Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.4, 2014
www.iiste.org

Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries

Ghulam Muhammad Kundi, PhD
Allah Nawaz, PhD
Department of Public Administration, Gomal University
DIKhan, Khyber Pakhtunkhwa, Pakistan
E-mail: kundi@gu.edu.pk

Robina Akhtar
MPhil Student, IER, Gomal University
DIKhan, Khyber Pakhtunkhwa, Pakistan
E-mail: alishba.daali@gmail.com

Abstract
Cyber-crimes the off-spring of cyber-space technology could be only monitored; controlled and prevented through cyber-legislation. Countries around the globe are facing the dangers of cyber-crimes due to several reasons ranging from the poor technology, incapacity and absence of legislation to financial constraints, lack of cooperation with international law and enforcing agencies. This study was undertaken to asses and analyzes the present state of cyber-crimes and legislation in the perspective of developing countries and to identify and analyze the challenges the governments of developing countries are facing in prevention of the cyber-crimes in general and focusing Pakistan being developing economy in particular and to suggest way-out. This qualitative study used ATLAS.ti software for data analyses. Hermeneutics, discourse and heuristic methods were employed to analyze the qualitative data. Experts suggested the use of different approaches for cyber-legislation for example the minimalist approach and prescriptive approach. However, this study proposes the use of two-tier approach for cyber-legislation against the cyber-crimes in developing countries and Pakistan.
Key Words: Cyber-space, Cyber-crimes, Cyber-laws, Minimalist approach, Prescriptive approach, Two-Tier approach.

1. INTRODUCTION

The computer and information systems have revolutionized the service mechanism around the globe. The services offered to individual and community manually are disappearing in favor of online services with the use of computer and internet technology (Lehman, 2000). E-Learning, E-Commerce, E-Business, E-Baking and now E-Government have changed the traditional modes of business into virtual world i.e. face to face without being face to face (Kundi, 2010). Innovation, differentiation in cost and growth, alliance, mergers are the present day features of the organizations, has been possible because of the digital revolution (Kundi et al. 2012). However, as we cannot count the numerous blessings it offer by the same coin we cannot afford the dangers associated with the use of this digital technology e.g. technical and social, yet the biggest and severe one, the developing countries are facing with is the issue of cyber security against the cybercrimes. Which is still shaking the trust and confidence of online community, this is why the pace and growth of going online is still very slow and humble in the developing countries as compared to curiosity and zest for being online (Kundi, 2010; Kundi et al., 2008).

According to Parker (1998), cyber-crime is a major concern for the global community as the introduction, growth, and utilization of information and communication technologies have increased the criminal activities. Cybercrime is an obvious form of international crime that has been affected by the global revolution in ICTs (Barr & Pease, 1990). Cybercrimes differ from terrestrial crimes in four ways that they are easy to learn how to commit, they require few resources relative to the potential damage caused, they can be committed in a jurisdiction without being physically present in it, and they are often not clearly illegal (Levi, 1998). On such a basis, the new forms of cybercrime present new challenges to lawmakers, law enforcement agencies, and international institutions (Madhava & Umarhathab, 2011). This necessitates the existence of an effective supra-national as well as domestic mechanisms that monitor the utilization of ICTs for criminal activities in cyberspace.

Pakistan has been making efforts to digitize not only public sector rather several initiated have been undertaken to facilitate the digital boom in the private sector too. IT-policy was introduced to create digital culture in the society besides broad-band policy. The internet connectivity and speed has been doubled in the recent past.

Recently government called upon bids for 3G and 4G technology, which is expected to bring revolution in the telecommunication sector. Moreover, huge funds are being provided to public sector organizations for computerization and networking. E-Government, eBanking and eLearning is mushrooming in the country. However, no proper legislation is made to prevent the electronic/cyber-crimes to protect the users from eFrauds etc., which is a major barrier towards trust and confidence of the users. Though, the Pakistan Electronic Crimes Ordinance (2002) modified (2008) were promulgated, however these lapsed after six weeks under the constitution of 1973. Moreover, Pakistan Electronic Crimes Act (2007) and now Pakistan Electronic Crimes Act (2014) have been initiated as draft law but still waiting to become law, thus in the absence of cyber-law, cyber criminals are enjoying to play with online community, who are easily falling their victims, losing not only their privacy, data and money but also in some cases, damage to their social and family life (Magalla, 2013).

This study is aimed to identify and analyze the challenges the governments of developing countries are facing in prevention of the cyber-crimes in general and focusing Pakistan being developing economy in particular and to suggest way-out.

