EFFECTIVE ENFORCEMENT OF CYBER LAWS IN PAKISTAN

Mr. Muhammad Usman Akram, GC University Faisalabad, Pakistan. anitpersonnel@gmail.com
Prof. Dr. Nadim Asif, GC University Faisalabad, Pakistan. n_asif@yahoo.com
Mr. Babar Saeed GC University Faisalabad, Pakistan. babarsaed@hotmail.com
Mr. Tahir Abdullah, GC University Faisalabad, Pakistan. tahir_wains@hotmail.com
Mr. Umer Sarwar, GC University Faisalabad, Pakistan. sarwaromer@gmail.com

ABSTRACT: The term 'Information Technology' evolved in the 1970s and if we consider a medium or large company providing goods or services, its information technology department will be responsible for storing, protecting, processing, retrieving and transmitting the information. Information Technology (IT) is a wide and varied sector, and is represented in some form in almost all the industries. It is a blend of computers and communication technology where IT professionals perform variety of duties, ranging from development and installation of applications to designing complex computer networks and databases. Although, the term 'Information Technology' is becoming more familiar to the common man some people still wonder, what is information technology? As a concept, it has evolved from the basic usage of computers, internet and processing of information in any industry. In Pakistan use of internet is growing rapidly day by day. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. It is very much obvious that there are two sides to a coin; Internet also has its own advantages and disadvantages. One of the major disadvantages is Cyber-crime or misuse of Information and Technology– illegal activity committed on the internet. The internet, along with its advantages, which has made the world into a ‘Global Village’ in return, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spam, software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise. In this study we would give suggestions and means with which effective enforcement of Cyber Laws in Pakistan would be implemented.

I. INTRODUCTION

In this era of technology, the people who are directly or indirectly linked with the internet as well as they are making their lives possible by utilizing internet more and more in daily routine are called ‘Netizens’ and their world is cyber world. The Netizens must have to follow the rules and regulations to survive in the global village. It is possible that use and misuse of technology may be done by someone while living in cyber world. Now days computing systems and related devices are associated with each other and all the development has been successfully done due to development in software engineering. We are now in situation to handle everything by using software made for some specific hardware, even managing better the flying objects in the air. The efficiency of software has made possible the things under control in every field of life as we can have shopping & banking online. People paying the less cost during using these technologies as compared before. The rate of effectiveness is higher than the paying less cost. Rapid success of internet has remitted the distances and smoothness, sharpness and many more attributes come into existence & generated massive openings for economic criminals. The people involved in fraudulent type activities have also the same benefits as others. They are also using the same opportunities and making relations with each other and they seem invisible in order to keep away from discovery and control. These criminals transfer funds to each other worldwide illegally. These people are operating their selves from all around the world online and making transactions. There is a risk factor for all the communities those surfing over internet. Due to the blessings of internet we can consider the risk factor as major block towards E-Commerce. As per new report from the CoE current leaning in the fields of IT & computer systems and the chain of network safety is quite better after implementing the different SOPs made for
security and getting it centralized as well. This is satisfactory situation to extend the roots of cyber technologies more and more.

The techniques used to commit cyber fraud are increasing every day. Especially in 3G technologies where video streaming on internet, calling on internet, has opened the new horizons. Annually, the cost of damages done by cyber-crimes are very much high. According to issues discussed related 3G and its applications, it is difficult task to identify and detect the cyber related fraudulent activities because conventional crimes, one can also use the computer and related devise from everywhere being online but cyber-crime must be done using computer system, computer network systems and all other communication devices. The assessment of cyber frauds and related crimes are self-contradictory. In light of reports generated by council of Europe, by certain parties; inspecting their financial welfares, the software manufacturers are keen interested for alarming people and to give them awareness about it to them. We have the suite able example of spamming which is most common and a bigger threat and this case of spamming obviously displays the hazard of cyber-crime that can be inflated. Aforementioned details show the evaluation of the severity of cybercrime. The report from the Council of Europe said above describes the work of an organization that is undoubtedly one of the most important forums for the protection of human rights, we should be afraid for the threat the problems in this list pose to individuals; actually, very afraid. If we accepted the report in its entirety the only possible conclusion is, cybercrime clearly and seriously threatens our information societies. Many criminologists are warning us not to draw such conclusions. They claim that this anxiety is being provoked, quite intentionally by certain parties pursuing their economic interests and by others trying to make their voice heard in the process of reallocating public funds. Yet the case of spam clearly shows us that the harshness of cybercrime can be magnified. At the beginning of 2007 there were estimates of spam represented 80% of e-mail traffic in 2005, 95% in 2006 and that the system will reach its capacity in 2007. This paper does not trust merely upon permissible definitions of illicit behavior in cyber world. Instead of we shall be examining the problem through sociological likenesses of cyber world and cyber culture. These are important for us if we have to understand the criminological/casualty rational couple criminals. The research exemplifies more exact physiognomies of cyber-crime persecution and cyber deviants, hacking personnel or ‘console cowboys’. One common definition describes cyber-crime as an action through which system either from the networks or stands alone, a target or a place of lawless movement. Other definition stab to have the target and maybe meanings for version and define cyber-crime further exactly. Somebody who creates flash devices that may contain some harmful malicious codes, finish information from systems the time of attachment of these devices. This act will succeed as cyber-crime as definition founded on a wider description including acts for example unlawful access to data. Obviously, there is substantial complexity in defining the term “cybercrime”. The term “cybercrime” is used to label a range of offences including traditional computer crimes. As these crimes differ in many ways, there is no single criterion could include. In contrast with discussion, consider a case if you are surfing over internet and buy something online. You have paid the amount online through debit/credit card and acknowledged by the company that you will get you purchased items in 15 days or so, etc. If you may fail to receive your items in time or may not receive, in another case you may be receive your desired items but they were not in condition in which company committed. After investigation you came to know that the company were fake from you had purchased. It is big trouble, you have paid the amount and fraudulent activity came into being. Now, what will happen? Will you bear the cost that you have paid? Or you will try to log complain in police station about situation held? Finally, you have decided to launch complain for the said matter. Did you know that what will be your 1st step to follow cyber-related issue? Is it quite obvious, that you will be confused to manage the situation because you don’t know how to log your query in this regard. You also don’t know what kind of institutes and judicial infrastructure is there in Pakistan to handle these cases. Defining Cyber Crimes; A number of terms are being used the opportunities for electronic crime are extensive and refer to as follows:

- Crimes in which information and communications technologies are the target of offences.
- Crimes in which technologies are used as tools to commit an offence.

Cyber-crimes are enabled by technologies (a computer is required to commit the offence such as ‘phishing’, it also enhanced by technologies computers make it easier to commit an offence, such as credit card fraud etc.

There are different mechanisms being used to clarify, manage and monitor the cyber related terms and conditions e.g. cyber-crime has a thin constitutional meaning in Australia. It is used in the Cybercrime Act 2001 and gives details about wrongdoings in contradiction of information stored in computers and its related devices too. At international level bigger terminologies being used for cyber-crime. Cyber-crime is used as an umbrella as well as an array of wrong action including offences to destroy stored information in system, computer-related offences, contented violations, and patent crimes. As per Council of Europe. Extensive definition of cyber-crime joins partially with overall crime groups which needs not be depend upon Technology and other information systems, such as managerial corruption and financial
misconduct. Collectively, we know that we don’t have complete land law in Pakistan due to which we are facing terrorism, bad economy, poor leadership, corruption etc & now we are attached with the cyber world in each way of life where everything is automated and computerized. Keeping in view the literacy rate of our state, Are we able to make and manage the new system which will deal with the issues related to cyber-crimes and avoidance in this cyber world? Do we have any system introduced for above said? If yes, then is it complete, reliable and able to overcome all the IT related issues? For this description, we have two problems;

Firstly, we have to build worthy & unblemished cyber reforms for Pakistan unlike existing Land Law. Secondly, its effective enforcement. So, there must be a mechanism which will deal with cyber related issues of Pakistan.

II. REVIEW OF LITERATURE

IT Act India (2000)

In year 2000 India has passed IT Act 2000 to deal with IT and cyber related issues. This Act stated all the terms of Cyber Security, by means that protection of information and followings;

1. Equipment
2. Devices
3. Computer
4. Computer resource
5. Communication device and
6. Information stored therein from unauthorized access
7. Use of information
8. Disclosure
9. Disruption
10. Modification or destruction

In context with the above said this Act defines the penalties against violations, Compensation process and authority of the implementation.

Mechanism for Implementation of Act

Indian IT personnel focused on some basic issues of cyber security areas. These IT personnel are the part of Computer Emergency Response Team of India.

- Organization of cyber incidents related activities

Benefits of Cyber Laws

In sight of the expansion in transactions and communications carried out through E-records & the Performance pursues to empower administration sections to receive fragment ad creating preservation of authorized documents in shape of computerized data. This Action has also projected a permissible outline for the authentication & cause of E-records done by “Digital Signatures”.

- As per the viewpoint of terminologies used for E-Commerce all over the India, the “IT Act 2000” and its supplies have much more constructive features. For example, the implication of this provision offered for the E-Businesses would be that electronic document would now be a legal and legal form of announcement in the country. It can be fashioned and appropriate in any courts of law in agreement with “IT Act 2000”.

- Companies will be able to take out E-Commerce consuming the permissible infrastructure for network offered by the “IT Act 2000”.

- Digital signatures will have the legal validity and sanction in the Act.

- The Act drag opens the ways for the entry of corporate institutions in the business of being Certifying Authorities for issuing ‘Digital Signatures Certificates’.

