Chapter III

Emerging International Cyber Law Regime
CHAPTER III

EMERGING INTERNATIONAL CYBERLAW REGIME

The rapid development in computer technology and internet has brought us in the midst of an unprecedented information revolution, which has simplified the storage and access to information and dismantled the constraints of distance and time in communication. The last decade of 20th century had witnessed information technology emerge as the most prominent technology which has had a revolutionary effect on the lives of the people across the world so much that the world has literally became a global village. There is no such period in the human history with such an innovation that has produced such incredible and significant changes in all walks of human life such as social, political, economic, cultural, military strategic operations, policing, academics, medicine, engineering, space navigation etc. The internet is an ideal delivery vehicle for providing each and every kind of information.

Thus, all spheres of human activities in modern world are being governed by the cyberspace. The internet has changed irreversibly the economic landscape and the fundamental assumptions on which the business of different kinds is based. It has connected each and every computer with each other and thus, has derecognized the geographical and political boundaries. The global electronic communications have created new spaces which require the new sets of rules to govern the cyberspace. The new sets of rules have become all the more important not only for governing the human transaction and economies at the global level but to prevent and combat the cyber crime. Since the use of the new technology to commit traditional crimes in not a new phenomenon since every new advancement in technology have always provided the
wrongdoers new means for engaging in unlawful conduct. The cyber space is not different in this manner and is simply a new medium through which new and traditional crimes are committed, albeit through the use computer systems with unprecedented speed and on a far-reaching scale.

This state of affairs, operating through the computer system, gave rise to the problem of cyber crime that has assumed gigantic proportions and has posed a challenge for the entire world. It has created an entirely new set of problems for legislative bodies and the law enforcement agencies all over the world. It has equally become a cause of serious concern legal fraternity to find effective ways and means to combat cyber criminality because of its wide and far reaching devastative effects.

Computer and Internet usage is on the rise due to lower costs of computer ownership and connectivity as well as faster and easier accessibility. As it is another mode of commercial and personal transaction and one that is heavily dependent on interaction through computers and automatic agents rather than face-to-face meetings, which increases distance and allows anonymity, it is another avenue for crimes to perpetuate.

“Computer Crime” encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism. “Cyber Crime” describes criminal activities committed through the use of electronic communications media. One of the greatest concerns is with regard to cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology. There are also many other forms of criminal behaviour perpetrated through the use of information technology such as
harassment, defamation, pornography, cyber terrorism, industrial espionage and some regulatory offences.¹

The existing criminal laws in most countries can and do cover computer-related crimes or electronically perpetrated crimes. Offences against the computer are relatively new as they arise from and in relation to the digital age, which threatens the functionality of the computer as an asset of a borderless information society. New laws are required in order to nurture and protect an orderly and vibrant digital environment. Offences through the use of computers merely constitute new ways to commit traditional offences using the electronic medium as a tool. In this case, existing legislation may not be suitable or adequate for several reasons; for example, the language in criminal statutes may not apply, jurisdictional issues may arise and punishments may not be appropriate.

The selection of the three jurisdictions as the subject of study is meant to provide a taste of the challenges facing different sovereign entities with their unique blend of political, social, cultural and economic personalities. It allows a comparison of the treatment of laws by a federation of states on the one hand and unitary states on the other, and of the contrasting approaches between western and Asian as well as older and newer nations.²

This will be set against a common law backdrop, as these countries share similar legal systems and historical ties, and considered in the context of nations with developed information technology infrastructure. They will also provide a good springboard to assess the current trends in domestic crime prevention initiatives and in regional and global approaches to evaluate the current weaknesses in global response as well

¹ Sood Vivek, Cyber Law, P. 81
² Das gupta, S.N., Cyber Crimes in India, P. 201
as to extract some suggestions to better the international criminal regime relating to electronically perpetrated crimes, which knows and respects no boundaries.

Because of the breadth of electronically perpetrated crimes and the depth to which an analysis of each type of crime can plume, the case study focus of this paper will be centered only on one of the most prominent form of crime that is relevant to both computer and cyber crime laws - Cyber-fraud and identity theft - through the act of what is commonly known as “phishing” and its progeny. The offence is also a useful case study as it is a ‘universal offence’ which is capable of uniform treatment, and that makes it a worthy subject for a good comparative study. “Phishing” is a term coined by the relatively new form of modus operandi by which scams are perpetrated through the Internet.

It involves the theft of the identity of a target organization (the secondary target) for the purpose of stealing the identities of its users or customers (the primary target) without their knowledge or consent (i.e. a series of identity theft). This is done through the use of professional-looking, HTML-based e-mails that include company logos, font styles, colours, graphics, and other elements to successfully spoof the supposed sender (i.e. constituting fraudulent conduct). Most also contain a

3. Moreover, cyber-fraud and identity theft is probably the biggest threat to electronic transactions (in particular, commercial transactions) today and it is the basis to many computer-related offences as well as other concerns relating to electronic transactions such as privacy and data protection, and the protection of intellectual property rights.

4. In contrast, for example, ‘content’ related offences such as obscenity legislation and defamation laws are susceptible to a range and variety of treatment in different jurisdictions depending on the political and socio-cultural personality of the nation. Hence they are less useful as subject matters of a fair comparison of laws. See, e.g., Sofya Peysakhovich, Virtual Child Pornography: Why American and British Laws Are At Odds With Each Other, 14 Alb. L.J. Sci. & Tech. 799 (2004); Katherine S. Williams, Child-Pornography and Regulation of the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations, 41 Brandeis L.J. 463 (2003); and Dina I. Oddis, Combating Child Pornography on the Internet: The Council of Europe’s Convention on Cybercrime, 16 Temp. Int’l & Comp. L.J. 477 (2002). Moreover, and this will be relevant later on in this paper, they are also less likely to be the subject of a universally harmonized legal response in the form of a widely subscribed treaty or of a consistently adopted model law. However, there are other approaches to dealing with such offences in as consistent a manner as possible.
hyperlink to a web site, which is almost always an exact replica of the spoofed site, to lure users or consumers into a false sense of security and into relaying their personal information. The motive may be purely pecuniary but not always necessarily so. Also, the approach may be similar, but the *modus operandi* has since mutated and taken on many innovative forms. Hence, the type of offence that may be implicated can vary and can constitute a computer crime, a cyber crime, or both.

A. Concrete Global Development

Many countries across the world have enacted their own criminal laws, computer laws, information technology laws and intellectual property laws etc. to prevent and combat the cyber criminality. But in view of the international dimension of cyber crime, the problem of jurisdiction arose particularly where the nationals or corporations of two or more than two countries were involved in the crime or where the criminal belongs to a different nationality and the crime was committed in a different country. The crucial problem, therefore, is that the law of which country is to be applied to resolve the dispute or to try the criminal(s), particularly when there is a variation in the cyber laws and penal laws of different countries. Internet being a vast global network of computers and the feasibility of the cyber criminals to perpetrate the crime from one destination and committing the crime at other destination with anonymity urgently requires development of a universal and uniform law governing and regulating the cyberspace transactions to resolve the issues of cyber criminality by mitigating the jurisdictional problem and the conflict of laws. The ever increasing phenomenon of cyber crime calls for immediate concerted efforts on the part all the countries, institutions, industries, technocrats and jurists alike to come up with universally uniform law so that the common criminals of mankind may be tried and
punished without the legal and jurisdictional hassles. In this direction the international community is taking the resolute efforts to address the problem of international cyber criminality.