2. REVIEW OF THE EXISTING LITERARURE

This section deals with the review of the existing sources of the research, which provides strong foundations for the subsequent analyses and interpretation of the results of the study.

2.1 What is Cyber-Crime?

The term Cyberspace was first used by William Gibson in his 1984 novel "Neuromancer", which is now used to describe the entire spectrum of computer networks and associated activities that take place over computers and their interconnected networks which is their largest manifestation form the internet (Jamil, 2006). So it is the virtual place without jurisdictional boundaries in which people interacts through network of hundreds of thousands if not millions of computers and users at the same time, thus, this cyber-space paved ways for cyber-crimes (Marvin, 1988).

While, according to Halder & Jaishankar (2011) cyber-crimes are the offences which are committed by individual and groups against the individuals, groups and organizations having criminal motives to intentionally damage i.e. physical or mental harm to the victim directly or indirectly, who uses telecommunication networks like, chat rooms, emails, notice boards and groups and mobile phones for SMS/MMS. Computer crime or cyber-crime can be grouped into, first, computer as a target, attacking other computer through infecting viruses & spreading malware, etc. second, computer as a weapon, by using computer to commit traditional crime i.e. fraud or illegal gambling and third, computer as an accessory, simply use of a computer to store illegal or stolen information or data (Mativat & Tremblay, 1997). However, there is no agreement on the internationally agreed upon single definition of cyber-crime (Collin, 1996). Yet, generally, it could be refer to an illegally internet-mediated activity that often take place in global electronic networks, may be domestic or international or transnational – without cyber borders. Moreover, international cyber-crimes are great challenge to domestic and international law and its effective implementation, as in many countries, the current legislation is not tailored to deal with cybercrime, thus criminals are increasingly conducting crimes through internet by taking benefits of the poor punishments or difficulties in tracing the criminal. So, computer crime implies any crime that involves a computer and a network or criminal exploitation of the internet.

Whereas, cyber-crime is the criminal activity, the source of which is a computer or computer network used for cyber-attacks and may include fraud, theft, blackmail, forgery and embezzlement, however due to virtual mode, it is notoriously difficult to detect and punish because technical complexity and unseen attackers sitting thousands of miles away. Though new technology is handy, dynamic and evolving, and each next spell bring into face new technology with advance features and security mechanism but due to the nature of cyber-crime, and its ability to evolve with technology, new threats are emerging with an alarming degree of regularity and the user's ability to co-op with become more challenging, which may also threaten a nation's security and financial health.

The issues emerge from such crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. These are also called the problems of privacy when hackers/ attackers attack the confidential information to make intentional distortions, steal and intercept lawfully or otherwise. Though international legal system is there which attempts to hold actors accountable for

criminal acts through International Criminal Court (ICC), however, lack of coordination or incompatibility of local laws with international laws become a barriers towards their fruits.

2.2 How and Why Does It Affect?

A research survey found that about 83% of the small businesses were the victims of cyber-crimes in 2010 with average cost of £27,000 - £55,000 (Price Water House Coopers Information Security Breaches Survey, 2010), whereas, in Wales, alone it was estimated more than £974m a year in the shape of financial loss, interruption of business, theft of valuable data, identity theft and deception due to unauthorized access to computer systems (New South Wales Independent Commission against Corruption, 1999) .
With this context, the security systems of the majority of the present day business organizations are based on the conventional, off-the-shelf anti-virus and firewall solutions, which does not provides them sufficient security and protection against the online threats despite the fact that thousands of businesses every year still becoming victim to cyber-crime (Parker, 1998) . Thus, it is observed and research studies time and again found the cyber-crimes on the rise with more sophisticated and creative ways to breach IT security, this means that simply relying on the existing IT security measures, if any, one not provide security from the breed of new hackers, scammers and virus designers who easily break the traditional security measures easily.

So why does it affect us is a million dollars question? Good, any organization which is using computer is now at risk, if their computers or other electronic device are connected to internet, using online systems, and this risk will be even greater, which is known to the criminal too. So the information on IT system of an organization is extremely valuable, which needs every possible precaution to be taken to protect it become necessity rather than luxury. Thus, the protection of the business and users from the electronic threats may does not cost more than its benefits which may spend on locks and alarms for your computers, so wise does not the take the risk.