- This “IT Act 2000"currentlypermitsmanagement to subject announcement for the network. Therefore, signaling E-Governance and E-Infrastructure.

- “IT Act 2000”correspondinglyreports the standing position to matters related to safety & security. That is very thoughtful for the accomplishment of “Electronic Transactions”.

- According to the “IT Act 2000” it is probable for companies to obligate a constitutional preparation in case if anyone breakdowns their system or computer network systems and being causes compensations or duplicates information. The compensation given as per the “IT Act 2000” is Rs: 1 crore maximum as financial compensations and not more than this.

Convention on Cybercrime Budapest, 23.XI (2001)

Member States of the CoE (Council of Europe) along with other stack holders allowing the aim of the “Council of Europe” have to obtain greater harmony
between other stack holders. Identification of the worth of advancement collaboration with the other Circumstances and gatherings for the conference Convinced of the essential to follow as junk of importance and a mutual illegal strategy by means that the defense of civilization in illogicality of cyber-crime in order to accepting appropriate legislature and reassurance worldwide collaboration. Awareness of the profound variations transport by the making things computerized. Combination and enduring centralization worldwide of computer system networks distinguishing the need for support between Countries& private industries in fighting cyber-crime as well as the need to defend authentic welfares in the use and growth of information technologies and related industry. Trusting an actual contest in contradiction of cyber-crime needs increase speedy & well-functioning worldwide collaboration in illegal issues. Openhearted modern expansions that additional advance intercontinental sympathetic and collaboration in opposing cyber-crime counting deed done by the UN and OECD. The European countries along with members of G8 also. reminding group of rectors references# R (85) 10 regarding the applied submission to ‘European Convention’ for common support in illegal substances for the interception of telecommunications # R (88) 2 on piracy in the field of copyright and neighboring rights # R (87) 15 regulating the use of personal data in the police sector # R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology; Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime; Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Agreed on given below;

1. Use of terms
2. Measures to be taken at the national level
3. International co-operation
4. Final provisions

Electronic Transactions Ordinance, Pakistan (2002)

ETO passed by the national assembly of Pakistan in 2002. In this ordinance electronic transactions and E-commerce business was focused to prevent from cyber-crime. The drafting of this ordinance was the 1st initiative taken by the Govt. of Pakistan towards the development of the legal frame work for cyber-crime as well as to legalize the cyber related issues in this order. Before drafting this legal frame work for cyber-crimes and the enforcement, general telephone and telegraph act was deployed for handling cyber-crime related issues and all the complaints were chandelier by the traditional courts of Pakistan. This ordinance supports to service provider companies and users as well those used the services provided by these companies to rectify their cyber-crime complaints. Further, ETO privileged to a single subscriber to log their complaints regarding cyber-crimes they faced. The ETO described the following legislation key points

- “Accreditation certificates” will be issued to service providers that will be granted by the certification council to a certification service provider
- “Certification council” is electronic certification accreditation council that is established under the section 18 of constitution of Pakistan
- Digital signatures
- Electronic Evidence

Under ETO certification, service provider issue certificates for the use of cryptography services. As per this ordinance the addressee is a person who intended the creator to have electronic communication. ETO deals with the electronic signatures by means that, an electronic signature will be unique for the person who is signing it & this electronic signature will recognize that person. These electronic signatures will be created in a specific way or a mean by the sole control used by that person. After making electronic signatures, these signatures will attach to the E-documents in a way that any change in E-documents will be detectable. Basically, ETO defines the following concerned entities;

- Accreditation certificate
- Certification council
- Accredited certification service provider
- Addresssee
Electronic signatures
• Appropriate authority
• Certification practice statements
• Cryptography services
• Electronic documentation
• Information
• Information systems
• Intermediary network service provider
• Originator
• Person
• Repository
• Security procedures
• Subscriber
• Transaction