Internet operations being of global nature that do not recognize any geographical and political boundaries enables the cyber criminals to operate beyond the national boundaries without being physically present at the scene of crime. The problem of cyber crime, therefore, calls for greater international support and co-operation. Though much has been done by the United Nations to muster co-operation of member nations to tackle the problem of cyber criminality as a common cause, the response from them has not really been very encouraging excepting that there is a general consensus among the countries that where a cyber crime involving country or countries are involved, trans-border assistance and co-operation between the concerned countries is the only viable alternative to prevent and control such crimes.\(^5\)

Global development in this direction began with the 12\(^{th}\) Conference of the Directors of “Criminological Research Institutes” of the Council of Europe, which discussed computer related crimes for the first time in 1976. As a sequel to this conference, the Select Committee of the Council of Europe on economic Crime conducted a study of economic crime in general and made its recommendations on the same. In 1983, the Organization for European Co-operation and development (OECD) undertook a study on the harmonization of international criminal laws, which resulted into the publication of the report entitled “Computer Related Crime – Analysis of Legal Policy” in 1986.\(^6\) The Report recommended a list of computer crimes that countries should consider prohibiting and penalizing by means of legislation:

---

\(^5\) 66th UN General Assembly Conference of the Interpol held in New Delhi in October, 1997.  
1. The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value;

2. The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;

3. The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;

4. The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put in on the market;

5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions."

Subsequently, the Council of Europe initiated its own study on computer crime with a view to evolve guidelines to help legislators determine the nature and nuances of computer related crime.\(^7\) The Committee of Ministers, of the Council of Europe accepted these recommendations in September 1989. The business transactions are now being carried on in the cyberspace through the nets and the online transactions have opened new vistas for unscrupulous cyber criminals to defraud and cheat the genuine businessmen and consumers. In view of the

\(^7\) Suresh T. Vishwanathan, “The Indian Cyberlaw”, at 104 (2001)
growing menace of cyber crime, the United Nations Congress in its 13th Plenary Session held in 1986, adopted a resolution calling up member States to intensify their efforts to combat cyber crimes through adequate legal measures.

1. **International de droit Ponel Conference in Germany (1992)**

The Association Internationale Droit Ponel (ADIP) held the collegiums on ‘Computer Crime and Other Crimes against Information Technology’ in Wartzburg (Germany). Its report stated that only 5% computer crimes were being reported to police. The factors contributing to non-disclosure of cyber crimes according to this report were as follows:

(i). Operational speed and storage capacity of computer hardware makes criminal activity very difficult to detect

(ii). The law enforcement agencies lack the necessary technological expertise to deal with cyber crimes

(iii). Victims of these crimes are themselves hesitant in reporting the crime to the police as they apprehend unnecessary harassment and waste of time and money in this fruitless endeavour

(iv). The fear of adverse publicity also dissuades the victim from reporting the crime

(v). Loss of goodwill, public confidence, investor’s faith or embarrassment etc. are also some of the factors responsible for non-reporting of cyber crimes.

2. **Twenty-Second G-7 Summit on Cybercrime (1996)**

The member nations at the G-7 Summit on Terrorism held in Leon (France) in July, 1996 resolved to accelerate mutual consultations and co-

---

8 The G-7 countries consist of Canada, France, Germany, Italy, Japan, UK and USA.
operation through appropriate bilateral and multilateral meetings on encryption that allows, when necessary, lawful government access to data and communications in order to prevent or investigate acts of cyber terrorism while protecting the privacy of legitimate communications.\(^9\) The member nations also emphasized the need to encourage non-member countries to recognize the guidelines laid down by the G-7 Summit in view of the global nature of information and communication networks. The focus of deliberation was on protection of security of information systems, privacy of personal data and protection of intellectual property rights of the people.

In order to raise awareness about the menace of cybercrime and to encourage countries to address this problem in the global perspective, efforts were made to provide necessary training through international law enforcement academies in Budapest, Hungry, Bangkok, Thailand etc. Besides this, The US National Infrastructure Protection Centre also organized workshops with other nations to share information on techniques of preventing cyber intrusions.\(^10\) A Cybercrime Conference was held in New Orleans in September, 1999 to provide training to law enforcement officials of different countries.


The menace of cybercrime has adversely affected almost all the countries of the world; therefore, a G-8 Hi-Tech Crime Sub-Group was formed in March, 1998 as a resolute move in the direction of international co-operation program to combat cybercrime. The Sub-Group organizes international conferences in order to review the legal system of G-8 countries to provide trans-border access to stored data and assistance in

---

hi-tech crime investigations which involve illegal alteration or distribution of electronic evidence. Each of the G-8 country has established a point of contact for law enforcement agencies to facilitate exchange of information regarding cybercrime access to its borders.

Since the cybercrime has made deep perversions in the form of fraud with its various dimensions that victimizes the commercial sector by subjecting them to irreparable losses, therefore, a G-8 Sub-Group Conference was convened in Paris, France in 1998 in which the representatives of industries and consumer groups participated to deliberate on the problems of the security of the internet affecting industrial and consumer establishments and to provide for a safe and secure environment for e-commerce, which the easy target of cybercriminals.

On the advent of a large number of cyber crimes, many nations have felt the need to have some control mechanism. In order to combat the challenges posed by cybercrime, many countries have beefed themselves up against such crime. A number of countries have introduced extensive amendments to their substantive criminal law.


A three day Cyber Crime Conference was held in Paris in May, 2000 which was attended by approximately 300 delegates including judges, police officials, diplomats, legal experts, leading businessmen and industrialists from G-8 countries. The conference stressed on the desirability of a global law to tackle the hackers, software pirates, crooks and virus attackers who were making the life of internet users miserable. The members unanimously agreed that there was a need for an international convention to deliberate on cyber crime related issues and urgency of setting up an International Criminal Tribunal having global
jurisdiction to deal with cyber crime and criminals. It was further resolved that the nature of cyber crime demands that the concerned countries should actively cooperate and coordinate in the investigation and prosecution of these hi-tech crimes regardless of their territorial boundaries. There should be prompt exchange of evidence in case of cross-country cyber crimes. Therefore, all efforts should be made by the member nations to initiate measures for security of networks on priority basis.

5. Internet Treaty by Council of Europe (2001)

Ever since 1980’s the Council of Europe had been working to address the growing international concern over the threats posed by hacking and other computer related crimes. All the member States of the Council of Europe unanimously resolved that international partnership to eliminate cyber crimes must be genuine, mutual and cooperative in order to meet the ultimate goal of tackling the problem of vulnerability of internet infrastructure.

According to Council of Europe, there are following three major challenges in maintaining internet security:

(i) Technical challenges that hamper the ability of law enforcement agencies to locate and prosecute cyber criminals that operate online.

(ii) Need for a change in certain substantive and procedural laws that have not kept pace with the changing technology, creating legal challenges to effective prosecution of criminals operating in cyberspace.
(iii) Infrastructural needs to enhance the capability and ability of law enforcement agencies to keep pace with changing technology with emphasis on training the people to fight cyber criminality.

A new internet treaty was contemplated by the Council of Europe\textsuperscript{11} in 1997 which was enforced in the form of a document in 2001. The treaty sought to control internet crimes by requiring participating nations to create a specific uniform body of laws to deal with unauthorized access, internet frauds and forgery, child pornography, copyright infringements etc.