2.3 Global Perspective on Cyber-Crimes

Online communication has become the norm in the digital age (R.S, 2007), whereas, the internet users and governments are facing the increased risks of becoming victims of cyber-attacks (Rasch, 1996). The cyber criminals are continuously developing the advance techniques by shifting their targets, mainly focusing less on theft of financial information and more on business espionage and accessing government information. In the context of fast-spreading cyber-crimes, governments in developing countries need to collaborate globally so that an effective model could be developed to control the threats.

Because of the development and advancements in computer and telecommunication technology, the developing countries are able to develop and expand their communication networks by enabling them with faster and easier networking and information exchange. With this, the cyber-crimes have been increased in couple of past years world-wide, which has changed the scenario dramatically, now criminals are using more sophisticated gadgets to break the cyber security. Moreover, recently malware, spam emails, hacking into corporate sites and other attacks of this nature is the work of computer ‘geniuses’ evident on their talent. These rarely malicious attacks have gradually evolved into cyber-crime syndicates siphoning off money through illegal cyber channels.

According to estimates, currently, about 2 billion internet and 5 billion mobile phone users are connected round the globe. About 294 billion emails and 5 billion phone messages are exchanged every day (Commonwealth Secretariat, 2002). The convenience of digital networks, however, come at a cost as business organizations in particular and societies in general are increasingly relying on the computers and internet-based networking, thus cyber-crime and digital attacks have increased manifold throughout the world. The attacks are categorized into financial scams, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred (Herhalt, 2011).
The basic and fore most steps towards protection is the better understanding of different kinds of threats which are being faced by the business community and online users. Below are the most common cyber-crimes which might influence the decision about the electronic security. The common cyber-crimes include, advance fee fraud, botnets explained, denial of service (DoS) and Distributed Denial of Service (DDoS), Domain name renewal scams, fake Ads, Hacktivism, Theft of Laptop or other hardware, Identity theft, IP theft, copying of information, phishing, scareware, social media, spam, spyware, Unsecured Wireless Local Area Networks (WLANs) and Virus attacks (KPMG, 2013).

The first major incident of the cyber-crime occurred in 2000, when approximately 45 million computer users worldwide were affected by a mass-mailed computer virus. Likewise, politically motivated cyber-crime had

penetrated global cyberspace (Herhalt, 2011). Experts are of the view that some government agencies may also be using cyber-attacks instead of armed war as a new mean of warfare, and such was reported in 2010, when Stuxnet (a computer virus) was used to carry out an invisible attack on Iran's nuclear program, which was to disable Iran's uranium enrichment centrifuges. Carders Stealing Bank, which is also known as credit card details, is also a major cyber-crime, in which duplicate cards are used to withdraw cash from ATMs or in shops (Chapman & Smith, 2001).

Keeping in view the international nature of cyber-crime, it may occurs not only in the regions from where it originate rather involve other countries or regions too. Therefore, cyber-crime needs not only highly responsive but also an internationally coordinated control measures. Likewise, the investigation and reporting mechanism for these crimes must be resource-intensive. To protect and restore cyber infrastructure, the cost of the businesses have increased rapidly, for example, UK's annual cost resulting from cyber-crime is estimated at GBP27 billion equal to US$43 billion respectively GBP9.2 billion for intellectual property (IP) theft, GBP7 billion (US$11 million) for espionage activities. Similarly, in Germany, phishing brings about 70% estimated cost year-over-year in 2010, resulting in a loss of EUR17 million (US$22 million) as reported by German IT Trade Group 'Bitkom' and the German Federal Criminal Police Office, besides, the indirect costs which is also associated with cyber-crime, occurs due to reputational damage to organizations and loss of confidence of the online users in cyber transactions (Herhalt, 2011; Council of Europe, 2003).

2.4 Cyber-Crimes: Challenges for Governments in Developing Countries

Although governments of the developed as well as developing countries are seen determined and actively focusing on fighting and preventing cyber criminals to prevent them from the damage of their cyber infrastructure, yet, the very nature of cyberspace shams multiple challenges in implementing the cyber regulations in these countries, as it is not easy to define and determine the political borders and culprits in cyber space. Moreover, cyber-criminals and their techniques are unceasingly changing, that make it more difficult rather challenging for governments and businesses to keep up with ever-changing techniques used by cyber-criminals.

According to Rob Wainwright, Director of Europol, Criminal Investigations of Cyber-Crimes, identifying and tracking the origin of crime is not only complex but sometime impossible due to its borderless nature, which is one of the great challenges for the developing world, who are already technology deficient (Council of Europe, 2003). Likewise, several experts wonder that the cyber-attacks and cyber-crimes are lucrative venture. In the cyber-world, the hackers commit organized crime by selling confidential stolen intelligence. According to a research, criminals are trading bank account information for US$10–125, credit card data for up to US$30 per card, and email account data for up to US$12.85 (Ghauri, 2014). The acquired data is often used for illegal online purchases and exchange of other monetary transactions. Thus, un-traceability of the origin of these transactions is a great challenge to governmental agencies.

