Information Technology and Cyber Law: A Globalized Review

Mr. Rajib Bhattacharyya[1]

I. Introduction & the Concept

In the today's era of rapid growth,[2] Information technology is encompassing all walks of life all over the world. These technological developments have made the transition from paper to paperless transactions possible. We are now creating new standards of speed, efficiency, and accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. Computers are extensively used to store confidential data of political, social, economic or personal nature bringing immense benefit to the society.

"Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek word for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.[3]

The growth of Electronic Commerce[4] has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic

[1]*B.A, LL.B; LL.M, CCL, DEM, DHR, PGDBO)Assistant Professor, University Law College, Gauhati University, Guwahati- 14, Assam, India E-mail: bhattacharyya.rajib@gmail.com*

[2] Cyber Laws: A Global Perspective Manish Lunker, available on http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005846.pdf, last visited on dated 28.03.2016 at about 8.30 P.M

[3]Overview of Cyber Laws in India, available on http://www.caaa.in/Image/cyber%20laws%20overview.pdf, last visited on dated 28.03.2016 at about 4 P.M

[4] Id.

Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law.

Cyber law[5] is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

Cyber law encompasses laws relating to:[6]

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology which we have discussed above. In short, cyber law is the law governing computers and the internet crimes.[7]

Cyber Legislation[8] World Wide Different countries have had their own experiences while framing and implementing cyber laws. Some early adopters in the US and the West in general, had come up with their own legislations in this regard by either adapting their existing laws in the context of cyberspace or creating new laws in respect thereof. Following their footsteps, the developing countries such as India, Pakistan, Indonesia, Malaysia, and Philippines have also enacted cyber law legislations. By and large, there are many complex legal issues that the law enforcement

[5] Ibid.
[6] Id.
[7] Cyber Crime and Cyber Law in India: An Analysis PrabhashDalei and TannyaBrahme, International Journal of Humanities and Applied Sciences (IJHAS) Vol. 2, No. 4, 2013 ISSN 2277 – 4386 106, available on http://journalsweb.org/siteadmin/upload/49474%20IJHAS024054.pdf, last visited on dated 26.04.2016 at about 8 P.M
[8] Id.

agencies of different countries have witnessed from time to time and still remain unresolved. The legislators of cyberspace law have faced peculiar obstacles in adapting the legal principles of the traditional legal systems in context of cyberspace.

The Union Cabinet[9] has in September 2012, approved the National Policy on Information Technology 2012. The Policy aims to leverage Information & Communication Technology (ICT) to address the country's economic and developmental challenges. The vision of the Policy is "to strengthen and enhance India's position as the Global IT hub and to use IT and cyber space as an engine for rapid, inclusive and substantial growth in the national economy".

II. The Genesis of IT legislation in India[10]

Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

---

[9] Ibid.

[10] Cyber Laws in India, available on http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf, last visited on dated 28.03.2016 at about 9 P.M

III. Objectives of I.T. legislation in India[11]

It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself.

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9th June and was made effective from 17th October 2000.

The Act essentially deals with the following issues:

_ Legal Recognition of Electronic Documents
_ Legal Recognition of Digital Signatures
_ Offenses and Contraventions
_ Justice Dispensation Systems for cyber crimes.

IV. Amendment Act 2008[12]

Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.

[11] Id.
[12] Ibid.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003- 04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analysed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

_ Focussing on data privacy

_ Focussing on Information Security

_ Defining cyber café

_ Making digital signature technology neutral

_ Defining reasonable security practices to be followed by corporate

_ Redefining the role of intermediaries

_ Recognising the role of Indian Computer Emergency Response Team

_ Inclusion of some additional cyber-crimes like child pornography and cyber terrorism

_ authorizing an Inspector to investigate cyber offences

V. Legislations in other Nations[13]

As against the lone legislation ITA and ITAA in India, in many other nations globally, there are many legislations governing e-commerce and cyber-crimes going into all the facets of cyber-crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in

[13] Ibid.

the particular area focused in the Act. In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. Companies dealing with US firms ensure HIPAA compliance insofar as the data relating to such corporate are handled by them. The Sarbanes-Oxley Act (SOX) signed into law in 2002 and named after its authors Senator Paul Sarbanes and Representative Paul Oxley, mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Besides, there are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, Children's Online Privacy Protection Act etc. In the UK, the Data Protection Act and the Privacy and Electronic Communications Regulations etc. are all regulatory legislations already existing in the area of information security and cyber-crime prevention, besides cyber-crime law passed recently in August 2011. Similarly, we have cyber-crime legislations and other rules and regulations in other nations.

