5.0 PREVENTION, PROTECTION AND CONTROL OF CYBER CRIMES

Like any other crime, the issue of legitimacy of criminalization is applicable in cyber crimes also. The very characteristics of cyber world make such an enquiry even more important. The boundary-less virtual cyber world is unique and needs special treatment with regard to all issue including criminalization. The target group of any criminal law in cyber world may not be amenable to the Sovereignty Of The State enacting the law. If it has to enforce the law, it may have to get the offender extradited from his native state for which the municipal court therein has to be satisfied first. In such situations, legitimacy of jurisdictions in criminalizing the impugned conduct (particularly when the conduct is not a crime in the other country) will definitely help in procuring the extradition.

The main issue remains as to what should be the basis of criminalization in cyber world? Should it be based on the harm caused to others? Or is it because the act is against the morality of the cyber world? Or is it necessary to protect the offender himself because he is the victim too? These issues need much more deliberation and global acceptance so as to make any fight against cyber crimes through criminalization of these activities effective.

"Indian Information Technology Act, 2000 has chosen a middle path in criminalizing certain activities and not criminalizing certain other activities, which fall within the purview of the term cyber crimes. The Act tries to impose penalties in the form of non-criminal monetary sanctions for certain actions that does not have serious consequences. Yet some other activities that are considered more serious in their consequences are treated as criminal and liable to imprisonment and fines".1

5.1 JURISDICTION;

"[W]e realize that attempting to apply ............ law in the fast-developing world of the Internet is somewhat like trying to board a moving bus"

- Judge van Graafeiland in Bensusan Restaurant Corporation U. King.

---

Did you ever think that launching an e-business could mean defending a lawsuit in any state or country where the end user reside? For example, your California Web Company could be doing business with customers in Florida or in India. If a user is deprived of a legal right in the user’s state, the user may be able to sue you in that state or foreign country if a court has jurisdiction over your company.

Once a company creates a web site it has a continuous online presence in every state and foreign country where an end user can access the Internet. Internet technology continues to pose a threat to the jurisdictional importance of state and national borders. Of great concern to an e-business is the daunting possibility of being sued by a consumer or other aggrieved party in a remote state or foreign country. In the United States an e-business merchant may be required to defend a law suit in a foreign jurisdiction only if the court has personal jurisdiction over the e-business defendant. Personal jurisdiction is the court’s authority and power to make the defendant obey a court order. E-business transactions transcend geographical boundaries and instantly reach global market place formerly unavailable to most merchants.

E-commerce introduces the novel business arrangement of establishing an electronic presence outside its local jurisdiction. But the expanded market opportunities come with strings: “doing business” in other states or countries might make the e-business accountable to those regions’ laws. A legally aggrieved plaintiff used in an on-line transaction may file a law suit anywhere in the world where the business violation occurred. In contrast to a mail order catalog company, which chooses the locations of its potential customers, an e-business does not choose its customers. They are wherever web access is, and they bring their local laws with them.

Jurisdiction is the authority of a court to hear a case and resolve a dispute. Because the legal environment of e-commerce has no geographical boundaries, it establishes immediate long-distance communications with anyone who can access the web site. Usually an online e-merchant has no way of knowing exactly where the information on its site is being accessed. Hence, jurisdiction issues are of primary importance in cyber space. Engaging in e-commerce on the World Wide Web may expose the company to the risk of being sued in any state or foreign country where an Internet user can establish Internet a legal claim. Legal Counsel and insurance underwriters should carefully review this potential risk and its accompanying cost to the
business. In each case, a determination should be made as to whether an online presence will subject the e-business to jurisdiction in a distant state or a foreign company.

When trial lawyer represent online clients who are being sued in a foreign court, they will always consider having the case litigated in the jurisdiction, where their clients primary business is located rather than the plaintiffs state or country. Although the case could be litigated in a state court, it will more commonly be a federal court because cyber space issues often involve federal statutes (e.g., copyright and/or trademark law) or diversity jurisdiction (i.e., a plaintiff from one state suing an e-business defendant from another state with damages of $ 75,000 or more).

5.1.1 Traditional Principles of Jurisdiction:

Common law principles of personal jurisdiction have evolved by judges opinions in their case decisions long before the online world existed. The cases that created our traditional principles of personal jurisdiction will be applied to e-commerce. When a non-resident e-business defendant raises the issues of lack of personal jurisdiction by a motion to dismiss, the plaintiffs must generally prove satisfaction of both the local states long-arm statute and the due process clause of the U.S. constitution.

Since e-commerce on the Internet reaches unknown market places, the aggrieved end user may file a law suit in any state (or country) where the court has personal jurisdiction over the non-resident defendant. Keep in mind that the term personal jurisdiction includes a “person” doing business as a sole proprietor, corporation, partnership, or other form of business organization. Since most e-business is corporations, a foreign court must have personal jurisdiction over it if challenged by a motion to dismiss2.

5.1.2 Personal Jurisdiction in the online Environment

When an e-business establishes and maintains a web site and engages in electronic commerce, it is entitled to the protection of the U.S. Constitution, the State Constitution and the local law where the company is located. Any person, including a distant user, who accesses the company’s web site is entitled to the same legal protection.

In World Wide Volkswagen V. Woodson, 444 286, the U.S. Supreme Court held that merely placing a product in interstate commerce does not of itself "purposefully avail oneself" to a forum states jurisdiction. What is required is additional conduct", defined as intent to serve the market in the forum state.

