CURRENT SITUATION AND ISSUES OF ILLEGAL AND HARMFUL ACTIVITIES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGY IN PAKISTAN

*Syed Abbas Ahsan**

I. INTRODUCTION

Information infrastructure is increasingly under attack by cyber criminals. The number, cost and sophistication of attacks are increasing at alarming rates. Such attacks threaten the growing reliance of commerce, governments and the public upon the information infrastructure to conduct business and process information. Most of the attacks are transnational by design, with victims throughout the world. Measures thus far adopted by the private and public sectors have not provided an adequate level of security. The reasons for lack of success in the field include the lack of timely sharing of information, slow and un-coordinated investigations, inadequacy of legal/investigative infrastructure governing cybercrime, jurisdictional assertions of multiple states, and lack of international co-operation.

Cybercrimes generally fall into two categories; first where the computer itself or the computer networks are the intended victims e.g. network intrusion, spoofing and spamming; secondly the use of computers to commit more traditional crimes e.g. identity theft and computer fraud, etc. Such activities have a significant negative impact and tend to discourage the use of computers that offer the chance for advancement in knowledge, convenience, commerce and intellectual interaction. This paper focuses on these very issues with reference to Pakistan. An effort has been made to ascertain the extent of problem and the legal and practical steps taken by the government to combat this growing menace. Bottlenecks and obstacles in the process and infrastructure already in place have also been identified.

II. PERSPECTIVE ON CYBERSPACE USE AND ABUSE IN PAKISTAN

It is very difficult to gauge the actual number of people using information and communication technology in Pakistan. The figures available from various sources, only on the number of Internet users in Pakistan, vary from 3 million to 17.5 million online users. However, all the major commercial institutions are making use of information and communication technology and use cyberspace to conduct their businesses, including all commercial banks. Most of the universities in Pakistan and many educational institutions in the major cities have online access and provide students access to computers and the Internet. The reason for establishing a legal framework to regulate electronic transactions and crimes was the dramatic rise in the number of Internet users in the country (almost 9,000%) from 2000 to 2008.

The legal apparatus to regulate electronic transactions and combat cybercrime was established through the Electronic Transactions Ordinance, 2002 and the Prevention of Electronic Crimes Ordinance, 2007. The laws established a regulatory mechanism for the conduct of electronic transactions and provided penal sanctions for the violation of the legal parameters established under these laws. The Prevention of Electronic Crimes Ordinance also provides the infrastructure for the investigation, prosecution and adjudication of cybercrimes along with the procedures for the same. On the abuse of cyberspace, the cybercrime figures may be quite misleading. In all, only 98 complaints have been received in the National Response Center for cybercrimes during the last year, since the promulgation of the Prevention of Electronic Crimes Ordinance. Of these complaints, only 21 cases have been registered and all of the cases are still under investigation. The majority of the complaints received were from corporate bodies and public institutions, mostly relating to fraud and unauthorized access. Almost all the cases required trans-border investigations and co-operation

* Superintendent of Police, Islamabad Capital Territory Police, Pakistan.

from international organizations, which is the main reason for delayed prosecution.

