International Research Journal of Human Resources and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor- 5.414, Volume 4, Issue 9, September 2017
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

CYBER CRIME --- A CHALLENGE

Gulab Singh Dahiya, **LL.M**

Introduction

In today's e-Age, we are living e-life in Cyber World. E-Life means our existence & living in the cyber world. Since Computers & Internet are now an integral part of our personal & professional life causing every one of us as a constituting part of this cyber world. Just like any other invention, Computers & Internet are a boon to human kind if used in a right way and to the advantage of the society. However, as we all know, everything has its pros and cons and so computers & internet are not an exception. Today's Cyber Space is also flooded with crimes i.e. Cyber Crime which is also termed as Computer Crime, e-Crime, Hi-Tech Crime or Electronic Crime etc.

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment."Most of us are using internet and computers for online transactions where we transmit personal information and possibly do all type of transactions including monetary transactions. Everyone who works on a computer must be familiar with the term "Cyber Crime" which is nothing but acriminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime. Simply put, it is an activity which is generally criminal in nature, where a computer or network is the source, tool, target, or place of a crime. To say in one line, cybercrime refers to all the activities done with criminal intent in cyberspace.

Cyber Crimes in e-life are similar to conventional crimes like extortion, forgery etc. are being done with the help of computers; which most of us are using for online monetary transactions. Thus the concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Cyber crime can be found in the United Nations Manual on the Prevention and Control of Computer-Related Crime. The manual includes fraud, forgery, computer sabotage, unauthorised access and copying of computer programs as examples of cyber crime. In general cyber crime may be defined as unlawful acts wherein the computer is either a tool or target or both.

2.Types of cyber crime

The cyber crime may be broadly classified under the following four categories. They are

1) Against Individuals:-

(i) Email spoofing :A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

(ii) Spamming: Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

(iii) Cyber Defamation: This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

(iv) Harassment & Cyber stalking : Cyber Stalking Means following the moves of an individual's activity over internet. It can be done with the help of many protocols available such at e- mail, chat rooms, user net groups.

(2) Against Property:-

(i) Credit Card Fraud :

(ii) Intellectual Property crimes: These include Software piracy, illegal copying of programs, distribution of copies of software, Copyright infringement, Trademarks violations, Theft of computer source code etc

(iii) Internet time theft: The usage of the Internet hours by an unauthorized person which is actually paid by another person.

(3) Against Organization:

(i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms: a) Changing/deleting data-- Unauthorized changing of data.b) Computer voyeur-- The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service: When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack :A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing: Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack: When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb: Its an event dependent programme , as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse :an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

(4) Against Society:-

(i) Forgery: currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism: Use of computer resources to intimidate or coerce others.

(iii) Web Jacking: Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

In 'The Concept of Law' Hart has said that human beings are vulnerable so rule of law is required to protect them. Applying this to the cyberspace it can be said, "Computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime."

3.Reasons for the vulnerability of computers

Some of the reasons for the vulnerability of computers may be:-

1) **Storage Capacity** - The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.
2) **Easy to access**- The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
3) **Complexity**- The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
4) **No evidence**- Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.
5) **Negligency- Negligence** is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

The cyber world has enabled not only the use of computers and other communication tools as new weapons from which traditional crimes can be committed, but also the creation of new crimes brought about by the very existence of such technology. And for these new crimes, older legislative instruments have become inadequate and difficult to apply to such an environment. Developing countries have become ideal breeding grounds as well as targets for online criminals. This is mainly due to the fact that many of these countries are new to the online environment and

technology in general. This is added to the rapid development and proliferation of advanced technological tools, software and know-how through ICTS. Developed countries themselves have only started dealing with these issues in the past decade or so, and it is a fact that technology progresses at a much faster pace than legislative bodies and governmental authorities respond. It is therefore not surprising that many criminals seek haven in countries where cyber crime laws do not yet exist in order to commit criminal acts without fear of criminal sanctions. Consequently, the more immediate concern is to elaborate and implement legislation which will be able to deal with cyber crime appropriately. Several international conventions exist which already try to deal with these new, sometimes complex, issues and adopt an appropriate framework for them.