To implement the cyber security measure, sufficient number of skilled manpower is required, while, the second issue in developing countries is the scarcity of the skilled cyber-crime fighters, as most of the developing countries are facing with the shortage of skilled people to counter cyber-attacks. According to Ronald Oble, the Head of Interpol, "an effective cyber-attack does not require an army; it needs just one individual. However, there is a severe shortage of skills and expertise to fight this type of crime; not only at Interpol, but in law enforcement everywhere" (Grabosky & Smith, 1998).

Lack of eForensic skills and expertise is another core issue remains unsolved over a long period besides widespread use of pirated software to prevent cyber-crime. Due to frequent use of pirated software, which is more prone to attacks by viruses, malware and Trojans, the control of cyber-crimes becomes more challenging and difficult. Experts believe that the rapid growth of consumer PC markets in developing countries, like India, Brazil, China, Malaysia and Pakistan have been contributing more to the rising piracy rates (Herhalt, 2011). China has spent US$19 on pirated software in 2009, whereas, India stands nearly at US$ 2billion on the unlicensed software market value (Herhalt, 2011)). Similarly, ensuring cyber security is a major challenge for Gulf Cooperation Council (GCC) countries, where 50% of software is pirated, moreover, about 70% software installed by users are pirated (Ghauri, 2014) .

2.5 Cyber-Crime Issues and Legislation: Pakistani Context

Cyber-crime is the one of the biggest issues round the world, as almost all countries, including developed and developing countries are fighting against the threats posed by cyber-crimes with extreme legal measures. They have enacted legislation to tackle cyber criminals. However, developing countries and Pakistan in particular are among the few unfortunate where cyber-crime laws are still in the infancy. It is certainly not as if we do not face that many cyber-crimes here; in fact, currently, Pakistan is also facing the cyber-crimes i.e. financial crimes in online transfer of funds, cyber pornography, sale of illegal articles, online gambling, intellectual property crimes, e-mail spoofing, cyber stalking, forgery, unauthorized access to computer systems networks, theft of information contained in electronic form, virus/worm attacks, logic bombs, trojan attacks, internet time theft, password cracking and buffer overflow etc. According the officials dealing with these, only 15 to 20 cases were registered in the year 2013 regarding cyber-crimes mostly filed by the women. Data on the latest cyber-crimes in Pakistan reports that software piracy costs over $315b annually (Pakistan Observer). While anti-malware war cost $500bn in 2014 alone (The News International, 2014).

Pakistan is one of the leading countries in cyber-crime, though Pakistan has a long list of laws to prevent cyber-crimes. According to a survey almost 10-15 cases are registered every day which may start from hacking an account to dangerous results like illegal and unauthorized fund transfer and withdrawal from customer's bank accounts.
It is evident from the above facts that cyber-crimes in Pakistan are rapidly growing with the exponential growth in usage of mobile phones and penetration of internet (Kundi et al., 2008). It has been found that these criminal uses advanced technology to commit these crimes (financial matters, information stealing and at times even in terrorism). Inorder to prevent and counter these criminals, Pakistan established the National Response Center for Cyber Crime (NR3C) to monitor, track and catch the cyber-criminals. NR3C is providing single point of contact for all local and foreign organizations for cyber-crimes in Pakistan. It is also imparting training and related security education to government /semi-government and private sector organizations besides holding seminars and workshops to educate the users against cyber-attacks on their information resources, information breech and to make their systems secure against all such threats (Jamil, 2006).