Every developing country need some guidelines and reference points to make their constitution as a role model. That specimen is important to standardize the terms and conditions especially for making a new one. Towards making a constitution for cyber-crimes in any nation, a reference model is required which will help the nation to make it so. In year 2004 a model for cyber-crime and for investigations is developed which was made by combining some other important related things for it. It was just a reference point as specimen. As per this journal, the terms and conditions used is quite different as compared to other models of laws. This clearly defined the scope of the investigation process along with capturing the same information used for investigation. Processing of information is also mentioned in it. An outcome of this assessment of the prototype by working cyber-crime detectives is offered. This new model has been compared with other existing models and presented for investigations. Although a perfect typical prototype of cyber-crime inquiries is significant as it make available the intellectual situational agenda. It also gives the liberated of any specific tools and technology or structural atmosphere. A reference model is also helping for the conversation of performances and equipment for supportive things for the work of agents. This new one offered a basics for mutual terminologies to support conversation and distribution of proficiency. Model can be helpful for development of methodologies an new technologies as well as the emerging technologies subject to investigations. Additionally, this proposed would be used in a very practical way to find out opportunities for the growth and implementation of new emerging technologies in order to help investigators. In terms of investigation it provides the background for the collected information and examination of needs for investigation tools. Now a time, we are lacking to have any reference points for making new cyber constitution and the available models are not briefly discussed the aforementioned things throughout from awareness to investigation. It also give benefit IT personal and the professionals responsible for security as well as the team examiners. Collectively these professionals can take part in investigation utilizing their experience. This article offerings a stretched model for cyber-crime inquiries which categorizes the happenings of the analytical procedure and the foremost evidence chain in that course. A significant issue of unindustrialized supportive riggings. Standing replicas from the fiction are designated and associated to the new exemplary. It is also important that the model defined in it is larger compared to those which deals with “digital evidence processing”. Efforts to collected as much as conceivable of the complete cyber-crime fact-finding procedure including the “Digital Evidence Processing “happenings.

The Proposed Model

The proposed model as per this article shows the followings,
• Awareness
• Authorization
• Planning
• Notification
• Search for and identify evidence
• Collection of evidence
• Transport of evidence
• Storage of evidence
• Examination of evidence
• Hypothesis
• Presentation of hypothesis
• Proof/Defense of hypothesis
• Dissemination of information

Advantages and Disadvantages of the Model

Most important advantage of this model in contrast to others is the clear recognition of information flow in the exploratory procedure. This will allow tools to be particular and developed & dealing with case management. Examination of proof and the controlled distribution of information. Model can also help send down the expertise and experience of investigators with techniques such as data-mining and Expert-System.
Evaluation of the Model

The approach take on early confirmation of model stood to achieve the opinion of the deliberate municipal i.e. detectives. It was handled through awarding the effort for many more well-informed forces agents those have involvement since from two to ten years in computer system corruption learning.


PECO is the constitution passed by the parliament and president of Pakistan under the clues (1) of article 89 of constitution Pakistan. This ordinance focused on any action against the privacy, reliability, use of E-Systems, communication networks and data as well as misuse of these systems & for the imprisonment of such vulnerable actions and methods for enquiring, hearing and evaluation of offences considered cyber-crimes. This ordinance implies all over the Pakistan and every person who commits a cyber-crime either he/she is Pakistani national or not near or far from Pakistan. PECO describes that it will be applicable if someone is being cause of any threat to the security of Pakistan, its nationals, National harmony, national property, E systems, and National data, located in Pakistan. This order defines the access, authority code of criminal procedure, data, decision of the authority, Electronic, E-devices, Email messages email address, e systems, encryption of data, function, interlope, offence. Plane version, rules, schedule, sensitive e system, Service providers, subscriber information, traffic data, unauthorized access. PECO elaborates following offences & their punishments

1- Criminal access
2- Criminal data access
3- Data damage
4- System damage
5- E-Fraud
6- E-forgery
7- Misuse of e system or e devices
8- Unauthorized access to code
9- Misuse of encryption
10- Malicious code
11- Cyber stalking
12- Spamming
13- Spoofing
14- Unauthorized interception
15- Cyber terrorism
16- Enhanced punishment for offences evolving sensitive e systems
17- Offences being done by corporate

Most important thing that is descrying bed in this ordinance is prosecution and trial of the offences made under the cyber-crimes. Ordinance declares in detail about the prosecution and the procedure of trial of offences and the payment of compensation that will be made to the victims of the cyber-crimes. Another positive key point of the said ordinance is the guideline for the establishment of investigation and prosecution agencies those will deal with the cyber-crime offences, powers of prosecution officers, real time collection of traffic data, retention of traffic data, trans-border access. As this law is implemented all over the world, international cooperation is discussed in this ordinance with deal, according to the ordinance federal government of Pakistan can cooperate with any other county’s government, Interpol and other international enforcement agencies for investigation and prosecution process regarding to the cyber-crime activities. Under this ordinance a tribunal with the name of ICTT (Information & Communication Technologies Tribunal) will be composed and the head-quarter of this tribunal should be placed in Islamabad. This order describer the powers, limitations, authorities and procedure to submit an appeal to this tribunal. After trial at this tribunal if applicant is not satisfied he has right to submit an appeal against the decision of this tribunal in high court. Civil courts of Pakistan do not have jurisdiction to try cyber-crime offence. In miscellaneous said ordinance will deal with ordinance to override the other laws, power to amend schedules, power to make rules, removal of difficulties of ordinance.
existing international instruments and lend hand countries in set up a sound legal groundwork. This guide being offered by ITU gives a complete impression of the most related topics connected to the legal characteristic of cyber-crime. ITU guide focuses on the load of developing nations regarding cyber constitution. Owing the international dimension of cyber-crime the legal gadgets are the same for developing and developed countries. However, the references used were selected for the benefit of developing countries. ITU report supply a large selection of possessions for a more in depth study of the different theme. ITU guide focused on mentioned below as core part of making laws and enforcement of cyber world;

1. International Dimensions of Cybercrime
2. Consequences for Developing Countries
3. Typology of Cybercrime

**The European Commission**

European Union has on hand a proposal for a new cybercrime legislation to be taken in all member of union. It will increase the EU protection against cyber assault.