The United Nations Resolutions 55/63and 56/121 on Combating the Criminal Misuse of Information Technology (Annex 36) tried to address the problem of safe havens for those who criminally misuse information technologies by requesting that States put into place laws to eliminate such havens. Recommendations included increased cooperation in law enforcement during investigation and prosecution of computer-related crime, the protection of confidentiality, availability and integrity of computer systems from unauthorized impairment by the legal system. Preservation of data in investigations of such crimes was an important concern as well as fast access to such data and the penalization of criminal abuse. Two further Resolutions were adopted, Resolutions 57/239 and 58/199on the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure. The first Resolution focused principally on the need for States to take action domestically on nine goals: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management and Reassessment. The second Resolution noted the interdependence on information infrastructures with other sectors of global infrastructure critical for public services. The Annex to the Resolution listed different elements for protecting critical infrastructures. The Eleventh UN Congress on Crime and Prevention and Criminal Justice, which took place in April 2005, undertook a Workshop which looked at measures to combat computer-related crime. The Workshop report identified several different types of computer related crime and has tried to elaborate a conceptual model with regard to definitions of cyber crime. This included illegal criminal conduct in the case of crimes directed at computing and communication technologies themselves, crimes involving the use of digital technologies, as well as crimes involving the incidental use of computers with respect to the commission of other crimes, making the computer a source of digital evidence. Crimes that target ICTs include theft of telecommunications and computer services by using hacking techniques in order to gain unauthorized access, password cracking, digital cloning, and credit card fraud. Other conduct, such as denial of service attacks, can effectively crash servers and websites, but this has been dealt with under the availability chapter.

4. Indian Perspective

The **Indian parliament** considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on Trade Law. As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th May 2000. The preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934.The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000 and So that they may regulate and control the affairs of the cyber world in an effective manner.

Now a days *Hacking, destroying files and data through spreading virus and Ransomware are the largest number of offences in the cyber world.* Although Russia, China and Brazil are world leaders in cyber crime. India is fast emerging as a major hub of cyber crime, however our legal

system is already in place to tackle this menace of cyber crime and to control it and punish the guilty. Cyber Crime, which we may define as "an unlawful act wherein the computer is either a tool or a target or incidental to the crime", has both civil as well as criminal remedies.

So let's talk about the remedies available against such crimes. In India, the offence of Cyber Crime is covered under Information Technology Act 2000 and under the Indian Penal Code. Cyber Crime Cells have been established by law in major cities. These Cells function directly under the Commissioner of Police of respective cities. Cyber Crime Cells empowers any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act. Central Bureau of Investigation (CBI) already has a cyber crime wing operational since 1999.The Government has established "The Cyber Regulations Appellate Tribunal" under the Information Technology Act, 2000. The Tribunal has the same powers as are vested in a Civil Court for requiring the discovery and production of documents, receiving evidence on affidavits. But the decisions of the Tribunal can be contested by the High Court. The Information Technology Act not only applies to the offence committed in India, but it can also be used to bring offenders from foreign countries to India for trial.

The Information Technology Act deals with the various cyber crimes in chapters IX & XI. The important sections are Ss. 43 &65. Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. One Crore by way of remedy. Section 65 deals with 'tampering with computer source documents' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent and the following loopholes/drawbacks in the Act are observed -

1) **The Act did not served the desired purpose:** Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.
2) **Cyber Torts:** The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T.Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T.Act 2000 read with the Penal Code is capable of dealing with these felonies.
3) **Cyber crime in the Act is neither comprehensive nor exhaustive:** it is believed that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view held is that IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have

appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes. It is also felt that a new legislation on cyber crime is totally unwarranted. The reason is that the new legislation not come alone but will bring with it the same confusion, the same dissatisfaction and the same desire to supplant it by further new legislation. Further there are other legislations to deal with the intellectual property crimes on the cyber space such as the Patents Act, Copy Right Act, and Trade Marks Act.