The first law however in Pakistan to control and prevent such crimes was passed as Electronic Transaction Act in 1996 followed by the Electronic Transaction Ordinance 2008, which was promulgated through an ordinance by Ex-president of Pakistan Gen. (Rtd) Pervez Musharraf promulgated on December 31, 2007, titled as "Prevention of Electronic Crimes Ordinance (PECO) 2007", however, it lapsed in 2010. Under this law cases were directly investigated by the Federal Investigation Agency of Pakistan with reference to spoofing of accounts, cyber scam, access of secured data, causing harm to any system etc. It has 21 sections and the important section of the law was the 6th one, which has said that if the accused has tampered any private, secured or public information or system or have used the stolen information in illegal way, will be punished with two years of jail along with a huge amount of fine (Jamil, 2006). Besides this law the Federal Cabinet approved the adoption of the Prevention of Electronic Crimes Bill 2007 on 17 January 2007. The proposed law titled as Prevention of Electronic Crimes Bill 2007 offers penalties ranging from six months imprisonment to capital punishment for 17 types of cyber-crimes, including cyber terrorism, hacking of websites and criminal access to secure data (Jamil, 2006). It also deals with cyber terrorism, criminal access, criminal data access, data damage electronic fraud, electronic forgery, misuse of electronic system or electronic device, unauthorized access to code, misuse of encryption, misuse of code, cyber stalking and suggest stringent punishment for offences involving sensitive electronic crimes (Kundi et al., 2012). This law suggests maximum punishment of death or life imprisonment against cyber criminals involved in the sensitive electronic systems offences.

In addition to the previous laws, government has presented a new draft law titled as Prevention of Electronic Crimes Act 2014 before cabinet for approval, which proposes some stringent punishments for cyber-crimes; however, it is deficient because it leaves all offences as baillable (Jamil, 2006). Yet, this proposed draft of law shall cover cyber terrorism, unauthorized interception, illegal access to information system and program or data, illegal interference with program or data, electronic forgery, identity crime and protection of women etc.

Unfortunately, this proposed law is still awaiting parliament approval to become an Act, is therefore, likely to face criticism as it gives absolute immunity to security agencies from any prosecution. Another weakness of the proposed law is that it also leaves for the government to decide which of its agencies would perform the task of investigation and prosecution. However, it says that cases would be tried at not lower than session court or higher courts, yet, the arrests could be made only after the permission of a court and once the investigation

officer satisfies the court that there exist reasonable grounds to believe it was necessary to proceed with such action.

Thus, in the absence of cyber-crime laws through which punitive action could be initiated against those criminals who will be committing crimes on the cyber world in Pakistan, individual and organizations both public and private are increasingly becoming victims of abuse on social media sites and internet frauds, etc. (Chaudhy, 2011; Bell, 2002; Grabosky et al., 2001).The complaint of fake Facebook Ids and profiles is the most rampant complaint, where people generate a fake profile of any person, mostly of girls, yet men are no exception to this crime.

2.6 Cyber-Legislation: Theoretical Foundations

Cyber-crimes laws in the different countries have been offered in a piecemeal fashion, where governments are trying to fit cyberspace within the four junctions of their known domestic laws. In majority of the cases, these governments have taken a 'functional equivalent' approach to legislation by analyzing the role of current laws in the non-digital world. They are identifying that how the same function could be achieved in eTransactions, and extending the existing law by analogy to cyberspace. Throughout the world legislatures and law making bodies are depending on the different approaches in their efforts to reap the benefits of this new technology. The three basic approaches include the minimalist approach, prescriptive approach and two-tier approach.

The purpose of the "minimalist approach" is to facilitate the use of eSignatures generally, rather than advocate a specific protocol or technology. Grandjean (1990) states that the minimalist approach is commonly used in the traditional common law countries i.e. Canada, US, UK, Australia, and New Zealand.

Whereas, motivation of the "prescriptive approach" mostly starts from a an urge to establish a legal framework for the operation of PKIs, whether or not other forms of secure authentication are included as well as a reflection of form and handwriting requirements that apply in the offline world (Kundi, 2010; Hakim & Rengert, 1981).

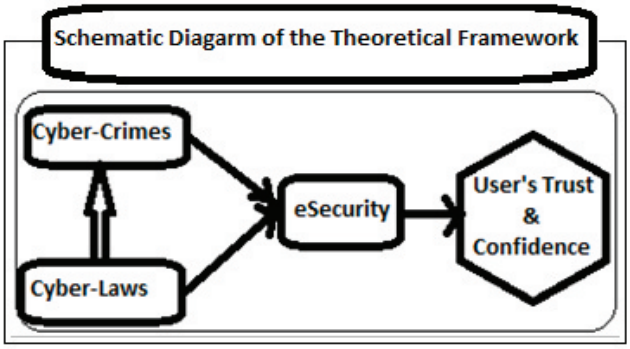
Under this approach the laws and regulations are to adopt asymmetric cryptography for creating a digital signature by imposing some operational and financial requirements on certificate authorities besides prescribing and defining the duties of key holders and the circumstances that may justify the use of eSignature. This approach facilitates the legislatures and regulatory bodies to play a direct role to set standards to influence the direction of this new technology. Germany, Italy and Argentina known for Civil law are the good examples using prescriptive approach for legislation against cyber-crimes (Halder, 2014).