The treaty of Council of Europe suggested measures which could control cyber crime activities at the global level. The treaty was entitled to be called the ‘International Convention on Cyber Crime’ and it was focused on the harmonization of national laws, which defines cyber crimes; delineating the procedure of investigation and prosecution to cope up with global networks and; the establishment of a rapid and effective system of international co-operation to combat cyber crime.


Another significant achievement in the direction of working out a uniform cyber law at the international level was the European Convention on Cyber Crime held in Budapest on November 23, 2001. This Convention was held for considering the changes brought about by the digitalization, convergence and continuing globalization of computer networks and the risks these computer networks and electronic information were creating in the form of modes and methods for the perpetration of cyber crimes.

\textsuperscript{11} Council of Europe (COE) is a 43 nations Alliance with US, Canada & Japan as the participating observes.
Recognizing the urgency for pursuing a common criminal policy aimed at protection of society against cyber crimes and desirability of cooperation between different nations, the convention drew up a comprehensive text of treaty comprising 48 Articles, divided into four chapters. The legal provisions of the European Convention have served as a model framework for the subsequent development of law on cyber crimes and preventive strategies through various international forums.


The European community has adopted the Directive on Electronic Commerce\(^{12}\) containing set of rules which lay down the standards that will apply to various online intermediaries for their involvement in illegal or infringing material put on their internet facilities by third parties.

There are different types of storage by an intermediary namely, mere conduit, proxy catching and hosting.\(^{13}\) The member states cannot impose upon online intermediaries an obligation to monitor the information which they transit or store, nor can member states require intermediaries to seek facts or circumstances indicating illegal activity.\(^{14}\)

The priority of the European Commission during 2007-07 has been on responding to the threat posed by cyber crime in various forms such as phishing, Trojan horses and spamming which affect all economic sectors and call for urgent actions. The Commission has laid greater stress on development of R & D as also the legal and economic initiatives to enhance information security.

---


\(^{13}\) European E-Commerce Directive, 2000; Article 13 distinguishes between 3 types of storage as follows:

a. Storage for the purpose of carrying out transmissions is known as ‘conduits’.

b. Storage for the purpose of making more efficient the transmission of information onwards is called ‘proxy caching’.

c. Storage of information provided by a subscriber is known as ‘hosting’.

\(^{14}\) Ibid., Article 15

An International Conference on E-security, Cyber Crime and Law was held in Chandigarh (India) on 19-20 February, 2004. The main issues for deliberation in the Conference included:

(i) Network security for corporate governance and industrial intrusions as also the hacking liability of network providers, which needed to be looked into with a fresh approach.

(ii) Data and transmission standards and encryption methods needed to be improvised. The electronic fund transfer and security of data banking was also taken up for discussion in the conference.

(iii) Issues related to computer forensics, preservation of computer evidence and methods to be adopted by the police to procure evidence required re-orientation and adequate attention.

(iv) Cyber law, data protection and need for appropriate legislation for the purpose were highlighted by the delegates. The issues like policing the cyberspace, role of judiciary in digital age, network security and law and public participation in prevention of cyber crimes were also extensively discussed in the conference.


An International Conference was organized by the Computer Crime Research Centre in collaboration with the World Anti- Criminal and Anti-Terrorist Forum at the Zaporozhe State University, Ukraine on May 26-28, 2004. The issues taken up for deliberation in the Conference included cyber terrorism, fight against cyber crime, IPR violations, piracy and legal aspects of information security.
10. ASEAN Regional Forum (2004)

The Association of South East Asian Nations (ASEAN) held a high level ministerial meeting on trans-national crimes in Bangkok (China) on January 8, 2004 recognizing the need for an effective legal cooperation to combat the growing menace of cyber crime in the south east region of Asia. The statement issued by the ASEAN Regional Forum on July 2006 reiterated its resolve to give a thorough fight against the growing menace of cyber space crime by extending common cooperation in legal and other areas of mutual concern. The theme of the discussion was various issues and challenges involved in the investigation of cyber crimes and measures to be taken to curb this ever growing evil.\textsuperscript{15}


The Conference organized by the members of the Asia-Pacific Economic Cooperation (APEC) resolved to work out a comprehensive legal framework for the prevention and control of cyber crime and for strengthening of cyber security in accordance with the set principles of the international law. In its ministerial meeting held in Santiago (Chile) in November, 2004 it was mutually agreed to strengthen economic cooperation to fight against cyber crime.


International Cyber Crime Conference held in Brazil, during November 6-9, 2006 was the 3rd major international meet in which hundreds of computer experts participated to deliberate on computer crime related issues and measures to prevent them.

The issues taken up for deliberation included electronic and online crime, crime task force model for 21st century, crucial infrastructure

protection program, cyber security, underground hacking activities, criminal file sharing on internet, cyber crime in international context and need for greater international cooperation in cyber crime investigation and extradition of cyber criminals.


In the Eleventh Congress on Prevention of Crime and Treatment of Offenders held in Bangkok on 18-25 April, 2005, the participants reviewed the global picture of cyber crimes and discussed priority concerns for prevention of these crimes. It was realized that the existing national laws were inadequate to check the constantly rising graph of cyber crimes at the international level. Therefore, there was need for bilateral, regional and international cooperation in crime prevention and strengthening of the criminal justice system by the participating nations.\textsuperscript{16}


The Seventh International Conference on Cyber Crime was held in Vigyan Bhawan, Delhi (India) on September 12, 2007. The Conference emphasized the need for generating cyber security awareness and evolving effective preventive measures to combat cyber criminality. The then Union Home Minister Mr. Shivraj Patil, in his inaugural speech at the conference observed- “notwithstanding its late entrance to the arena of serious crimes, cyber crime today represents a wide array of offences. Hacking, spoofing and botnet attacks are capable of serious security breaches in the information system of vital installations…… the potential danger on account of such attacks to the national security is immense.

Globally, instances of money laundering through e-channels for terrorist funding have assumed menacing proportions.”

The focus in the conference was on computer generated terrorist activities and organized crimes through internet which the criminals have found to be a lucrative means to generate huge proceeds of time. It was generally agreed that online child pornography, trafficking in contrabands and e-commerce frauds are showing a rising trend and the acts of vandalism and cheating were increasingly frustrating the e-governance efforts. Therefore, the need of the time demands quick response to the Interpol references and bilateral requests, liberal sharing of forensic technology and more cross-country training exchange programs besides, timely alert to tackle the cyber crime menace effectively.\(^{17}\)


An International Conference on Terrorism and Organized Crimes was held in Anaheim (USA) on August 25, 2008. It deliberated on problems of international and domestic terrorism, misuse of weapons of mass destruction, organized crime, human smuggling and trafficking, identity theft, online drug trafficking international monetary laundering, e-commerce, cyber frauds and computer forensics. The focus of the conference was on the extensive use of forensics in cyber crime investigations and involvement of computer experts in the process of investigation.

\(^{17}\) “Global anti-crime Centre mooted at Interpol Conference”, *The Tribune*, September 13, 2007, p. 1

This conference was held in Prague (Czech Republic) on September 3, 2008. The deliberation was burning issues relating to information technology and the prevention of illegal activities generated by advances in this field. There was consensus on need for working out an international legal strategy to protect national security and privacy of persons particularly the computer users.