**III. MATERIALS AND METHODS**

Classifications of Cyber Crimes

In general there are three classes of cyber-crimes for which we are finding out the ways for avoidance of this crime through effective enforcement and awareness to the communities related to cyber world. Cyber-crime can be done against any of followings;

- Cyber Crime Against Person
- Cyber Crime Against Property

**Banks**

With the revolution of IT, Banks are conducting their business online. Thousands of bank branches are connected with each other and making transaction. Banks providing their services through internet and this kind of transactions are growing day by day. The usage of internet and making transactions online are most probably introduced firstly in banking sector where banks have offered services online e.g. ATM cards, online money transfer credit cards etc. below mentioned table shows the ratio of fraudulent activities through credit cards from year 2002 to year 2007.

<table>
<thead>
<tr>
<th>Year</th>
<th>Losses due to Fraud (USD billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>1.0</td>
</tr>
<tr>
<td>2003</td>
<td>1.5</td>
</tr>
<tr>
<td>2004</td>
<td>2.0</td>
</tr>
<tr>
<td>2005</td>
<td>2.5</td>
</tr>
<tr>
<td>2006</td>
<td>3.0</td>
</tr>
<tr>
<td>2007</td>
<td>3.5</td>
</tr>
</tbody>
</table>

Credit Card Frauds 2002 to 2007

Followings are the key areas of cyber-crime related banks;

- Electronic Money Laundering and Tax Evasion
- Sales & Investment Fraud
- Electronic Funds Transfer Fraud

**Police**

Regarding collection of facts, figures and SOPs related to cyber-crime and its enforcement; Different Police stations have been searched out. It is being noticed...
that the two things are involved in context with the enforcement and awareness of cyber laws as follows:

- Less rate of Computer Literacy
- Less use of internet computing

In this survey of police stations, the police staff is not equipped with neither computer knowledge nor any newly introduced technologies that may be used in online fraud. They didn’t have offered any kind of computer education and refresher courses related to investigations, enforcement of cyber laws. This is observed that police department has been short of utilization of computers and the new technologies that may help them to investigate the cases being logged.

Courts

Differentiating citizens & Netizens, we have gone through the visits of different courts. It is followed that not a single court is exists to hear the cyber related case separately. Its experimental also that the staff of courts are not familiar with the circumstances of cyber cases and other details. Cyber cases are only handled by the FIA’s wing for cyber-crime named as NR3C. As a first step cyber case can be logged online or can be reported through an email to be sent on NR3C’s cell. Generally people suffering from cyber frauds and cyber terrorism don’t know the SOP of complain resolution. So, in this stair the involvement of courts and the authority of court is not up to mark in order to facilitate the concerns. As mentioned earlier, the cyber related cases and implementation of respective laws only being monitor at federal level up till rectification of case, although FIA is dotted in all the big cities of Pakistan but it is being taken in that district level monitoring is not made yet.

Judges

In order to accomplish the task of testing the competence level of judges we take several interviews of different courts. The following tools, techniques, procedures have been discussed with them to explore the computer literacy in context with the followings:

| Email |
| Email Tracking |
| Website / Web Hosting/Domain Naming |
| Governing bodies of cyber issues in Pakistan |
| Digital signatures |
| Hacking / Cracking |
| Cyber-crime detection |
| Cloud Computing |
| Phishing / Spamming |
| Investigating cyber crime |

| Cyber terrorism |
| Electronic frauds |
| Jurisdiction process for cyber related cases |
| Imprisonment (Minimum to Maximum) |
| Legislation for Cyber Laws |
| Enforcement of cyber laws |
| Awareness of cyber laws in civil society |
| Trainings attended (Cyber related) |
| Cyber constitution for Pakistan |

Investigated Computer & Internet Literacy from Judiciary

Lawyers

Lawyers are the core entity that plays an important role after once the case has registered either of land law or cyber law. In fact Police, courts, judges and lawyers are collectively a forum which deals with the case (no matter what kind of). As for as cyber law & order concerns the lawyers are an independent community which is little better than the judges as they are maximum in numbers, so that we may consider the same proportion for knowledge comparing attributes and size of community. It is placed in documents during these visits that lawyers are interested to have cyber related courts at regional or district level for the convenience of their clients as well as for easy access to contact the concerned in terms of easy, proper, in time, less in cost enforcement towards resolution of that specific cases. Some of the lawyers has proposed the ideas for detection of cyber-crimes and give awareness to civil society so that the prevention may come into being. e.g. I have arranged meetings separately with lawyers those randomly belongs to Criminal, civil, trade Marketing domains. Mr. Thair (Barrister), Mr. Mian Muhammad Umer Shahzad (Advocate High Court), Mr. Sardar Abdul Qayyum (Advocate High Court). They have acute knowledge of internet computing and little about new tools/technologies. They are in practice more than ten years but still they don’t have any experience to lead any case which is being logged properly apart from some trade marketing related cases.

Software Houses

Software houses are the important part of cyber world. Software development companies are giving us support to interact with internet by applications being developed by them. It is noted that software houses are the place where an intellectual can make plan and execute the undesirable action may being caused for a fraudulent activity or cyber terrorism to be performed online. It is observed during a trip to software house that most of the
developers are working on to make some applications which may be used to detect viruses in order to save web documents from hackers/crackers.

Telecommunication Companies

There are different telecom operators exists in Pakistan e.g. Telenor Pakistan, Warid Telecom, Ufone (PTML), Mobilink, Zong (Chine Mobile), PTCL etc. All aforementioned companies belongs to cyber world generally. In context with the new trends of VAS (Value Added Services) they are facilitating their clients for their convenience. For this perspective they are promoting their business to be done online. Many of above said has commercially launched the financial services for electronic transactions to avail the opportunity to pay bills online, money transfer online etc. Periodic visits of the sale & service centers of these mobile operators arranged to know about the areas of FS (Financial Services). Through these visits we tried to find out fraudulent activities may be held in this new business. Further, we have explored the ground realities of making business online. It is observed that every operator is willing to provide better services to their clients as well as to enhance the business of company accordingly.

Randomly, we have selected the sales & service center of Telenor Pakistan at Faisalabad to find out the followings;

- Key areas of FS (Financial Services)
- Electronic Transaction fulfillment mechanism
- Instructions of PTA for online transactions with cell phone

While elements of Financial Services of Telenor Pakistan are mentioned below;

- Easy Paisa (Online money transfer)
- Online mobile phone’s bill payment
- Online bill payment (Utility bills)
- Branchless banking
- International remittance

By this kind of initiatives, the awareness regarding connecting online is increasing day by day. These starting points will be very helpful towards implementation and enforcement of the cyber laws. Now days other operators are following trends of Telenor Pakistan and converting business online in Pakistan. Its a very good sign.

Teachers & Students

Teachers & students are also the big part of cyber world. This academic related community can play a vital role for effective enforcement of cyber laws in Pakistan. What we can achieve by this community, is the awareness to the new students by giving them assignments to be the part of cyber world. It is being captured in survey that this community surely be suitable to implement and govern cyber law in stair of effective enforcement.

Randomly, the computer literacy and internet computing is being tested from several different communities and the findings are mentioned below;

Cyber Laws enforcement

After developing of any act or ordinance, important step is the enforcement of it. For the enforcement of act or ordinance government institutions are key entities. These law enforcement institutions have responsibility to implementation and enforcement of law in the country.

The term enforcement

“Local legal actions to attain fulfillment with law, rule or agreement and/or obtain penalties or criminal endorse for breach. This procedure may be different. its depending on the necessities of dissimilar environmental laws and related regulation of implementation..“

Enforcement of cyber law in Pakistan

In light of all afore mentioned discussion, though Pakistan has passed cyber-crime ordinances ETO 2002 & PECO 2007 but the facts shows the clear picture of poor enforcement of these acts in Pakistan. First of all if we talk about ETO 2002, this act only deals with all electronic transactions and do not cover all the cyber related crimes specifically. This act only covers the crimes related to banking sector, like ATM, online money launderings and credit card frauds.

Reasons of Poor Cyber Laws Enforcement

- Lack of computer literacy
- Unawareness of internet computing
- Lack of cyber world knowledge in judiciary
- Complaints logging mechanism of cyber crimes
- Enforcement institutions
- Detection of cyber crimes
- Process of investigation of cyber crime
- Legislation process of cyber crimes
- Unidentified jurisdiction

Lack of computer literacy

If we have look around the causes of poor enforcement of compliance of law & order of cyber related issues, the big reason that must be observed will be "lack of computer knowledge". Obviously, how nations can make a way into the global village without
having sound computer literacy? It means, knowledge about computer and cyber related devices, tools, techniques, technologies are compulsory to be the part of cyber world as well as important to understand the things related to enforcement of cyber law & order. As far as concern Pakistan, there is no solid arrangements has been made yet for this except to launch few computer courses at SSC level. It is also distinguished that in order to achieve high points towards the enforcement of cyber laws; the changes needs to be deployed at gross root level. So that in next 5 to 10 years the desired results can be met and the changes can be reflect. For this cause, the initiatives to be taken for computer literacy are discussed in this research report later.