4) **Ambiguity in the definitions: The** definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The infamous go2nextjob has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the netizens are till Sec 66 exists in its present form. Further section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by the BalBharati case.
5) **Uniform law:** It is held that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.
6) **Lack of awareness: One** important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling Microsoft pirated software over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for online cheating by buying Sony products using a stolen credit card.
7) **Jurisdiction issues: Jurisdiction** is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 is very silent on these issues.
8) **Extra territorial application: Though** S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.
9) **Raising a cyber army :**By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) 11) is definitely a welcome step in this direction.
10) **Cyber savvy bench :**Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. Mr T.K.Vishwanathan, member secretary, Law Commission, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated "if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System".

11) **Dynamic form of cyber crime: Speaking** on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind."The (de)creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.
12) **Hesitation to report offences: As** stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the Delhi time theft case. "The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business." This attitude of the administration is also revelled by incident that took place at MerrutandBelgam. For complete realisation of the provisions of this Act a cooperative police force is require.

To overcome the above drawbacks The Information Technology (Amendment) Act, 2008 was enacted in October 2009 with the following salient features.

The term "digital signature" has been replaced with "electronic signature" to make the Act more technology neutral. A new section has been inserted to define "communication device" to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image. A new section has been added to define "cyber café" as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public. There is an addition of several new offences into the Act. Section 66 has now been expanded to include sections 66A, (offensive messages) 66B, (Receiving stolen computer) 66C, (Identity theft), 66D (Impersonation), 66E (Voyeurism) and 66 F (Cyber Terrorism). Section 67 has been expanded to include Sections 67A (Sexually explicit content), 67 B (Child Pornography) etc.

5. Preventive Measures

It is rightly said that prevention is always better than cure. It is always better to take certain precaution while operating the internet. One should make them part of one's cyber life. The 5P mantra for online security is **Precaution, Prevention, Protection, Preservation and Perseverance**. An internet user should keep in mind the following things-

1) To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2) Never send your credit card number to any site that is not secured, to guard against frauds.
3) Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
4) Use of firewalls may be beneficial.
5) It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
6) Always use latest and updated antivirus software to guard against virus attacks.
7) Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
8) Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

9) Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

10) Web servers running public sites must be physically separate protected from internal corporate network.

With all new wonders, come new worries. The internet is no exception. In just over a decade, this technological miracle has brought societies the world over closer together than in the whole history of international relations. Unfortunately, this has meant that disruption of its infrastructure will have a global effect. With the use of encryption technologies, electronic signatures have become binding on contractual documents. Cryptographic techniques such as the Public Key Infrastructure have become one of the most reliable technologies to date for authenticating individuals. This form of electronic signature has become internationally recognized, with involvement by the United Nations with the UNCITRAL Model Lawon Electronic Signatures of 2001. Encryption technologies also help secure confidentiality of communication, for contractual and noncontractual communication alike. Cybercrime has also taken on a global scale, with criminals basing themselves in countries with little or no legislation against cybercrime. Countries should be aware, however, that, with the current pace of technological developments, the international dimension of cybercrime, and consequently of cyber security, is yet unchartered. The targets of attacks affect the whole of the internet. Developing countries are the most concerned with this. Lack of security can and will effectively spoil the benefits of the internet, both on an economic and governmental scale. Law enforcement and national security must also play a determining role. But ensuring security in cyberspace will require an international law enforcement effort. It will also be imperative that countries cooperate with each other, and that real efforts are made to assist developing countries, which often lack experience and legal knowledge on this front. It is vital that countries do not underestimate the importance of curbing the cyber crimes and securing cyberspace if the internet is to flourish to its full capacity, bestowingits benefits on a global scale.

6.Bibliography ---

Nagpal R. – What is Cyber Crime

Duggal Pawan - Cybercrime

The Information Technology Act 2000 - Bare Act

The Information Technology (Amendment) Act, 2008 – Bare act

Digit Monthly Magazine ---