An International Conference on Cyber Security and Protective Strategies was held on November 2-3, 2009 in Gatineau (Quebec). The delegates agreed on urgent need to step up protective measures to meet the new challenges which they were facing due to growing menace of cyber crimes.

Prior to the Quebec meet, a Conference on Cyber Crime Security Control System was held in Washington DC on October 1921, 2009. The conference reviewed the security measures initiated by member countries and emphasized the need for further cooperation and coordination to fight cyber criminality unitedly.

A Conference on Emerging Security Information Systems and Techniques was held on June 18-23, 2009 in Athens (Greece) to review the initiatives taken by participating countries to strengthen their intelligence security informatics.


The International Conference on Digital Forensics and Cyber Crime was held in Albany (New York, US) from September 30 to
October 2, 2009 and it deliberated that a uniform pattern of forensic mechanism should be evolved to tackle the digital related cyber crimes.\textsuperscript{18} This conference was preceded by the Conference on Digital Forensics Security and Digital Law which was held in Pretoria (South Africa) on July 22-24, 2009. It deliberated that the confidential information transmitted through internet and computer system needs to be protected against cyber attacks. The cyber criminals generally resort to spoofing to fish out data and digital informatics. Cyber crimes involving digital copying or piracy specially need a comprehensive digital protection. The need to upgrade digital law providing both civil and criminal liabilities for violation of digital forensics is also an area of paramount concern to facilitate investigation of crimes involving digital violations.


This Conference was held in Strasbourg on March 25, 2010. The focus of the conference was on the following 2 major issues:

(i). combating online child pornography
(ii). Netting networks etc. with a view to enhancing information technology security and combating cyber crimes effectively.

There was general agreement on the part of participants that legislative reform underway to prevent and control cyber crimes and ensure e-security should sustain. The majority of participants expressed a view that many countries have the global capacity to initiate measures to combat web-based crimes, therefore, there was need to enhance trust in information and communication technology. Primacy should, however,

be on protection of privacy and confidentiality, which are subjected to cyber attacks to clinch data pertaining to financial, commercial and technical or defence related computer program. The delegates shared common concern for strengthening of e-security by extending legal protection to database and digital information in view of the fact that internet jurisdiction involves the presence of multiple parties across the globe whose place of residence and cause of action shrouds in uncertainty and defies specific infringement and remedial actions.19

20. UN Congress on Crime Prevention (April 2010)

It enabled the participating nations to have an opportunity to re-enforce the earlier global responses to the threat of cyber crime. The member countries resolved to launch a crusade against cyber criminals particularly, the cross-border terrorists and the perpetrators of cyber fraud operating internationally.


It was held in Virginia (US) on 18-20 August, 2010. The focus was on cyberspace related IPRs, privacy security and development of computer forensics to combat transnational cyber criminality.

These international conferences/congresses held from time to time suggest that international community is making all out efforts to control and prevent cyber crimes. However, many countries have also enacted their own domestic legislation on cyber laws.

B. Comparative Cyber Law of Various Countries

Many countries have adopted cyber law in their legal regime to meet the challenges against the internet criminal activities. Some

---

countries have substantially updated\textsuperscript{20} their cyber laws while others have partially updated them.\textsuperscript{21} However, there are number of countries which have not initiated measures for adoption of cyber laws to combat computer and cyber space crimes. As the cyber crimes do not have any geographical or territorial boundaries, they are capable of breaching national borders which may cause serious threat to countries where legal protections against this crime are not adequate. Gaps and variations in domestic cyber laws of different nations render prosecution of international cyber criminals uncertain.

Inadequate legal protection of digital information and weak enforcement mechanism for protecting networked information enables the perpetrators of cyber crime to carry on their online criminal activities across the national borders undeterred with least chances of their being apprehended or nabbed.

The extent of progress made by countries around the world in updating their cyber crime laws according to UN report shows that 23\% of world nations have fully updated cyber law while 21\% have partially updated cyber law and 56\% have not updated their cyber law as yet.

1. United States

The first federal computer crime statute enacted in USA was the Computer Fraud and Abuse Act, 1986 which was reduced to hacking of computer systems. It was amended in 1994, 1996 and again in 2001 by the Patriot Act which addresses new abuses arising from misuse of new technologies.

\textsuperscript{20} Notably, USA, UK, Canada, Australia, Japan, Philippines, Turkey, Peru, Bestonia etc. have full-fledged cyber laws of their own. Consequent to the passing of the Information Technology (Amendment) Act, 2008, India has also become a country having a comprehensive full-fledged cyber legislation of its own.

\textsuperscript{21} Brazil, China, Chile, Czech Republic, Spain, Poland, Malaysia, Denmark, Sri Lanka, Bangladesh etc. have partially updated cyber law
i. U.S. Federal Criminal Code

The US Federal Criminal Code relates to the cyber crimes in the following 3 ways:

a. Fraud and related activities in connection with access devices
b. Fraud and related activity in connection with computers
c. Communication lines, stations and systems

a. Fraud and related activities in connection with Access Devices

The Federal Criminal Code provides for certain cyber offences which are punishable under the Code in the following manner:

(A). whoever –

(1). Knowingly and with intent to defraud produces, uses or traffics in one or more counterfeit access devices;

(2). Knowingly and with intent to defraud, traffics in or uses one or more unauthorized access devices during any one year period, and by such conduct obtains anything of value aggregating $ 1,000 or more during that period;

(3). Knowingly and with intent to defraud, possesses 15 or more devices which are counterfeit or unauthorized access devices;

(4). Knowingly and with intent to defraud, produces, traffics in, has control or custody of, or possesses device making equipment;

(5). Knowingly and with intent to defraud effects transactions, with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1 year period, the aggregate value of which is equal to or greater than $ 1,000.

22 The US Federal Criminal Code; Section 1029
(6). Without the authorization of the issuer of access devices, knowingly and with intent to defraud, solicits a person for the purpose of:

(a). offering an access device; or

(b). selling information regarding or an application to obtain an access device.

(7). Knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunication services;

(8). Knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9). Knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10). Without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device; shall, if the offence affects inter-state or foreign commerce, be punished as provided in sub-section (c) of this section.23

---

23 Ibid.
(B) Whoever-

(1). attempts to commit an offence under sub-section (a) of this section shall be subject to the same penalties as those prescribed for the offence attempted.

(2). is a party to a conspiracy of two or more persons to commit an offence under sub-section (a) of this section, if any of the parties engages in any conduct in furtherance of such offence, shall be fined an amount not greater than the amount provided as the maximum fine for such offence under sub-section (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offence under sub-section (c) of this section, or both.