The advocates of the "two-tier approach" on other hand contends that when some of the jurisdictions began to realize that the first two approaches are not necessarily mutually exclusive, so they use a synthesis of the both labeling it as "two-tier". It takes the form of enacting laws that prescribe standards for operation of PKIs, and concomitantly take a broad view of what constitutes a valid eSignature for legal purposes.

This approach is popular, notably in the European Union and Singapore, and Pakistan has also followed the two-tier approach for legislation of Electronic Transactions Ordinance in 2002.

2.7 Theoretical Framework of the Study

The schematic diagram of the theoretical framework was developed which is based on the survey of the existing studies. The diagram elaborates the relationship, and cause and effect of the dependent variable on the independent variables of the study.



3. METHODOLOGY

Literature survey was carried out to exhaust the relevant sources of the existing studies. ATLAS.ti, a computer based software was used for qualitative data analysis. Major concepts, variables and sentences were entered into ATLAS.ti, coding, extraction of quotes and memos creation was done with ATLAS.ti. In qualitative research, experts are using different methods like examining, categorizing, tabulating and recombining for data analysis. However, in this study, the researchers have used hermeneutics (James, 1992), discourse (Max, 1990) and heuristic (Moustakas, 1990) for data analyses and draw inferences and conclusions from the results of the data. The theoretical framework of the study presented in the above section 2 elaborates the cause and effect relationships between the dependent and independent variables of the study.

4. DICUSSION ON AND CONCLUSIONS

Cyber-crime is the emerging criminal offences committed illegally via internet like, breaking internet securities, spoofing or trespassing of email accounts, breaking passwords of bank accounts, spyware attacks etc. are highly punishable cyber-crimes.

Based on the observations from the previous cyber-laws in the world, it could be safely said that no law can be implemented to effectively eradicate the menace of cyber-crime. Several attempts have been made locally and internationally, but these laws still have deficiencies. What constitutes a crime in a country may not be considered a crime in another, so this has always made it easier for cyber criminals to go free after being caught and difficult for the other to handle and prevent the crimes and criminals.

In Pakistan, apparently the legislation that is intended to safeguard online community from cyber-crimes, cannot pulled into protect non-commercial issues including extremist communications and ideologies which are hatched in the cyber space. In Pakistan, extremist activities are carried out on social media to disturb and disrupt the sovereignty, integrity and credibility of individuals and institutions, this demands intensive legislation against cyber-extremism and terrorism and its linkage with international community fighting in war against terrorism (Kundi et al., 2012; Bell, 2002).

State-of-the-art technology is the driven feature of today's digital economies, the development and advancement of the nations is measured in terms of use of these advance technologies (Kundi, 2010; Ratcliffe, 2002) , however, when one look into the economic conditions and backwardness, where developing countries mostly facing severe financial crisis, they are unable to enjoy the latest machines, neither they have the capacity to use these machines due to lack of sufficient number of qualified IT-professionals, this is why they are dependent on the obsolete technology, on other side, criminals are using highly sophisticated systems and technologies hence, developing countries like Pakistan is facing the challenge how to prevent the cybercrimes with old versions of the systems.

Likewise, instead of off-the-shelf, customizations of technology especially the software in the forms of firewall and anti-virus tool kits is a prerequisite, however, in Pakistan off-the-shelf tool kits are used, and mostly these are unlicensed and pirated (Repetto, 1976). A study shows that 70% of the software used in Pakistan is pirated (Kundi, 2010). Though, laws are in the offing to prevent piracy and to protect the patent rights, however, due to weak implementation of law, piracy and use of pirated software are one of the biggest issues in Pakistan which is a barrier towards prevention of such crimes, and to ensure eSecuirty.

How to secure the computers, digital assets, and networking being used by the online community means how safe are their computers and software systems. Is all software housed on the user's network continually up to date (Harrington & Mayhew, 2001)? Exploitation through software is a common way through which hackers gain access to systems and sensitive information. User's mostly update software on network-connected machines is also easy way to cyber criminals. Thus, up-to-date anti-virus software tool-kits may be very helpful in protecting the network and systems used by the online users because leading antivirus software can detect, remove, and protect the user's machines and networks from malware etc. Likewise, the users must be careful and should avoid pirated software.