Unawareness of internet computing

The second reason being caused for poor compliance of cyber law & order is unawareness of internet computing. For this, course contents of academics at different levels has been checked both in public and private sectors and found not well because neither there are basic courses offered nor some sort of special courses offered related to internet computing and learning too. Both the computer literacy & internet computing are significant accordingly. Other than academic society, only fewer organizations are taking part for utilization of computers and they are producing some refresher courses for their employees time to time as technology is changing its mass rapidly. The organizations are those who are following the international standards. It is found in domestic search at Faisalabad (also called the city of commerce), more than 80% of organization which are registered with the “Chamber of Commerce Faisalabad, Pakistan” are having the staff without computer literacy. Under these kinds of circumstances the results of proper enforcement of cyber law & order cannot be achieved in years to come.

Lack of cyber world knowledge in Judiciary

For hearing cyber related cases, the existence of separate special courts are required to manage and monitor the cases well. The lackness of computing and internet computing knowledge in judiciary is the big reason for resolution of cases, as for as concern the personnel those involved in trial of cyber case. It is being noted that the judiciary has insufficient knowledge that is the resistance for resolution of the case throughout.

Enforcement institutions

Not a single institute is found during this study that may cause of enforcement of cyber laws in Pakistan. Only FIA are dealing with the cyber related issues.

Detection of Cyber Crimes

Detection of cyber-crime is important process in terms of rectification of case. It is also being considered as 1st step to have good and solid enquiry. With respect to enforcement of cyber laws, there is no such technologies are there for investigations. Especially the law enforcement agencies are equipped with neither the computer education nor latest tools and technology to find the committed crime from cyber domain.

Process of Investigation of Cyber Crimes

The term investigation is directly interlinked with detection. Both are used to find the committed crime as well as to find out the ways for which said crime has been done. The investigation agencies for cyber-crimes needs to have access all related entities through which they can have reached to the blameworthy people.

Legislation Process of Cyber Crimes

Legislation for the laws to be implemented is the big problem being faced since Pakistan exists in the world. As per constitution of Pakistan, All the legislation will be done in parliament. The members of the parliament are the responsible for legislation of any law. This is very 1st time happened in general elections 2002 that all members of national assembly were graduate. Though, there were ‘graduate’ but all were failed to produce the legislation for cyber-crimes except they have made the ETO (Electronic Transaction Ordinance) in 2002 and PECO (Prevention of Electronic Crimes Ordinance). Keeping in view the literacy rate for computer knowledge and technology related education in the judiciary, lawyers and law enforcement agencies; is the obstacle to build an IT Act for Pakistan.

Unidentified Jurisdiction

Although the ETO, PECO is being implemented but Jurisdiction identification is also the big problem to deal with the cyber related cases. Due less knowledge of technology, the traditional courts are in conflict to separate the cyber related cases from civil and criminal cases. To avoid such kind of issues the separate courts must have exists to monitor only cyber related cases.

IV. RESULTS & DISCUSSION

According to the conducted survey a large number of people don’t go online for their work or different purpose. That is described in Fig 4.1. The ratio of such type of people is 38.5 %. And the people of using online systems on 2 to 4 hours daily are also in large number. It’s about 30.8%. But this ratio is less than the persons not using online systems. Remaining low using people are on average.
Although survey was conducted on well-educated people of the society (i.e. Lawyers, judges, Education sector, Law and Order Agencies etc.), but a large percentage of people even don’t know about cyber-crime. This percentage approaches to 38.5 as shown in Fig. 4.2. Then the majority of the people have a minimum knowledge about cyber-crimes. The people having excellent knowledge is very low i.e. only 11.55 as shown in Fig. 4.2. This situation is so much critical that even most of the people have never heard about cyber-crime. And this percentage is about 57.7% as shown in Fig 4.3. Since most of the people don’t know about cyber-crime, so a large number of people also don’t know about cyber laws working internationally and this percentage is 46.2%. Only a small number of people have excellent knowledge about cyber laws. i.e. 7.7% only as shown in Fig. 4.4 and hence same number of persons have excellent knowledge of Cyber Law in Pakistan as shown in Fig. 4.5.

The main reason for not having knowledge of such type of cyber-crimes is that most of the people have never suffered such type of crimes. These crimes can be included victimization of email regarding crimes, hacking, hacking of Debit/Credit cards and data stealing etc. A large percentage has never been victim of email regarding crimes i.e. 61.5% as shown in Fig 4.6. 50% of the people are not regular user of online systems and 46.2% have never faced hacking. Only 3.8% people have faced hacking as shown in Fig. 4.7. So these people have much knowledge about cyber crimes. 19.2% people among the people using online systems don’t use
debit/credit cards for online transactions and 76.9% people were never suffered hacking of their debit/credit card hacking. Only a small number of 3.8% people have suffered hacking of their debit/credit card hacking (Fig 4.8). Data of only 15.4% people have been stolen many times while using online system and 53.4% have never faced data stolen (Fig. 4.9).

All the above-given factors also affect the knowledge of registering complaints regarding cyber-crimes. 42.3% people don’t know how to register complaint about cyber-crime. 42.3% people don’t know how to register complaint of cyber-crime. 19.2% think that there is no such mechanism to register complaint and only 38.5% people who are using online systems, know the procedure to register the complaint about cyber-crime (Fig.4.10). And most of the people have never registered the complaint of cyber-crime. The reasons of not registering reports are

- Some people never suffered cyber crime
- Some people don’t know the process to register complaint.
- Some people have not proper response from judiciary or law enforcement agencies.

42.3% people have never suffered cyber-crimes, 53.9% people are unaware of the process of registering complaint and 3.8 have not proper response from judiciary and law and enforcement agencies when they previously registered their complaint of cyber-crime (Fig 4.11).
A large number of people don’t have knowledge of judicial infrastructure for cyber laws. i.e. 46.2% people don’t have knowledge about infrastructure and 19.2% people think that there is no such mechanism in Pakistan (Fig 4.12).

According to given facts and figures above it is analyzed that knowledge of cyber laws is dependent on the knowledge of law, Information technology and use of online systems. As Fig. 4.13 and Fig. 4.14 show the persons having excellent knowledge of Law also have good knowledge of cyber laws. But even there also a large number of such people also exists among these people that still don’t know the mechanism to register cyber-crimes. And this number is 42.3% .

26.9% people claims that they have knowledge to register complaint but they never registered complaint because they never suffered cyber-crime. And most of the people i.e. 42.3% don’t know how to register so they never registered crime. (Fig. 4.15)

Lawyers and Judges

When we see the persons involved in judicial infrastructure then it was seen that the persons in judicial infrastructure i.e. Judges and Lawyers, were also not having excellent knowledge about cyber-crimes and international laws about cyber-crimes. A large number i.e. 64% were unaware of international cyber laws. Only a small number 25.67% were having good enough knowledge about international cyber laws. This situation is represented in Fig 4.16. And this problem was also reflected in case of cyber law of Pakistan. Only a small number of 12.5% of Lawyers and Judges have well enough knowledge of cyber law in Pakistan (Fig 4.17).
Due to this unawareness of cyber laws Judges and lawyers have to face many problems during trial. Some of these problems are:

- Evidence Problems
- Knowledge of Technology Problem
- Discrepancies in Law
- Incompleteness of Law

In evidence during trial 75% of cases faced extreme problems in evidence as shown in Fig 4.18. Same as the knowledge of technology was also a major hurdle in case trial. Because lawyers and judges didn’t have technology knowledge. And in 75% of cases this problem was also faced extremely (Fig 4.19).

50% of the lawyers and judges faced very much problems during case trials due to discrepancies in existing cyber law in Pakistan (Fig 4.20). 50% of Lawyers and judges are of the view that there is extreme problem of incomplete law in Pakistan (Fig 4.21).
Facing all given problems the results of the cases were also not satisfactory. Only 25% cases were solved and decided satisfactorily. And a large number 50% of cases were unsolved and were referred to higher courts or some legislation authorities (Fig 4.22).

**Fig 4.21**
Problem of Incomplete law

**Fig 4.22**

**CONCLUSION**

In this study, it is being found that majority of the computer literate people not using the online systems. Ratio of these people is 38.5% while the same size of people has knowledge about cyber-crime. The fewer of them 12% have the sound knowledge of cyber-crimes at expert level. Research illustrate the almost 58% people those have not even heard about cyber related crimes. Near about half of the people 46.2% don’t have knowledge about cyber-crimes. Report mentioned the following reasons of not having knowledge related to cyber space i.e.

- A large number of people have not been suffered from cyber related crime due to unawareness of technology & mostly they are not been the part of internet more than 2-4 hours a day
- 50 % people not being online
- 46.2% never faced hacking, only 3.8% have been suffering from it

As per survey report, there is only a one minor unit of FIA (NR3C) is working on cyber-crime related crimes as well as the related complaints. The complaint logging procedure is not so simple and most of the people are not familiar with it. Even though, most of the people don’t know how to log complains against committed cyber-crime. The main reasons for lackness in reporting cyber-related queries are due to less knowledge of technology as well as the judicial infrastructure for cyber-crimes. There are many problems faced by lawyers and judges during trial for said cases such as digital evidence problem that has been resolved partially after the passed ordinance named as ETO 2002 (Electronic Transaction Ordinance) and less knowledge of technology. Discrepancies and incompleteness of cyber laws are also the main problems being faced by law enforcement agencies. Hence, due to these problems most of the cases are undecided or decided unsatisfactorily.

**References**