VI. Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.[14]

1. Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.
2. Cyberspace has complete **disrespect for jurisdictional boundaries**. A person in India could break into a bank'selectronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

[14] Introduction to Indian Cyber Law, This document is an extract from the book IPR & Cyberspace – Indian Perspective authored by RohasNagpal. This book is available as courseware for the Diploma in Cyber Law and PG Program in Cyber Law conducted by Asian School of Cyber Laws, available on https://dict.mizoram.gov.in/uploads/attachments/cyber_crime/intro-indian-cyber-law.pdf, last visited on dated 28.03.2016 at about 8 P.M

3. Cyberspace handles **gigantic traffic volumes every second**. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace is absolutely **open to participation by all**. A tenyear- old in Bhutan can have a live chat session with an eightyear- old in Bali without any regard for the distance or the anonymity between them.

5. Cyberspace offers **enormous potential for anonymity** to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

6. Cyberspace offers never-seen-before **economic efficiency**. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

7. Electronic information has become the main object of cyber-crime. It is characterized by **extreme mobility**, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

8. A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release.

9. **Theft of** corporeal **information** (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions.

However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.

VII. Cyber Law: The Position in India

Firstly, India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is The Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the

Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and so on. However, the arrival of Internet signalled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. Despite the brilliant acumen of our master draftsmen, the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous ticklish legal issues and problems which necessitated the enactment of Cyber laws.[15]

Secondly, the existing laws of India,[16] even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence, the need for enactment of relevant cyber laws.

Thirdly, none of the existing laws[17] gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

Fourthly, Internet requires[18] an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet,

[15] Supra Note 4
[16] Ibid.
[17] Id.
[18] Ibid.

can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth.

All these[19] and other varied considerations created a conducive atmosphere for the need for enacting relevant cyber laws in India.

VII. History of cyber law in India[20]

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, ofthe various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft.

After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber-crime and to facilitate speedy locating of a cyber-criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft. The Union Cabinet approved the bill on May 13,

[19] Id.
[20] Id.

2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.

With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

VIII. Cyber Crimes / Cyber Frauds[21]

The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life.

Fraud is the intentional deception of a person or group for the purpose of stealing property or money. Internet fraud includes any scheme using Web sites, chat rooms, and email to offer nonexistent goods and services to consumers or to communicate false information to consumers. Customers then pay for the fraudulent goods over the Internet with their credit cards. Internet fraud involves a wide variety of schemes limited only by the imagination and creativity of a seller intent on deceiving a buyer. A few general characteristics one can find in all cyber scams. Most scams are done by e-mail. They entice users to give them critical information like usernames, passwords, credit card information, or other types of account information.

[21] Ibid.

Cyber fraud has the potential of hindering the economic and social development of any nation. This is because among other dire consequences, foreign investment is seriously discouraged. Cyber fraud can also destroy our good and morally sound culture. This is because the youth will no longer work but resort to that means to earn their living.

VIII.I. Definition of cyber crime[22]

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

The OECD Recommendations of 1986 included a working definition as a basis for the study: Computer-related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.

VIII.II. Cyber frauds in India[23]

According to Norton Cybercrime Report 2012, 66% of Indian online adults have been a victim of cyber fraud in their lifetime. In the past 12 months, 56% of online adults in India have experienced cyber fraud. As per the report, at least 1,15,000 people fall prey to cyber fraud every day, while 80 per minute and more than one per second leading to a rise in the average direct financial cost per victim to around Rs10,500.

[22] Ibid.
[23] Id.

According to the survey, the cybercriminals have now shifted their focus to the increasingly popular social platforms. One in three adults online Indians (32%) have been either social or mobile cybercrime victims.

While most internet users delete suspicious emails and are careful with their personal details online. However, 25% don't use complex passwords or change their passwords frequently and 38% do not check for the padlock symbol in the browser before entering sensitive personal information.

Online adults are also unaware of the evolution of most common forms of cybercrime. In fact, 68% of adults do not know that malware can operate in a discreet fashion, making it hard to know if a computer has been compromised, and one third (35%) are not certain that their computer is currently clean and free of viruses.

VIII.III. Preventive measures[24]

The first line of defense to prevent online consumers from becoming online victims is good education. Tips on the major forms of Internet fraud and how to combat them have been developed by public authorities, enforcement agencies, and the private sector on various platforms such as government websites, brochures, posters, videos, reports, etc. The International Consumer Protection and Enforcement Network (ICPEN), an informal network of enforcement authorities from OECD and other countries, has launched Fraud Prevention Month, an awareness campaign taking place on a designated month every year. The private sector also offers a number of technical tools to provide consumers with real-time protection against cyber fraud. For example, business has developed means to counter spam messages, which are a significant source of fraud, through authentication, filters, and listings. Likewise, anti-phishing systems have been put in place allowing Internet users to report phishing sites and block them.

Preventive measures to be taken by corporates to protect their businesses –

- Setup an e-security program for your business.

[24] Ibid.