Education and literacy can help better in preventing the cyber-crimes, so education and training on how to use information systems and how to avoid or safeguard from the criminals on cyber space is need of the hour, that the users must understand the most common hacking tactics, such as phishing, social engineering, or packet sniffing etc. (Herhalt, 2011). The education and awareness across the country of the online users must go a long way to protect them against many types of cybercrime (Smith & Urbas, 2001). Because the introduction of new technology need education and awareness not only about the new systems usage but also, the rights, duties and

responsibilities associated with the new machines. Similarly, the regulations and laws which govern the eSystems should be widely disseminated, so that user becomes aware of the cyber-crimes regulatory laws and measures introduced by their governments as well internationally. It is commonly observed and several studies reports that users do not know about the cyber-laws, this why they easily become victims of the eFrauds and eCrimes in the developing countries generally and Pakistan specifically.

On the other hand, poor & conservative investigative system is also a barrier towards eSecurity as professional incompetency and political interference in the registration of FIRs, investigation system and cumbersome delaying procedures in the judicial system of the country delays the justice thus hampers the proper implementation of the cyber-laws (James, 1992).

Another means of eradicating cyber-crime is to harmonize international cooperation and law; this goes for the greed motivated and cyber-terrorists (Smith et al., 2002). They can-not be fought only by education, because they are already established criminals, so they can not behave. The only appropriate way to fight them is by enacting new laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies and international community. Though, cyber-laws exist to some extent in the country, however, their incompatibility & lack of coordination with International Cyber-Law enforcing agencies is the biggest issue to prevent cyber-crimes occurrence, as in most of the cases, criminals commit these crimes sitting outside the territorial boundaries and legal jurisdiction of the user's countries. Experts like, Zinnbaur (2005) believe that harmonization of the local laws with international laws, cooperation and coordination with global cyber-crimes enforcement agencies and courts in the forms of international treaties on cyber-crimes will be more helpful in preventing the cyber-crimes.

In the final analysis, it could be concluded that although Pakistan has initiated number of steps to control the eOffences, still there is room for much improvement. The government has shown its interest in finding solutions for recognition of electronic transactions and criminalizing eOffences by promulgating laws in this perspective. Moreover, some practical steps and measures could also be seen to counter cyber-crimes, yet, there is a need for more proactive approach and efforts. The implementation of law for the maintenance of electronic traffic data is one of the facets that need special attention, as most of the investigations reach to dead ends because of the lack of data, and therefore, the investigations remain incomplete. Likewise, another significant obstacle in the investigations process is the issue of jurisdiction and international co-operation. Till the moment these issues are not settled down on international level, the problems will seems continue to impede the combating of cyber-crimes.

Similarly, the practical issues in prosecution and adjudication of law are yet to be encountered as none of the investigations, initiated so far, have reached to final destination (UNCITRAL Model Law, 1996). Because the criminal justice system in Pakistan is based on Common Law, decisions by the courts could only be helpful to interpret and elucidate the essence of the law. However, nevertheless, the legal framework needs certain clarifications, and modifications. It is expected that practical application of the law and more research will be significant to develop legal structure and remedying the flaws in existing system.

At last but not the least, in the absence of cyber-law there is a strong urge on the Pakistani legislators to pass a law with two-tier model legislation that can stand against today's complexities of the cyber world to apprehend the accused instead of accusing people of political revenge and calling them the cause of government's own negligence and failure to meet the demands of today's fast moving cyber world.

References

1. 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.
2. Bell, R.E. (2002). The prosecution of computer crime, *Journal of Financial Crime*, 9(2): 308-25.
3. 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.
4. Chaudhy, 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).
5. Clarke, R.V., & Weisburd, D. (1994). Diffusion of crime control benefits: Observations on the reverse of displacement, in: R.V. Clarke (ed.), *Crime Prevention Studies*, 2: Willow Tree Press, Monsey, New York.