Internet Statistics Asia						
ASIA	Population (2008 Est.)	Internet Users, (Year 2000)	**Internet Users, Latest Data**	Penetration (% Population)	(%) Users in Asia	Use Growth (2000-2008)
Afghanistan	32,738,376	1,000	580,000	1.8 %	0.1 %	57,900.0 %
Armenia	2,968,586	30,000	172,800	5.8 %	0.0 %	476.0 %
Azerbaijan	8,177,717	12,000	1,035,600	12.7 %	0.2 %	8,530.0 %
Bangladesh	153,546,901	100,000	500,000	0.3 %	0.1 %	400.0 %
Bhutan	682,321	500	40,000	5.9 %	0.0 %	7,900.0 %
Brunei Darussalem	381,371	30,000	176,029	46.2 %	0.0 %	486.8 %
Cambodia	14,241,640	6,000	70,000	0.5 %	0.0 %	1,066.7 %
China *	1,330,044,605	22,500,000	253,000,000	19.0 %	43.7 %	1,024.4 %
East Timor	1,108,777	-	1,200	0.1 %	0.0 %	0.0 %
Georgia	4,630,841	20,000	360,000	7.8 %	0.1 %	1,700.0 %
Hong Kong *	7,018,636	2,283,000	4,878,713	69.5 %	0.8 %	113.7 %
India	1,147,995,898	5,000,000	60,000,000	5.2 %	10.4 %	1,100.0 %
Indonesia	237,512,355	2,000,000	25,000,000	10.5 %	4.3 %	1,150.0 %
Japan	127,288,419	47,080,000	94,000,000	73.8 %	16.2 %	99.7 %
Kazakhstan	15,340,533	70,000	1,400,000	9.1 %	0.2 %	1,900.0 %
Korea, North	23,479,089	--	--	--	--	0.0 %
Korea, South	49,232,844	19,040,000	34,820,000	70.7 %	6.0 %	82.9 %
Kyrgystan	5,356,869	51,600	750,000	14.0 %	0.1 %	1,353.5 %
Laos	6,677,534	6,000	100,000	1.5 %	0.0 %	1,566.7 %
Macao *	460,823	60,000	238,000	51.6 %	0.0 %	296.7 %
Malaysia	25,274,133	3,700,000	14,904,000	59.0 %	2.6 %	302.8 %
Maldives	379,174	6,000	33,000	8.7 %	0.0 %	450.0 %
Mongolia	2,996,081	30,000	320,000	10.7 %	0.1 %	966.7 %
Myanmar	47,758,181	1,000	40,000	0.1 %	0.0 %	3,900.0 %
Nepal	29,519,114	50,000	337,100	1.1 %	0.1 %	574.2 %
Pakistan	167,762,040	133,900	17,500,000	10.4 %	3.0 %	12,969.5 %
Philippines	92,681,453	2,000,000	14,000,000	15.1 %	2.4 %	600.0 %
Singapore	4,608,167	1,200,000	2,700,000	58.6 %	0.5 %	125.0 %
Sri Lanka	21,128,773	121,500	771,700	3.7 %	0.1 %	535.1 %
Taiwan	22,920,946	6,260,000	15,400,000	67.2 %	2.7 %	146.0 %
Tajikistan	7,211,884	2,000	19,500	0.3 %	0.0 %	875.0 %
Thailand	65,493,298	2,300,000	13,416,000	20.5 %	2.3 %	483.3 %
Turkmenistan	5,179,571	2,000	70,000	1.4 %	0.0 %	3,400.0 %
Vietnam	86,116,559	200,000	20,159,615	23.4 %	3.5 %	9,979.8 %
TOTAL ASIA	3,776,181,969	114,304,000	578,538,257	15.3 %	100.0 %	406.1 %

III. LEGAL FRAMEWORK

The laws related to information and communication technology follow the separation of the e-commerce and cybercrime model. There are separate laws governing both the aspects of the information and communication technology, nonetheless, the laws supplement each other in the regulation of all electronic transactions. The laws relating to electronic transactions provide the legal basis for evidence and give recognition to electronic documents and electronic communications. The laws governing electronic and cybercrime in Pakistan cover both crimes that are traditional in nature, i.e. theft, fraud, forgery, mischief and terrorism in which computers or any other electronic device is used to commit these crimes, as well as misuse of computers that is criminal in nature, or what we call content-related crimes, e.g. damage and access to electronic devices and data with criminal intent.

A. Penal Sanctions for Cybercrime in Pakistan

The first law promulgated in Pakistan regulating all electronic transactions is the Electronic Transactions Ordinance, 2002. The Electronic Transactions Ordinance provides a comprehensive legal infrastructure to facilitate and give legal sanctity to electronic documents as well as protection to e-commerce locally and globally. This law also penalized the misuse of electronic communication and charts the boundaries for certification of service providers. The more recent law, the Prevention of Electronic Crimes Ordinance,

2007, relates to cybercrime and has been framed specifically to criminalize the misuse of electronic media. Furthermore, the Prevention of Electronic Crimes Ordinance creates the structure required for the investigation and adjudication of cybercrimes.

1. Electronic Transaction Ordinance 2002

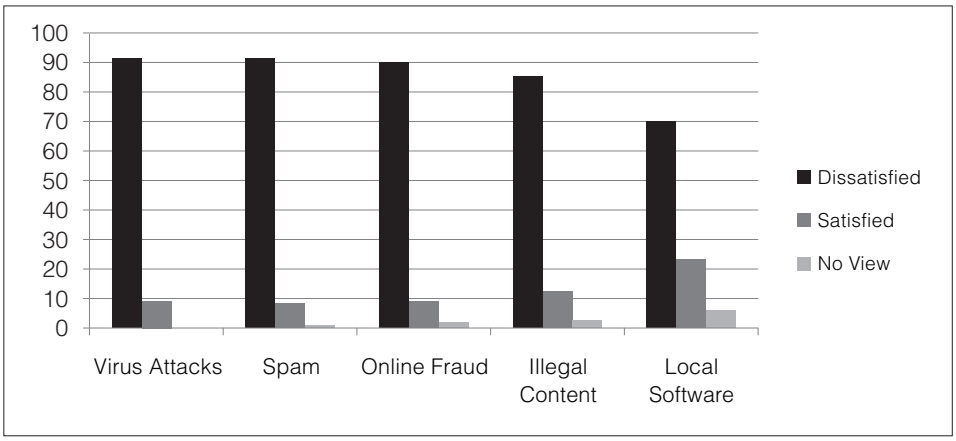
The Electronic Transactions Ordinance was promulgated in 2002, primarily to provide for the legal recognition and facilitation of documents, records, information, communications and transactions in electronic form. The law gives legal recognition to documents, information and records and allows their admissibility in a court of law without the requirement of a witness. The maintenance of documents in physical terms is also satisfied under this law if the document or record is accessible and retrievable. Moreover, the Ordinance delineates the rules on compliance and retention of documents in electronic form. The law also establishes the parameters for electronic communications and thus creates rules for associating documents with the recipient as well as the sender. Rules are also designed for legal acknowledgement, time and date of sending, along with establishing the place of sending and dispatch of electronic communication.

The Electronic Transactions Ordinance also formulates the principles that are required for any document, record, or communication and information to be deemed legally secure, thus setting up a digital signature regime whereby electronic signatures and electronic applications provide the legal security required for any electronic transaction. The Ordinance also establishes the criteria for the authenticity and integrity of advanced digital signatures provided by the certification service providers. The certification service providers extend certifications to websites and digital signatures.

The law does not criminalize most of the offences as supported by different international forums; however, the law does provide legal cover for the evidentiary value of all electronic transactions by amending Pakistan's evidence laws. The law recognizes the authenticity of all electronic transactions and brought these at par with other documentary transactions. Moreover, the Electronic Transactions Ordinance provides the foundation for the subsequent penal law, the Prevention of Electronic Crimes Ordinance, 2007. As an interim measure to prevent the misuse of now legally acceptable documents and to restrict the misuse of incentives granted in the law, certain offences are penalized. The penal sections of the law relate to false information from the subscriber to the certification service provider, issuance of false certificates, violation of privacy of information and damage to information systems or data.

2. Prevention of Electronic Crimes Ordinance 2007

The Prevention of Electronic Crimes Ordinance, 2007 was enacted against crimes related to the confidentiality and integrity of electronic systems, networks and data, as well as the misuse of such systems, networks and data. The law, apart from providing penal sanctions against the abuse of electronic transactions, also provides the procedural regime for the investigation, prosecution and adjudication of cybercrime. The following chart represents the survey responses of Internet users in Pakistan on Internet Governance, showing their top five concerns.



The chart above not only represents the concerns of Internet users in Pakistan, but also gives an informed opinion about the state of affairs in the field of combating cybercrime in Pakistan. The huge rate of growth of Internet users and the opinions of Internet users, both corporate and individual, have been the key drivers for the creation of the electronic regime in Pakistan. The ordinance based on such feed-back penalizes the following:

- Criminal access or damage to electronic data or systems
- Electronic fraud or electronic forgery with wrongful intent
- Misuse of electronic system or device with criminal intent
- Unauthorized access to codes or passwords with wrongful intent
- Encryption of incriminating communication or data
- Spamming, spoofing or use of malicious codes
- Cyber stalking, especially against minors
- Unauthorized interception by technical means
- Use of electronic system with '*terroristic intent*'

A detailed scrutiny of the law shows that its framers intended to adopt a very broad interpretation in the definitions and explanations of the crimes. This point is evident from the title and definitions as well as the penal sections of the law. Instead of using the terms "cyber" or "computer" crimes, the emphasis is on "electronic" crimes. As far as possible all definitions and interpretations are kept open with the use of phrases like '*including but not limited to*', etc. The broad interpretation may have been adopted keeping in view the common law tradition of prosecutorial discretion providing protection against inappropriate application of the law. Furthermore, in-depth interpretation and setting up of the limits of the application of law is left to the thorough scrutiny of judicial decisions during court proceedings.

A noticeable omission in the law is the non-differentiation of "negligent" and "intended" misuse of technology. The law is criticized for not making any distinction between what is unethical and what is illegal. In the Ordinance the sections relating to spamming, spoofing and unauthorized interception allow criminal proceedings without requiring criminal intent of the person involved in such acts. Without giving due consideration to criminal intent there is a possibility of misapplication of the law either by mistake or abuse. Therefore, the intent of the offender must be considered in all circumstances before any criminal sanction is applied against that person. Only when the criminal intent of a person is established, penal proceedings should be initiated against the person. There is a need to remedy this omission by establishing criminal intent in the forefront before the application of any penal sanction.

The law has been criticized for a number of other reasons. First, the law has been condemned as a curb on the freedom of expression, especially the part relating to cyber-stalking. Distribution of photographs of persons without their consent/knowledge and display/distribution of information are issues that need clarification in this section. This explanation amounts to censorship and can prove to be a hurdle for sharing of information, healthy criticism, or even common gossip over blogs. Moreover, the definition of cybercrime as given in the law is quite vague and includes terms prone to a wide multitude of interpretation e.g. vulgar, profane, indecent, immoral, etc. Such words have an extremely wide interpretation even in dictionaries and can have different connotations for different cultures, regions, or even individuals. The law, while establishing penal sanctions, should be clear so that any person coming under the jurisdiction of the law knows what limits the law has established and what constitutes an offence.

Secondly, section 11 of the law against the misuse of encryption has been censured for coercing self-incrimination which is contrary to fundamental civil rights. This section penalizes any person who encrypts any incriminating communication or data contained in an electronic system. However, this section is against Article 13 of the Constitution of Pakistan, 1973, which provides protection against self incrimination. As this section provides a criminal penalty for concealing incriminating evidence, it coerces an offender to decrypt such evidence, which may be self-incriminating. Hence, the law violates the right of protection against self-incrimination granted by the Constitution of the country.

Thirdly, section 18 has been disapproved for putting the burden of proof on the person accused of the offence under that section. This section deals with the offences involving sensitive electronic systems and

provides greater punishment if such systems are accessed. Although the burden of proving the crime in itself, i.e. illegal access to the system, lies with the prosecution, the law presumes that the accused had the requisite knowledge that the system accessed was a sensitive electronic system. This presumption shifts the burden of proof on the accused which is against the basic norms of criminal jurisprudence, which requires the crime to be proved beyond reasonable doubt by those who bring the charges against the accused.

Finally, the most vociferous denunciation has been directed against the term 'terroristic act' and the penal section associated with it. The evidently broad definition and explanation of this section is vulnerable to misinterpretation as well as manipulation. It is pertinent to note that the definition and explanation of terrorism is much more restricted and specific in the Anti-terrorism Act; as such many offences that may not attract the Anti-terrorism law can be prosecuted under this law. Use of malicious code against a public entity or computer network operated by the government and "violence" against the sovereignty of the state has been included in the definition of terrorism. "Violence" has further not been elaborated and is left to the discretion of the person applying and therefore interpreting the law. In addition to this, the explanation of terroristic intent has similar flaws and is open to misapplication.

B. Comparison with Convention on Cybercrime

With regard to the definitions of offences against confidentiality, integrity and availability of computer data and systems, these have been criminalized in Pakistan as explained in the Convention on Cybercrime of the Council of Europe. Comparable criminal sanctions are available in the Prevention of Electronic Crimes Ordinance 2007 for illegal access, interference, misuse and interception of electronic data or systems. The definitions in Pakistan are comparable with the convention and have rather been kept broad to take account of any offence related to the illegal use of all electronic devices, including computers or computer data. Computer-related fraud and computer-related forgery has also been amply covered in the laws in Pakistan. The same principle has been followed that all electronic devices have been included which may be used to commit any fraud or forgery.

Regarding the content related offences, the Prevention of Electronic Crimes Ordinance has limited application. Spamming, spoofing, cyber-stalking and malicious codes, which include viruses and Trojans, etc., have been criminalized. However, these do not cover all content-related offences as enumerated in the Convention. Moreover, the laws in Pakistan do not provide any sanctions against offences described in the Additional Protocol relating to racism, hate crimes and xenophobia. The issue of child pornography is not penalized in the law, but it is argued that the sanction against cyber-stalking provides protection to minors against abuse. The section on cyber-stalking does provide protection to the extent of soliciting illegal acts, which may include sexual acts; but the section does not criminalize production, transmission or possession of child pornography. A relevant observation in this regard is that all pornography, whether child pornography or otherwise, is illegal in Pakistan.

Protection of Intellectual Property Rights is another omission in the cybercrime laws in Pakistan. Again, it is contended that Intellectual Property is protected by laws particularly drafted for the protection of the same, and the cyber laws provide protection against accessing codes and passwords for the purpose of any illegal use of electronic data.

IV. IMPLEMENTATION OF THE CYBERCRIME REGIME

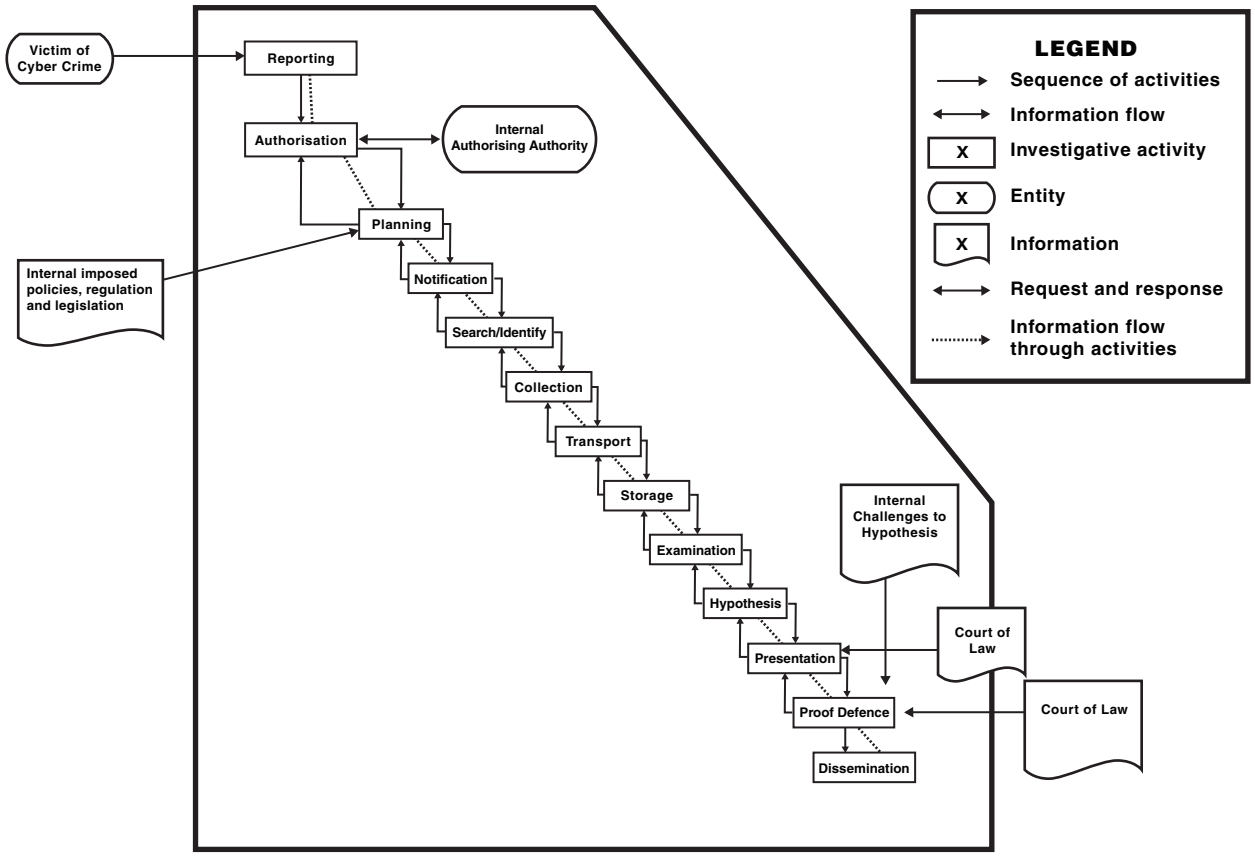
A National Response Center for Cyber Crimes has been established under the Federal Investigation Agency to deal with all issues related to cybercrimes. The functions of the National Response Center as declared by law are to ensure the enforcement of cyber laws, and to prevent, investigate and prosecute electronic crimes. The law also envisages a tribunal for the adjudication of all crimes under the Prevention of Electronic Crimes Ordinance. The National Response Center, apart from being the primary investigation agency against cybercrime, performs the following functions:

- Co-ordination with international organizations to handle trans-border cases;
- Technical support to government organizations for data and network security;
- Real-time network traffic patrolling and collection of data;
- Capacity building of law enforcement agencies in cybercrime;
- Provision of forensic services for cybercrime.

The tribunal for the adjudication of cybercrime as proposed in the law is yet to be established. All cases related to cybercrime are prosecuted in the normal penal courts as required by law until the tribunal is established.

A. Investigation

The National Response Center for Cyber Crime, which is the premier investigating agency against cybercrime, has its head office in the national capital, Islamabad, with three regional offices across the country. The centre's facilities consist of a Digital Forensic Laboratory and a cybercrime reporting and investigation centre. It provides special investigative services under the Telecom Act 1996, the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Ordinance 2007. The National Response Center for Cyber Crime also provides technical support to the local police in investigations involving the use of electronic devices. Such support is provided in investigations of ordinary crimes where electronic devices or media is used in commission of the crime.



The proposed model of cyber crime investigation

A waterfall model is used for investigation of cybercrime. All activities follow each other in sequence. The model progresses from crime reporting to authorization of investigation. The next step in the process is the collection and storage of evidence. Finally evidence is examined, a hypothesis established regarding the incident and the case is prepared for prosecution in a court of law. In fact, the investigation steps require several repetitions before the case is finally prepared for prosecution. The last step of examination-hypothesis-presentation may be reiterated a number of times as the understanding of the evidence grows in connection with other relevant evidence.

However, as the whole structure established against cybercrime is still in its infancy and the processes are not formalized, The National Response Center will come across many practical and procedural challenges in due course. Experience in handling electronic crimes will help the Center to determine its future course of action in combating cybercrime. Interaction with other international agencies and further

research and development will educate those involved in this endeavour to chart out the best methods to probe electronic offences. Apart from the lack of experience in handling electronic offences, there is a lack of awareness regarding the handling of such cases, not only in the general public but also amongst those affiliated with the criminal justice system.

1. Reporting System

Electronic crimes are reported to the National Response Center, which after initial inquiry and internal authorization approves the registration of a criminal case under any of the laws governing electronic offences. The cases are registered with the police stations of the Federal Investigation Agency, which has an established network around the country and deals with a number of other specialized crimes.

The major issue with the reporting mechanism is the lack of awareness amongst victims. Electronic crimes are normally not reported for the reason that it is assumed that such crimes cannot be traced and the criminals are faceless. Moreover, the victims of electronic crimes do not know where and how to report electronic crimes. Most electronic crimes go unreported till they have reached an alarming stage, whereby the investigations are conducted on the initiative of either the National Response Center or another government agency. In certain instances, electronic crimes have been initiated in response to requests from law enforcement agencies of other countries.

2. Digital Forensics

The increasing problems of cybercrime have enhanced the importance of digital evidence and digital forensics. Digital forensics includes the preservation, identification, extraction, documentation and interpretation of digital data. As electronic evidence presents special challenges for its admissibility in courts, proper procedures are required for collection, examination, analysis and reporting of evidence. The National Response Center has established its procedures based on the above mentioned objectives.

The collection phase involves search, recognition and documentation of electronic evidence. The examination phase includes the documentation of the content and state of evidence. This phase also involves the search of any information that may be hidden or obscured. Analysis differs from examination in that it looks at the evidence for its significance and probative value to the case. Examination is the technical review that is the province of the forensic expert, while analysis is performed by the investigation team. The process is completed with a written report outlining the examination process and the pertinent data recovered. Examination notes are also preserved for purposes of discovery and testimony. The examiner may be required to testify about the conduct of the examination, the validity of the procedure and his or her qualifications to conduct the examination. In this regard, the digital forensic laboratory provides technical support for examination of evidence for prosecution of electronic crimes.

The digital forensics laboratory has the facilities for the collection, validation, identification, analysis, interpretation and documentation of data as well as its preservation as digital evidence. It has the capacity for reconstruction of corrupt data which may have evidentiary value. The laboratory is equipped with the necessary software and equipment to achieve these ends. Although the Digital Forensic Laboratory has successfully supported the investigations conducted so far, there is room for further improvement with regard to technical expertise and equipment. An issue with evidence collection from cyber space is the maintenance of traffic data by service providers. In many instances, traffic data is not available from the service providers to identify criminals or the origin of the crime.

3. Co-operation and Liaison

The National Response Center is the focal point for all cases relating to electronic crimes and electronic security. Government departments liaise with the Center for their network and data security. Pakistan Telecommunication Authority, which regulates service providers and network traffic data, also co-ordinates with the Center for the enforcement of electronic laws. The Center is the central repository for research on network security and electronic crimes. To increase awareness and understanding of electronic offences the Center also conducts training and seminars for different agencies related with the criminal justice system. The National Response Center aids local law enforcement agencies in investigations where electronic media is used in the commission of crimes. Support is provided in the examination of electronic evidence and tracing criminals through electronic media.

International co-operation for detection of cybercrime is also routed through the Center, which has established liaison with Interpol. However, international co-operation is not very forthcoming for a number of reasons. First, electronic crimes are not criminalized in many jurisdictions and network traffic data is not available in many jurisdictions. This helps cyber criminals establish spoof network addresses, which makes it difficult to detect the actual perpetrators of the crimes. Secondly, international co-operation is not very forthcoming because the victim is in another jurisdiction, therefore less importance is attached to such investigations. There is also animosity and doubt about the credibility of investigations carried out in other jurisdictions and at times problems arise due to the admissibility of evidence collected in a foreign jurisdiction by a foreign investigation agency. Furthermore, priorities differ amongst states on the prosecution of certain offences. It is for these reasons that the cybercrime law in Pakistan is based on reciprocity as far as international co-operation is concerned. Furthermore, it does not make international co-operation mandatory. Rather it allows ample discretion in assisting investigations and sharing information regarding electronic crimes and data with other jurisdictions.

B. Prosecution and Adjudication

As the infrastructure against electronic offences is in its early stages and investigations in some cases have only recently been initiated; none of these have reached the prosecution or adjudication phase. The law requires setting up a Tribunal for the adjudication of electronic crimes, which has not been established yet. Until the Tribunal, ordinary courts are empowered to adjudicate electronic crimes; the Tribunal is empowered to take cognizance of offences under the Prevention of Electronic Crimes Ordinance.

1. Jurisdiction

The law allows for a wide application of jurisdiction covering the principles of territorial, extra-territorial as well as personal jurisdictions. However, such a wide interpretation of jurisdiction of the law is not advisable and practically unrealistic. The principle of territorial jurisdiction is accepted in all criminal offences, based on the principles of respect for the sovereignty of other states. Jurisdiction is applied if the offence is committed within the territory of the state or if the offence produces its effects in the territory of the state. Even such application of limited jurisdiction leads to conflict of laws. Extraterritorial jurisdiction may result in the non-availability of evidence which may be present in the jurisdiction where the actual offence was committed. Moreover, even if, through international co-operation, evidence and the suspect are brought to the jurisdiction of the victim, the cost of numerous such investigations and prosecutions would lead the system to failure. Another issue with extraterritoriality is that an act performed in one jurisdiction may not be an offence but it may be criminalized in the jurisdiction where the act effects. Such a system is also prone to abuse, as it may be used to prosecute public officials or extraterritorial investigations may form an excuse for espionage. There is a need to establish a mechanism to settle jurisdictional conflicts through recognition of the investigative processes and evidence in other jurisdictions around the world and to standardize the priority of exercising jurisdiction.

2. Electronic Evidence Admissibility and Evaluation

The evidential issues, as already discussed, have been sorted out through the Electronic Transactions Ordinance, which has made amendments in the existing evidence laws to provide legal recognition to all electronic transactions. In addition to this, for the purpose of evaluation of evidence, the Prevention of Electronic Crimes Ordinance allows the tribunal to appoint and take assistance in technical aspects from *amicus curiae* having knowledge, experience, expertise and qualifications in information and communication technology, of which the government is bound to maintain a list.

V. CONCLUSION

In the final analysis, it is concluded that although Pakistan has taken a number of steps towards controlling electronic offences, there is room for much needed improvement. The government has shown its interest in finding solutions for recognition of electronic transactions and criminalizing electronic offences through promulgation of laws in this context. Although practical measures have also been taken to counter electronic crimes, there is a need for a more proactive approach. The enforcement of law, especially in the field of maintenance of electronic traffic data, is one aspect that requires special attention, as most of the investigations have reached dead ends due to the lack of data. Consequently, investigations remain incomplete. Another obstacle in the path of investigations is the issue of jurisdiction and international

co-operation. Till the time these issues are settled on an international level the problems will continue to obstruct the combating of electronic crimes.

Practical issues in prosecution and adjudication are yet to be encountered as none of the investigations, initiated so far, have reached that stage. As the criminal justice system in Pakistan is based on Common Law, decisions by the courts would help in interpreting and elucidating the essence of the law. Nevertheless, the legal framework needs certain clarifications, and modifications. It is hoped that practical application of the laws and further research will help in developing the legal structure and remedying its flaws.

BIBLIOGRAPGHY

Commonwealth Secretariat. (2002, October). *Model Law on Computer and Computer Related Crime*. Retrieved August 3, 2008, from http//:commonwealth.live.poptech.coop/shared_asp_files/uploadfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

Constitution of the Islamic Republic of Pakistan. (1973). Pakistan.

Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189)*. Retrieved August 15, 2008, from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Council of Europe. (2001). *Convention on Cybercrime (ETS 185)*. Retrieved August 15, 2008, from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Electronic Transactions Ordinance. (2002). *Gazette of Pakistan, Extraordinary, Part-I of 2002*. Pakistan.

Internet World Stats. (2008, June 30). Retrieved August 21, 2008, from http://www.internetworldstats.com/stats3.htm

Jamil, Z. U. (2002, September). *E-COMMERCE LAW IN PAKISTAN*. Retrieved August 20, 2008, from www.jamilandjamil.com/publications/pub_reports/IBP%20Paper%20151004.pdf

Prevention of Electronic Crimes Ordinance. (2007). *Gazette of Pakistan, Extraordinary, Part-I of 2007*. Pakistan.

United Nations. (2000). *Tenth United Nations Congress on the Prevention of Crime and Treatement of Offenders*. Retrieved August 10, 2008, from https://www.asc41.com/10th%20un%20Congress%20on%20the%20Prevention%20of%20Crime/013%20ACONF.187.10%20Crimes%20Related%20to%20Computer%20Networks.pdf

United Nations. (1994). *The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime*. Retrieved August 7, 2008, from http://www.uncjin.org/Documents/irpc4344.pdf

Zinnbaur, D. (2005). *Internet Governance Priorities and Practices*: Pakistan. Islamabad: United Nations Asia-Pacific Development Information Programme.