(C). penalties –

(1). generally, the punishment for an offence under sub-section (a) of this section is– In the case of an offence that does not occur after a conviction for another offence under this section:

(i). if the offence is under paragraphs (1), (2), (3), (6), (7), or (10) of sub-section (a), a fine under this title or imprisonment for not more than 10 years, or both, and

(ii). If the offence is under paragraphs (4), (5), (8) or (9) of sub-section (a), a fine under this title or imprisonment for not more than 15 years, or both;

In the case of an offence that occurs after a conviction for another offence under this section, a fine under this title or imprisonment for not more than 20 years, or both; and In either case, forfeiture to the United States of any personal property used or intended to be used to commit the offence.
(2). Forfeiture procedure – the forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for sub-section (d) of that section.24

b. Fraud and related activity in connection with Computers

(A). whoever –

(1). Knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defence or foreign relations, or any restricted data, as defined in paragraph (i) of section 11 of the Atomic Energy Act, 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2). Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act.25

(3). Intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the

---

24 Ibid.

25 15 USC 1681 et. seq.
government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government’s operation of such computer;

(4). Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

(5). Intentionally accesses a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby:

(a). Causes loss to one or more others of a value aggregating $ 1,000 or more during any one year period; or

(b). modifies or impairs, or potentially modifies or impairs the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6). Knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization, if:

(a). such trafficking affects inter-state or foreign commerce; or

(b). such computer is used by or for the Government of the United States; shall be punished as provided in sub-section (c) of this section.²⁶

²⁶ Ibid.
Whoever attempts to commit an offence under sub-section (a) of this section shall be punished as provided in sub-section (c) of this section.

(c). the punishment for an offence under sub-section (a) or (b) of this section is –

(1) (a). a fine under this title or imprisonment for not more than 10 years or both, in the case of an offence under sub-section (1) (a) of this section which does not occur after a conviction for another offence under such sub-section, or an attempt to commit an offence, punishable under this sub-paragraph; and

(b). a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offence under sub-section (1) (a) of this section which occurs after a conviction for another offence under such sub-section, or an attempt to commit an offence punishable under this sub-paragraph; and

(2) (a). a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offence under sub-section (2) (a), (3) (a) or (6) (a) of this section which does not occur after a conviction for another offence under such sub-section, or an attempt to commit an offence punishable under this sub-paragraph; and

(b). a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offence under sub-section (2) (a), (3) (a) or (6) (a) of this section which occurs after a conviction for another offence under such sub-section, or an attempt to commit an offence punishable under this sub-paragraph; and

(3) (a). a fine under this title or imprisonment for not more than 5 years or both, in the case of an offence under sub-section (4) (a) or (5) (a) of this section which does not occur after a conviction for another offence under
such sub-section, or an attempt to commit an offence punishable under this paragraph; and

(b). a fine under this title or imprisonment for not more than 10 years, or both, in case of an offence under sub-section (4) (a) or (5) (a) of this section which occurs after a conviction for another offence under such sub-section, or an attempt to commit an offence punishable under this sub-paragraph.\textsuperscript{27}

c. Communication lines, stations and systems

Whoever, willfully or maliciously injures or destroys any of the works, property, or material or any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defence functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned for not more than 10 years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerned activities for the purpose of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defence function of the United States.

\textsuperscript{27} Ibid.
ii. U.S. Privacy Protection Act, 1980

The United States Privacy Protection Act, 1980 seeks to safeguard a person’s right to privacy in the information stored in computer in electronic form or any other electronic storage device such as laptop, floppy disk, diskettes etc. under his control. When the law enforcement authorities have reason to believe that the information possessed by a person in electronic form may provide evidence of a crime, they may inspect it or search, after obtaining a search warrant from the competent judicial authority. Thus, search in cases involving computers is constitutional provided it does not violate a person’s legitimate expectation of privacy.\footnote{Warden v. Hayden, 387 U.S. 294 (1967)}

Besides this, the US Electronic Communications Privacy Act\footnote{11 USC Section 2701-11} secures statutory privacy rights to customer and subscribers of computer network service providers. The Act protects the communications held by providers of electronic communication service when such communications are in electronically stored form.


The US Congress enacted the U.S. Computer Security Act, 1987 requiring Federal agencies to improve the security and privacy of Federal computer systems. A National Institute of Standards of Technology (NIST) was set up under the Act for laying down standards of security of Federal information technology.

Subsequently, the Paperwork Reduction Act, 1995 was passed which established a comprehensive information resources management framework giving recognition to transmission of information through computers and internet. This Act was further modified by the Information...
Technology Management Reforms Act, 1996. It was again amended in December, 1998 for setting definite guidelines and standards for security agencies to ensure security planning and introduce electronic record keeping as far as practicable and make sure that there is complete switch over to electronic filing and provide for authentication of digital signature. Now the US has passed the Government Information Security Act, 2000 replacing the earlier Act with a view to incorporating the latest technology developments and policy changes which have taken place over the years.

2. Canada

The Criminal Code of Canada provides unauthorized use of computers and illegal interception of communication as statutory offence which are punishable u/s 342 and 184 respectively. As a signatory to the European Convention on Cyber Crime, Canada has adopted cyber crime prohibitory law of the European Council with effect from November 23, 2001. The treaty defining cyber crime covers 5 major areas of computer related crime, namely, unauthorized access, breach of security and privacy rights, IPR violations, offences against confidentiality and computer related frauds.

3. United Kingdom

i. Computer Misuse Act, 1990

The United Kingdom had enacted the Computer Misuse Act, 1990, but due to later developments in computer technology and consequent emergence of new cyberspace crimes, a new law against cyber crime was enacted by the British Parliament which came into force with effect from November 7, 2006. The law mainly targets Denial of Service (DoS)
attackers with punishment up to 10 years of imprisonment. It clarifies that the old Computer Misuse Act did not contain provisions regarding DoS as a specific cyber offence; it only provided penalties for altering or modifying the computer data and its contents without authorization. The new Act explains DoS attack as an act of flooding the server with huge quantities of data until the server collapses.

ii. Computer Act, 2006

As per the new Computer Act, 2006, impairing the operation of any computer, preventing access to any program or data to computer and destructing the operation of any program on computer are crimes which are punishable with maximum of 10 years imprisonment. Also, causing someone to do any or all of the above crimes is punishable with imprisonment which may extend up to 2 years.

4. Australia

Australia has been relatively slower in adopting specific legislation for cyber crime and had divergent approaches throughout the various State territory and Federal jurisdictions. The Federal and State Governments in Australia have adopted legislations creating different offences to tackle the problem of computer crime.31

Under the Australian legal system, a new Act called as the ‘Cyber Crime Act, 2001’ was introduced which came into force on April 2, 2002 for amending the law relating to computer offences. The Act creates following 3 major computer offences:

---

i. Unauthorized access

Modification or impairment with intent to commit a serious offence is punishable with maximum penalty for the serious offence which is committed. For e.g. where person who hacks into a bank computer and accesses credit card details with the intention of using them to obtain money, he would be liable for the penalty applying to the offence which he was intending to commit.

ii. Unauthorized modification of data

Where the person is reckless as to whether the modification will impair data (maximum penalty of 10 years imprisonment). This is intended to cover a range of situations, such as where a hacker obtains unauthorized access to a computer system and impairs data.

iii. Unauthorized impairment of electronic communications

It is an offence punishable up to 10 years. This is designated to prohibit tactics such as ‘Denial of Service attacks’ (DoS), where a website is inundated with a large volume of unwarranted messages crashing the computer server.

The Act also creates 4 other computer offences:

1. Unauthorized access to, or modification of restricted data which is punishable with maximum penalty of 2 years imprisonment.

2. Unauthorized impairment of data held on a computer disk etc. which is punishable with maximum penalty of 2 years imprisonment.

3. Possession or control of data with intent to commit a computer offence which is punishable with maximum penalty of 3 years imprisonment.
(4). Producing, supplying or obtaining data with intent to commit a computer offence for which a maximum penalty of 3 years imprisonment is provided under the Act.