6. Collin, B. (1996). *The future of cyber terrorism*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, Denning, D. E. (2001). Cyberwarriors: Activists and terrorists turn to cyberspace. *Harvard International Review, XXIII (2)*: 70-75.
7. 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).
8. Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189), [Online] available at: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, (March 30, 2014).
9. Ghauri, I. (2014). *Electronic Crimes Act: Cybercrime to be made non-cognisable offence,* The Express Tribune with the International New York Times, [Online] available at: http://tribune.com.pk/story/672721/electronic-crimes-act-cybercrime-to-be-made-non-cognisable-offence/ (February 17, 2014).
10. Grabosky, P.N., & Smith, R.G. (1998). *Crime in the digital Age: Controlling telecommunications and cyberspace illegalities*, Federation Press, Sydney/Transaction publishers, New Brunswick.
11. Grabosky, P.N., Smith, R.G., & Dempsey, G. (2001). *Electronic theft: Unlawful acquisition in cyberspace*, Cambridge University Press, Cambridge.
12. Grandjean, C. (1990). Bank robberies and physical security in Switzerland: A case study of the escalation and displacement phenomena, *Security Journal*, 1: 155-9.
13. Hakim, S., & Rengert, G.F. (1981). Introduction, in: S. Hakim & G.F. Rengert (eds), *Crime Spillover*, Sage Publications, Beverly Hills, 7-19.
14. Halder, D. (2014). Information technology act and cyber terrorism: A critical review, Academia.edu, [Online] available at: http://www.academia.edu/945156/Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review , (March 28, 2014).
15. Harrington, V., & Mayhew, P. (2001). *Mobile phone theft*, Home Office Research Study No. 235, Home Office, London.
16. 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).
17. James, P. Gee (1992). *Discourse analysis*, In: LeCompte, M. et al. (2001). *The handbook of qualitative research in education* ((Eds). chapter 6), San Diego, Academic Press, USA.
18. 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/wp-content/uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf, (March 26, 2014).
19. KPMG (2013). *Global eFr@ud Survey*, KPMG Forensic and Litigation Services.
20. Kundi, G.M., Bartoli, A., & Baile. S. (2012). *E-local government: Implementation barriers in Pakistan*, Lap-Lambert Academic Publishing, Germany.
21. Kundi, G.M., Shah, B., & Nawaz, A. (2008). Digital Pakistan: Opportunities and challenges, *JISTEM, Revista de Gestao da Technologia e Sistemas de Informacao Journal of Information Systems and Technology Management, Sao Polo, Brazil*, *5*(2): 365-390, [Online] available at: http://www.revistasusp.sibi.usp.br/pdf/jistem/v5n2/10.pdf (April 6, 2014).
22. Kundi, GM. (2010). *E-Business in Pakistan: Opportunities and Threats*, Lap-Lambert Academic Publishing, Germany.
23. Lehman, D. (2000). Feds ID hacker who stole 485,000 credit-card numbers, *InfoWorld Daily News*, InfoWorld Media Group.
24. Levi, M. (1998). Organized plastic fraud: Enterprise criminals and the side-stepping of fraud prevention, *The Howard Journal*, 37(4): 423-38.
25. 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.
26. 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).
27. Marvin, C. (1988). When old technologies were new: Thinking about electric communication in the late nineteenth century, *The Journal of Law and Lawyers, 4(1)*: 88-97
28. Mativat, F., & Tremblay, P. (1997). Counter-feiting credit cards, *British Journal of Criminology*, 37(2): 165-83.
29. Max, V. Manen (1990). *Hermeneutical Analysis: Researching lived experience*, New York, State University of New York Press, USA.
30. Moustakas, C. (1990). *Heuristic research*, Academic Press, Newbury Park, USA.
31. New South Wales Independent Commission against Corruption (1999). *Weighing the waste: An investigation into the conduct at local council waste depot weighbridges at St Peters and Elsewhere*, New South Wales Independent Commission against Corruption, Sydney.
32. Parker, D. (1998). *Fighting Computer Crime: For Protecting Information,* John Wiley, USA, p. 10.
33. Prevention of Electronic Crimes Ordinance (2007). Ministry of Law, Justice and Human Right, Government of Pakistan, Islamabad. December 31, 2007.
34. 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).
35. 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.
36. Ratcliffe, J. (2002). Burglary reduction and the myth of displacement, *Trends and Issues in Crime and Criminal Justice*, 232; Australian Institute of Criminology, Canberra.
37. Repetto, T. (1976). Crime prevention and the displacement phenomenon, *Crime and Delinquency*, 22: 166-77.
38. Smith, R.G., & Urbas, G. (2001). Controlling fraud on the internet: A CAPA perspective: A report for the confederation of Asian and Pacific accountants, *Research and Public Policy Series*, 39; Confederation of Asian and Pacific Accountants, Kuala Lumpur/Australian Institute of Criminology, Canberra.
39. Smith, R.G., Nelson, D., & Mayhew, P. (2002), Robberies at automated teller machines in Australia, *Trends and Issues in Crime and Criminal Justice*, 228; Australian Institute of Criminology, Canberra.
40. UNCITRAL Model Law (1996), Article 7.
41. Zinnbaur, D. (2005). *Internet governance priorities and practices*, United Nations Asia-Pacific Development Information Program, Islamabad, Pakistan.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Recent conferences: http://www.iiste.org/conference/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar