., & Cherukuri, A. K. (2020). Crime data set analysis using formal concept analysis (FCA): A survey. *Advances in Data Sciences, Security and Applications*, 15-31.

Kashyap, S. and Kalyan, V., 2019. Cyber Crimes against Women in India and its Prevention. *Journal of the Gujarat Research Society*, 21(1), pp.127-129.

Kerr, O. S. (2018). Computer Crime Law (Introduction). *Computer Crime Law (4th Ed. 2018), West Academic Publishing*.

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

Keyser, M. (2002). The council of Europe convention on cybercrime. *J. Transnat'l L. & Pol'y*, *12*, 287.

Khalid, A. U. (2019). A Case Study of Pakistani News Channels: Media Education and Journalists' Training. In *Smart Technologies and Innovation for a Sustainable Future* (pp. 1-9). Springer, Cham.

Khan, D., & Daniyal, M. (2018). Cyber Bullying in Pakistan: Statistical, Legislative, and Social Analysis.

Kundi, G. M., Nawaz, A., Akhtar, R., & 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), 61-71.

Lee, H., & Lim, H. (2019). Awareness and perception of cybercrimes and cybercriminals. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(1), 1-3.

Mills, C. E., Freilich, J. D., Chermak, S. M., Holt, T. J., & LaFree, G. (2021). Social learning and social control in the off-and online pathways to hate crime and terrorist violence. *Studies in Conflict & Terrorism*, *44*(9), 701-729.

Mittal, S., & Sharma, P. (2017). A review of international legal framework to combat cybercrime. *International Journal of Advanced Research in Computer Science, ISSN*, (0976-5697).

Mohammed, A. M., Benson, V., & Saridakis, G. (2020). Understanding the relationship between cybercrime and human behavior through criminological theories and social networking sites. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 979-989). IGI Global.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Öztürk, Z., Pekkaya, M., & Temli, M. (2020). Evaluation of Cybercrime Economy via MCDM and Decision Tree Approaches: The Case of Zonguldak. In *Digital Business Strategies in Blockchain Ecosystems* (pp. 521-554). Springer, Cham.

Patil, A. P., Nawal, D. J., & Jain, D. (2020). Crime prediction application using artificial intelligence. In *Proceedings of ICETIT 2019* (pp. 238-245). Springer, Cham.

Payne, B. K. (2018). White-collar cybercrime: White-collar crime, cybercrime, or both. *Criminology, Crim. Just. L & Soc'y*, *19*, 16.

Riaz, N., & Amjad, S. (2019). The Status of Restorative Justice in Pakistani Legal System: An Analysis of Pakistani Laws With Special Reference to Certain Case Studies. *Restorative Justice in Pakistan*.

Siahaan, A. P. U. (2018). Impact of Cybercrime on Technological and Financial Developments.

Saunders, J. (2017). Tackling cybercrime–the uk response. *Journal of Cyber Policy*, *2*(1), 4-15.

Shakir, N. (2015). Islamic shariah and blasphemy laws in Pakistan. *The Round Table*, *104*(3), 307-317.

Singh, A., & Singh, A. (2017). Review of Cyber Threats in Social Networking Websites. *International Journal of Advanced Research in Computer Science*, *8*(5).

Sueishi, T., Yucel, M., Ashie, Y., Varquez, A. C. G., Inagaki, A., Darmanto, N. S., ... & Kanda, M. (2017, December). Investigation of Future Thermal Comforts in a Tropical Megacity Using Coupling of Energy Balance Model and Large Eddy Simulation. In *AGU Fall Meeting Abstracts* (Vol. 2017, pp. GC21G-1025).

Todd, D. (2018). *The world electronics industry*. Routledge.

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.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security*, *83*, 22-37.

Tsukahara, T. (2019). Legacies and Networking: Japanese STS in Transformation. *East Asian Science, Technology and Society*, *13*(1), 143-149.

Turban, E., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2015). E-Commerce security and fraud Issues and protections. In *Electronic Commerce* (pp. 457-518). Springer, Cham.

Zamir, A., Khan, H. U., Iqbal, T., Yousaf, N., Aslam, F., Anjum, A., & Hamdani, M. (2020). Phishing web site detection using diverse machine learning algorithms. *The Electronic Library*.