5. Germany

The law protecting internet and electronic communications was enacted in Germany during 1970’s. However, the Federation Data Protection Act, 1990 was introduced with a view to providing protection to individual against his right to privacy being impaired through handling his personal data.  

Germany also enacted the Information and Communication Services Act, 1997 which was not only confined to the protection of specific copyright violations but also imposed liability for online unlawful activities holding the Internet Service Provider invariably liable unless he could prove that he had no knowledge of the illegal content of the stored data.

The Federation Data Protection Act, 1990 as amended in September 1994 was subsequently replaced by the Federal Data Protection Act, 2002. This Act defines data processing and also contains provisions relating to admissibility of data processing and its use. It deals with confidentiality of data and also with inalienable rights of persons. It contains provisions relating to the compensation payable to public and private bodies in case of illegal activities done in violation

33 The German Information and Communication Services Act, 1997; Section 5 (2)
34 Federal Data Protection Act, 2002; Section 3
35 Ibid., Section 4
36 Ibid., Section 5
37 Ibid., Section 6
38 Ibid., Section 7
39 Ibid., Section 8
of the Act. It also deals with offences and penalties under the Act. It provides that anyone who without authorization starts, modifies, retrieves or alters any personal data protected by the Act, shall be liable for imprisonment which may extend to one year or with fine.\textsuperscript{40} It further provides that anyone who illegally obtains by means of internet, information and communication of personal data protected by this Act, and which are not publically known, shall be liable for punishment up to 2 years of imprisonment or fine.\textsuperscript{41} It also deals with administrative offences and provides that data can be taken from generally accessible sources or from the Controller of Data File, who would be entitled to publicize them. However, if anyone fails to comply with this provision, he shall be punishable with fine which may extend to 5000 DM.\textsuperscript{42}

A German cyber law expert Joerg Ziercke, pointed out that militant groups of terrorists are meeting in cyber space on internet and holding their training camps online. Al-Qaida has launched a practical website that shows how to use weapons, how to carry out kidnapping and how to use fertilizers to make explosive bombs.\textsuperscript{43}

6. Denmark

The Danish Criminal Code contains provision relating to computer crimes.

Any person who, for the purpose of obtaining for himself or for others an unlawful gain, unlawfully changes, adds or erases information or programs for the use of electronic data processing, or who in any other manner attempts to affect the results of such data processing, shall be

\textsuperscript{40} Ibid., Section 43 (1)
\textsuperscript{41} Ibid., Section 43 (2)
\textsuperscript{42} Ibid., Section 44
\textsuperscript{43} The Times of India (Delhi ed.) dated November 23, 2007
guilty of computer fraud.\footnote{The Danish Criminal Code; Section 279} It is punishable with imprisonment for any term not exceeding 1 year and 6 months.\footnote{\textit{Ibid.}, Section 285 (1)} Where the offence is of an aggravated nature or where a large number of such offences have been committed, the imprisonment may be enhanced for any term not exceeding 8 years.\footnote{\textit{Ibid.}, Section 286 (2)}

If the offence dealt with in section 279 of the Code is of a minor nature because of the small value of the objects appropriated or of the loss of property sustained or for any other reason, it may be punished only with fine and this penalty may be remitted in the mitigating circumstances.\footnote{\textit{Ibid.}, Section 287 (1)}

7. Poland

The Criminal Code as amended on June 6, 1997 expressly prohibits computer offences.

It provides that whoever interferes with, or disables or otherwise affects the automatic processing, gathering or transfer of information, shall be liable to imprisonment which may extend for a period from 6 months to 8 years depending on the gravity and seriousness of the offence.\footnote{The Polish Criminal Code, 1997; Article 165 (Section 4)}

Whoever does unauthorized destruction, removal or damaging of information or changing it or preventing its access to a person who is authorized to have it or in any way impedes the process or transmission of information shall be liable for punishment which may extend to 2 years imprisonment.\footnote{\textit{Ibid.} Article 268 (Section 1)}
Whoever, without permission or authorization processes personal data in a file, shall be subject to fine, confinement or imprisonment up to 2 years.\textsuperscript{50}

It provides punishment for misuse of personal file data\textsuperscript{51} and the failure to protect data against theft by unauthorized person, damage or destruction is punishable with imprisonment which may extend to 1 year.\textsuperscript{52} Even unintentional failure to protect data or negligence in protecting it has been made punishable under this provision.

Where a person who is obliged to submit a data file for registration fails to do so, he may be subjected to confinement or imprisonment for a period up to 1 year.\textsuperscript{53} Failure to observe the obligation to notify the data subject about his rights is also made a punishable offence and the penalty may extend to a fine, restraint of liberty or imprisonment for a period up to 1 year.\textsuperscript{54}

8. Turkey

There is no special cyber penal legislation for computer offences in Turkey. However, the Turkish Penal Code provides that any person who unlawfully obtains programs, data or any other components from an automated data processing system, shall be sentenced to imprisonment which may extend from 1 to 3 years and having fine ranging from 1 to 15 million Turkish Liras. It further provides that any person, who uses, transmits or reproduces a program, data or any other component within an automated data processing system with intent to cause loss or damage to

\begin{footnotes}
\textsuperscript{50} Ibid. Article 49 (Section 1 and 2) \\
\textsuperscript{51} Ibid. Article 50 \\
\textsuperscript{52} Ibid. Article 52 \\
\textsuperscript{53} Ibid. Article 53 \\
\textsuperscript{54} Ibid. Article 54
\end{footnotes}
another, shall be liable to punishment similar to one, which is provided for unauthorized access.55

9. Japan

Japan is also one of the countries to be a party to the International Treaty (European Convention on Cyber Crime) designed to combat computer crimes. In Japan, there are following 2 laws relating to the protection from cyber crimes:

i. Unauthorized Computer Access Act, 2000

The main purpose of this Act is to take measures by the Metropolitan or prefecture Public Safety Commissions for preventing unauthorized computer access by prohibiting such acts and to prevent computer-related crimes that are committed through telecommunication lines and to maintain the telecommunications-related order that is realized by access control functions and thereby, to contribute to the sound development of the advanced information and telecommunications society.56

The Act also lays down certain definitions,57 it contains some other parts where the functions related to the unauthorized computer access are defined as offences,58 for which it also make penal provisions.59

a. Prohibition of acts of unauthorized computer access:

1. No person shall conduct an act of unauthorized computer access

2. The act of unauthorized computer access means an act that falls under one of the following items –

55 The Turkish Penal Code; Section 525 (a)
56 Unauthorized Computer Access Act, 2000; Article 1
57 Ibid., Article 2
58 Ibid., Articles 3 and 4
59 Ibid., Articles 8 and 9
(i). An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person’s identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of authorized user for that identification code);

(ii). An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item); and

(iii). An act of making available in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.\(^{60}\)

A person who has infringed the above provision shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 Yen.\(^{61}\)

\(^{60}\) Ibid., Article 3
\(^{61}\) Ibid., Article 8
b. Prohibition of acts of facilitating unauthorized computer access:

No person shall provide another person’s identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computers specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.⁶²

A person who has infringed the above provision shall be punished with fine of not more than 300, 000 Yen.⁶³

ii. Computer Crime Act, 1999

This is an Act by which Japan Penal Code is amended and a separate Act is evolved to combat cyber crime problem. By this Act, most of the provisions were changed to meet the new challenges posed by cyber crimes.

10. Sweden

Adopting the UK pattern of computer crime legislation, Sweden has also banned DoS attacks on website from June 1, 2007. Therefore now all websites attacks including DoS whether committed manually or automatically by misuse of computer are illegal and punishable with imprisonment up to 10 years. Even an attempt to launch DoS attack is an offence punishable under the law.⁶⁴

---

⁶² Ibid., Article 4
⁶³ Ibid., Article 9

{168}
It is significant to note that the Swedish National CID Department is handling nearly 500 computer crime cases yearly of which more than 50% are internet related offences having national and international ramifications. In order to deal with these crimes effectively, the Swedish Ministry of Justice has enacted a new cyber law providing for coercive means of detecting, monitoring and tapping cyberspace crime perpetrators. The new law is popularly called as the FRA law and it has been approved by the Swedish Government on June 18, 2008 and became effective from 2009. It gives the Swedish National Defence Radio Establishment the right to intercept all internet and other e-traffic crossing Swedish borders.

11. France

The French law relating to internet and computer crimes is modeled on European legislation which provides foundation of legal rules that apply throughout the European country. The European Parliament had issued the Council of European Directives in legal framework for electronic signature and certain information services particularly the e-commerce on December 13, 1999, which has been adopted by France from June 8, 2000.

As regards the protection of IPRs on internet transactions there is a French IP Code which protects the intellectual property rights to creative works regardless of time, form, value or purpose. France had enacted legislation for regulating the electronic processing of nominated data. So far domain name regime is concerned; French Government has adopted ICANN rules for the protection of domain names.65

---

65 The French Penal Code; L. 112-1
12. Spain

The Spanish Penal Code also deals with computer crimes such as unauthorized interception of electronic mails or information or its transfer, reproduction or distribution which is punishable with imprisonment up to 4 years.\textsuperscript{66} The Code also deals with computer fraud which is punishable with imprisonment up to 3 years and also with fine.\textsuperscript{67}

13. Russia

The Russian Federation has not enacted any separate cyber crime law but the provisions relating to cyber crimes and punishment for them are contained in the new Russian Federation Criminal Code (RFCC) enforced from January 1, 1997. The elements of computer crimes are embodied in Chapter 28 (Articles 272-274) of the Code which is entitled as “Crimes in Computer Information Sphere”.

The unauthorized access to computer information is an offence punishable with 2 years long deprivation of liberty (i.e. imprisonment). Further if the crime is committed by a group of persons or by those misusing their official position then the sentence is enhanced to 5 years.\textsuperscript{68}

The creation, use and spread of detrimental computer program are a serious offence punishable with 3 years deprivation of liberty.\textsuperscript{69}

The infringement of operating rules of a computer, computer system or computer network is an offence, the violation of which shall entail punishment of deprivation of right of taking certain posts or occupation up to 5 years.\textsuperscript{70}

\textsuperscript{66}The Spanish Penal Code; Article 197 (1)
\textsuperscript{67}Ibid., Article 248
\textsuperscript{68}Ibid. Article 248.
\textsuperscript{69}Russian Federation Criminal Code, 1997; Article 272
\textsuperscript{70}Ibid., Article 273

14. China

The Republic of China had enacted a legislation called as the Regulation for Protection of Software under Chinese Copyright Act, 1990 during the communist regime. However, with the later developments and socio-economic changes particularly, the development of internet and voices raised through media against the conventional orthodox regime, the Government of China pursuant to an executive order of February 1, 1996 took control and management of the entire infrastructure of online internet connectivity. Under this law, information task forces have been established to coordinate connections to the internet. Any connection to the internet has to go through the Ministry of Telecommunication and individual entities are prohibited to establish internet connections. Prospective ISP’s are to apply for license to the Government departments in order to procure internet service. The Bureau of Public Security (BPS) has the authorization to shut down the internet connection when its operation is in violation of the above rules. BPS may also impose fines on illegal operation, the amount of which shall not exceed 15000 RMB.

15. Philippines

While the ‘Love Bug’ virus (technically a ‘worm’) travelled as an attachment to e-mail messages of companies and individuals around the world in May, 2000, its source was traced by the US investigative agencies with the help of National Infrastructure Protection Centre (NIPC) in Philippines within 24 hours. They were able to identify perpetrators with the help of Philippines National Bureau of Investigation. Realizing that the investigation in this case was hampered due to lack of specific computer crime law, the Philippines enacted a law called the Philippines E-commerce Act, 2000.\footnote{The Act came into force with effect from June 14, 2000.} The perpetrator of ‘Love
Bug’ virus Onel de Guzmun was charged with the offence of fraud, theft, malicious mischief and violation of the newly enacted computer crime law. The Act has been considerably effective in controlling the incidences of computer crimes in Philippines.

16. Mauritius

Mauritius has enacted the Information Technology (Miscellaneous Provisions) Act, 1998 for the prevention and control of cyber crimes. Part II of this Act deals with computer related offences and penalties for such offences.

The punishment for the offence of unauthorized access to computer data may be a fine not exceeding 50,000 Rupees and imprisonment up to 5 years.\footnote{Mauritius Information Technology (Miscellaneous Provisions) Act, 1998; Regulation 369A.}

The offence of unauthorized access and interception of computer service is punishable with a fine not exceeding 100,000 Rupees and to a penal servitude for a term not exceeding 10 years. Unauthorized modification of computer material is also an offence punishable with similar penalty.

The Act treats illegally denying access to or damaging computer system as a serious offence which makes the offender liable to a fine not exceeding 200,000 Rupees and to a penal servitude not exceeding 20 years. Similar punishment is awarded to a person who is convicted of electronic fraud.

The making, publishing, showing or distributing indecent photographs or pseudo-photographs of children online or on the net is an
offence which is punishable with imprisonment or/and confiscation of article or apparatus used.\textsuperscript{73}

17. Sri Lanka

Sri Lanka enacted its Computer Crime Act, 2007 and its key feature is that it primarily addresses the computer related crimes and hacking offences. It also contains provision for expert penal to provide assistance to police in the investigation of cyber crimes.

The Act criminalizes attempts at unauthorized access. It provides that any person who intentionally or without lawful authority carries out a function that can potentially affect or damage any computer or computer system or computer program, will be guilty of a crime punishable under this Act.

The Act empowers the expert panel with specific powers such as visiting the scene of crime for purposes of investigation and access to examine computer system etc. It provides for retention and prevention of information required from computer devices for the purpose of carrying out investigation.

According to Sri Lankan Information and Communication Technology Agency (ICTA), computer crimes consist of 3 components, namely, (i) Computer related crimes, (ii) Hacking offences, and (iii) Content related cyber crimes.

18. Bangladesh

The computer networks were established in Bangladesh for the 1st time in 1964, but the main frame installation had to be closed in 1971 due to outbreak of war with Pakistan following liberation movement in

\textsuperscript{73} Ibid., Section 15.
Bangladesh. It was, however, restarted in 1975 after the independence of that country.

The Government of Bangladesh appointed an Expert Committee in June, 1997 to provide a legal framework for prevention and control of cyber crimes. The Committee submitted its report in January, 1999 in which as many as 45 recommendations were made for a comprehensive legislation of cyber law. The Government suggested certain changes and modifications in the proposed legislation, which were duly considered by the Expert Committee and it submitted its revised recommendations to the Government in June, 2002. Consequently, the Bangladesh Cyber Crime Act, 2004 came into force. This Act provides stringent punishment for cyber offenders.\textsuperscript{74}

19. Pakistan

Pakistan enacted its Prevention of Electronic Crimes Act, 2007 on January 17, 2007 providing stringent punishment to those who steal, deny or destroy valuable information available on electronic networks. Thereafter, in order to remove certain lacunae and deficiencies of the Act, a Bill entitled Cyber Crime (Prevention of Electronic Crimes) Bill was laid before the National Assembly on September 7, 2007 but the Bill invoked sharp criticism from the legal luminaries and was characterized as an archaic and draconian legislation which could do more harms than good to the computer users.

Explaining the alleged shortcomings of the Bill, Barrister Zamid Jamal observed that, “once this legislation is promulgated by the National Assembly, innocent Pakistani persons who use computer on a daily basis would be victim of its draconian effect as merely an act of formatting a

\textsuperscript{74} N. Muddaraju and Dr. Ramesh, “Cyber Crimes: Need for an Effective Law”, \textit{Criminal Law Journal}, 2009, p. 228
hard disk will lead to a punishment of 7 years imprisonment and/or a fine of 10 lakh Rupees.”

The Bill deals with as many as 21 cyber issues ranging from malicious code to spinning and spoofing. Overtly, it may seem to cover all aspects of new digital era but a closer scrutiny reveals quite contrary. The major shortcomings of the proposed Bill are as follows:

(a). The Government is coining and re-inventing a new definition of cyber crime deviating from the internationally accepted norms, leaving more area of confusion and exploitation with the law;

(b). The proposed law allows more room for Federal Investigating Authorities (FIA) to interfere with the life of innocent people who are genuine computer users;

(c). FIA is given unrestricted power to arrest and confiscate property and therefore, the Bill is of a hideous nature;

(d). There are 17 types of cyber crimes for which the punishment may extend up to death penalty. This is further indicative of the draconian nature of the proposed legislation.

C. International Agencies for Regulating E-Commerce

There are certain international agencies which function to regulate trade and e-commerce at the global level and provide a forum for resolution of disputes and problems by mutual negotiations.\(^75\) The main among them are as follows:

1. World Trade Organization (WTO)

It was during the end of World War II (1939-45) that the economists around the world met in Briton Woods, Hampshire and suggested the setting up of an international agency to restore the

\(^{75}\) Shri Pranam Kumar Rout, “Cyber Law is the Need of the Time”, Cuttack Law Times, 2000, p. 108
economic order to harmonize tariff and international trade and solve the monetary problems. There was proposal to set up an International Trade Organization but it could not come into existence due to opposition from US Congress. However, the representatives of 56 countries met again in Havana in 1947 to formulate guidelines to improve and regulate international trade. Consequently, a General Agreement on Tariff and Trade (GATT) was signed by the contracting countries in December, 1947. Initially, GATT dealt with reducing tariffs and improving trade among the nations, but there was not any dispute settlement mechanism provided in it.

The 8th round of GATT held in Uruguay in 1986, led to the proposal for creation of the World Trade Organization (WTO) which was supposed to deal with the following issues:

(a). trade related IPRs
(b). trade related investment measures
(c). trade related services
(d). agricultural subsidy
(e). trade related dispute settlement mechanism

Thus, the GATT continued to operate nearly 5 decades. Finally, the draft prepared by Author Dunkel, the Secretary General of the Board of Trade was approved and finally signed on April 15, 1994 by 125 countries at a meeting held in Morocco and it was resoled the World Trade Organization be established from January 1, 1995 to function as a trade policy reviewing body and a trade relation dispute settlement forum. The WTO as a successor to the GATT is an international organization designed to supervise and liberalize international trade.
2. WIPO Internet Copyright Treaty, 1996

The origin of World Intellectual Property Organization (WIPO) can be traced back to 1883 when Paris Convention for protection of industrial property was held and a treaty was signed for the protection of intellectual creations known as patents. Thereafter, copyright entered the international arena with Burne Convention (1971) on protection of copyright. In 1974, WIPO became a specialized agency of UNO with mandate to administer intellectual property matters.\textsuperscript{76}

In 1996, the WIPO made 2 treaties commonly known as internet treaties for countering the challenges posed by internet crimes. These treaties are silent on the subject of liberty of Internet Service Providers (ISPs), as the issue of liability has been left to the national legislations for determination.

The WIPO Copyright Treaty which was adopted in Geneva on December 20, 1996, and came into force with effect from March 6, 2002, mentions about the right of communication but does not contain a provision on the right of reproduction. It only declares that digital copies will be considered as reproduction for the purpose of copyright law.\textsuperscript{77}

3. Internet Cooperation for Assigned Names and Numbers (ICANN)

The domain name disputes are being settled by online arbitration under the Uniform Domain Name Dispute Resolution Policy adopted by the ICANN which is headquartered in California. It was created on September 18, 1998 in order to handle a number of tasks such as managing the assignment of domain names and IP addresses. The disputes pertaining to domain name are settled by the Alternative Dispute Resolution Service Providers. It exercises jurisdiction over the entire

\textsuperscript{76} Nicholas v. Universal Pictures Corp., 450 US 584 (1978).
\textsuperscript{77} The WIPO Copyright Treaty, 1996; Article 1 (4).
internet and thus mitigates the hardships of citizens and respects sovereignty of the existing legal systems of different nations.  

D. REVIEW

An overview of the international perspective of law on cyber crime suggests that despite internet and cyberspace laws having been enacted by several countries, many complicated legal issues that have emerged in cyberspace (which know no boundaries and physical environment), still remained unresolved in the existing legal regime. In the context of India, though the Information Technology Act, 2000 has been introduced as a comprehensive legislation to prevent and control cyber crimes, yet it is only a gap-filler and has no applicability in many situations. The legal position as regards electronic transactions and civil liability for the acts executed in cyberspace still remain hazy in the absence of an adequate global law on this crucial issue.

The impact of internet and gravity of the problem of cyber crime in the context of the existing global regime can be well appreciated by the fact that US Congress had to introduce more than 50 Bills pertaining to internet and e-commerce in the first 3 months of 1999 alone. The issues which need to be addressed urgently at the international level are security of transactions, privacy protection of children against pornography, validity of contracts, uniformity in procedural rules of evidence, certainty of jurisdictional issues and a host of other related problems.

It is well known that cyber crimes include a variety of criminal activities which are done in the cyberspace. A cyber criminal may destroy

80 Jim Puzzanghera, 'U.S. Law Makers Clamoring to Regulate Internet', San Jose Mercury News, April 9, 1999
websites and portals by hacking or planting viruses, carry out frauds by illegally transferring funds, gain unauthorized access to highly confidential and sensitive information by breaching security, intrude in personal privacy, cause e-mail threats or harassment and indulge in cyber pornography and commit many other similar activities. In fact, the whole world has become a operational canvas for cyber criminals to commit innumerable other crimes on the internet. Though most countries have introduced anti-cyber crime legislation to tackle the problem domestically at the national level but there is a need for global control mechanism to combat these crimes. Therefore, the countries should rise above their regional conflicts and stand together to give a tough fight against the menace of cyber crimes in a spirit of mutual understanding and cooperation.