- Ensure your security program facilitates confidentiality, integrity and availability.
- Identify the sources of threats to your data from both internal and external sources. Examples: disgruntled employees - leaving bugs behind in your system, hackers looking to steal confidential information.
- The security program that you create for your business must have provisions to maintenance and upgrades of your systems.
- Administrators have access to all files and data. Therefore, one must be mindful of who is guarding the guards.
- Roles for security should be defined, documented, and implemented forboth your company and external contractors.
- Establish a security awareness program for all users. Content should be communicated in non-technical terms. This could include briefings, posters, clauses in employee contracts, security awareness days etc.
- Implement security training for technical staff that is focused on the security controls for their particular technical areas.
- Maintain logs of all possible activities that may occur on your system. System records must note who was using the system, when, for how long, deletions etc.
- User accounts should not be shared. User authorization should be mandatory. Employees should only be able to see information that they are authorized to see.
- Employee user accounts must be disabled or removed when no longer needed. Example: in case an employee leaves the company.
- Ensure network security from external sources by installing firewalls and intrusion detection systems.
- Allow remote access to employees only through secure communication channels like SSL or VPN.

- Install antivirus software on all desktops and servers. Buy Anti-Virus software solutions that allow real time upgrading of systems with antivirus patches.
- Create a data backup and disaster recovery plan in case of unforeseen natural calamities.
- Ensure back-up procedures are in place and tested.
- Ensure back-up procedures include all the critical as well as back office data such as finance, payroll etc.
- Incident response is the ability to identify, evaluate, raise and address negative computer related security events.
- In case of an incident, do not panic, and continue to save logs.
- Incident response - Take a backup of the affected system and notify the authorities.

The draft National Cyber Security Policy of India has been prepared by CERT-In. The policy is intended to cater to a broad spectrum of ICT users and providers including Government and non-Government entities. Besides this CERT-In in coordination with MHA, NIC and other stakeholders prepared and circulated Computer security guidelines and procedures for implementation across all Central Government Ministries/Departments.

VIII.IV. Types of Cyber crimes[25]

Some types of cyber crimes found in India are:

1. Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). (Delhi Public School case)

2. Sale of illegal articles:

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by

[25] Ibid.

using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

3. Online gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported. Whether these sites have any relationship with drug trafficking is yet to be explored.

4. Intellectual Property crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cyber squatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.

5. Email spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Gauri, her friends could take offence and relationships could be spoiled for life.

6. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business

involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates. Some of the students are caught but this is very rare phenomenon.

7. 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 to all of that person's friends.

8. Cyber stalking
The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

9. Unauthorized access to computer systems or networks
This activity is commonly referred to as hacking. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". However, as per Indian law, unauthorized access does occur, if hacking has taken place. An active hackers' group, led by one "Dr. Nuker", who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

10. Theft of information contained in electronic form
This includes information stored in computer hard disks, removable storage media etc.

11. Email bombing
Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

12. 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.

Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

13. Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

14. Denial of Service attack

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

15. Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

16. Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

17. Trojan attacks

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

18. Internet time theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours.

19. Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

20. Theft of computer system

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system

This crime is committed by physically damaging a computer or its peripherals.

This is just a list of the known crimes in the cyber world. The unknown crimes might be far ahead of these, since the lawbreakers are always one-step ahead of lawmakers.

IX. Concluding Remarks

The conclusion may,[26] therefore, be drawn that computer-related crime is a real, (at least in respect of certain offences) expanding phenomenon. Furthermore, a steady increase in number of such crimes in this area is expected which demands for greater attention of lawmakers. Let's now once again review the alternatives available for establishing a comprehensive legal framework. Can we make only territorial laws applicable to online activities that have no relevant or perhaps even determinable geographic location? It seems to be very difficult. We must also allow responsible participants on the Internet to set their own rules and

[26] Supra Note 1

to help all concerned (online and offline). The law of the Internet has already emerged, and we believe can continue to emerge with individual users voting to join the particular systems they find most congenial. However, this model also does not solve all problems, and various governance issues cannot be resolved overnight. We will need to redefine Cyber Legal processes in this new dynamic context. Finally, the Cyber Law defined as a thoughtful group conversation about core values and distinct benefits to the Society will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically defined territories.

To sum up,[27] every stakeholder should be aware of and actively involved in preventing and solving together the *destructive* side of ICTs - i.e., cyber-crimes - with an appropriate balance between regulations and self-regulations subject to the different types of crimes in cyber-space, in order to optimize more *creative* side or benefits of ICTs, which will further transform the paradigms of our cultures, politics, and socio-economy beyond national jurisdictions in the interconnected world today.

[27]Information Technology in Developing Countries, available on http://www.iimahd.ernet.in/egov/ifip/dec2004/dec2004.pdf, last visited on dated 28.03.2016 at about 8.45 P.M