Digital Equipment Corporation v. Alta Vista Technology, Inc., 960 F. Supp. 456 (D. Max. 1997) involved a trademark infringement case. The case was based on the theory that Digital, a Massachusetts Corporation, contracted with Alta Vista Technology, a California Company, that changed its corporate name to Alta Vista Corporation, not to use its trade mark "Alta Vista" in a product or serviced Offering Digital paid Alta Vista for all rights to the trade mark other than Alta Vista Technology's right to use the trademark, as part of its corporate name and address less than two months after the contract was signed, Alta Vista Technology’s website used the trademark “Alta Vista” at the top of its home page and later added banner ads. The California defendant, Alta Vista Technology, brought a motion to dismiss the case from the Massachusetts federal Court for lack of personal jurisdiction. The Court denied the motion and found jurisdiction since the Massachusetts long-arm statute was satisfied because there was evidence of Alta Vista Technology doing business in Massachusetts based on its solicitations for banner ads.

This case has special significance to the e-business community because it involves a trademark licensing agreement between a company that owned a common law trademark Alta Vista and a company that wanted to use that trademark and was willing to pay a great deal of money to do so. A trademark search may reveal that another company is using your mark. It may be worthwhile to explore the possibility of entering into an agreement allowing the company to continue using the trademark for its name and address but not for online purposes3.

5.1.3 International jurisdiction in Cyber Space

Online Web Sites are electronically carried to international users. A transaction may require an e-business plaintiff to litigate in the United States against a defendant in a foreign country or be a defendant in a foreign country. An e-business should be aware of the possibility of being sued by litigants from a foreign country. Web sites that have a drag down list of foreign countries where a customer may wish to purchase their products or services are inviting litigation in that country.

3. (Supra 2 – PP. 23-24).
Principles of international law apply to electronic commerce and generally permit a country to regulate only those activities that have a substantial effect in their country. The United States, Canada and the European Union (EU) are working on universal laws that will be transnational and predictable to an e-commerce transaction. The EU is developing a “country of origin” principle that would apply the law of the country where the contract originated. In opposition to the “country of origin” principle is the “country of reception” rule that would allow consumer end users to have the benefit of their country’s own consumer protection laws. This principle would apply only to a consumer transaction and not to a business-to-business e-commerce contract.

Global solution to international e-commerce transactions will depend on the revisions and developments of international laws to accommodate the internet. Global organizations such as the United Nations Commission on International Law, the World Trade Organization, and the Organization of Economic Co-operation and Development are all working in this direction  

5.1.4 Jurisdiction of Governmental Agencies.

The rules of international law that define the jurisdiction of governmental agencies are different with respect to criminal conduct and non-criminal (or civil) conduct.

5.1.5 Criminal Jurisdiction

In order for a legislative assembly to adopt, an executive to enforce, or a court to adjudicate criminal sanctions internationally, there must be some nexus, or connection, between the agency or organization and the crime or criminal. Five such connections may be used to justify an exercise of international jurisdiction. Legal Commentators refer to these connections as principles.

1. The territorial principle of jurisdiction holds that the place where an offense, is committed to determine jurisdiction.

2. The nationality principle looks to the nationality or national character of the person committing the offense to establish jurisdiction.

3. The protective principle provides for jurisdiction when a significant national or international interest is injured by the offender.

4. The universality principle allows for taking the offender into custody.

4. (Supra 2 – PP. 29).
The passive personality holds that jurisdiction arises from the nationality or national character of the person injured by the offense.

The example, a person engaged in the unauthorized broadcasting of radio or television signals from a ship on the high seas may be arrested and tried by the state whose flag the ship is flying (this is a form of territoriality principle); or, if the ship is not flying a flag, by any state (this being based on the universality principle); by any state whose radio communications are being affected (this is based on the protective principle); by any state where the transmission can be received (the passive personality principle) – United nations on the Law of the Seas, Articles 109(3) and (4), and 110 (1982).

Not all of these principles are used in all cases. In fact, the territoriality principle is the jurisdictional nexus most commonly relied upon in legislation, and often it is the only such connection. For example, Britain’s Obscene Publications Act of 1959 only imposes criminal sanctions on offenders who publish obscene materials in the United Kingdom. A British defendant in the case of Crown v. Waddon (BBC News, July 1, 1999, posted at http://news.bbc.co.uk/hi/english/sci/tech/newsid 38200/382152.stm ) attempted to avoid liability under that act, accordingly, by posting pornographic materials on a server located in the United States. A British court, however, found that publication had occurred in the United Kingdom. It had, the Court said, because the defendant transmitted the pornographic materials from his computer in the United Kingdom to the U.S. Server, and those materials were downloaded from the U.S. Server for viewing on a computer in the United Kingdom.

5.1.6 Civil jurisdiction

In order for a government agency to exercise jurisdiction over civil matters, there must be a nexus between the persons or property involved and the territory (nation, state, province, municipality, and so on) where the agency is located – known as the forum. This is known as jurisdiction over persons (in personam) and jurisdiction over property (in rem) jurisdiction.

5.1.7 Jurisdiction over persons

In personam jurisdiction is the power of a government agency to regulate matters involving natural and juridical persons. Natural persons are human beings. Juridical persons are legal created by national or international law and granted the
privilege of carrying on many of the functions of natural persons such as engaging in business, swing, and being sued.

The basis for in personam jurisdiction is consent, which may be actual or implied. Actual consent can be given on a forum selection clause in a contract in which the parties designate the forum where disputes will be settled, and a choice of law clause in a contract, wherein the parties designate the forum whose law will govern their relationship. For example, Netscape communications includes the following forum selection and choice of law provisions on its web site.

In addition to those clauses, actual consent can also be given by incorporating or otherwise registering to do business in a forum and by bringing suit in a court. Consent can be implied from (1) having the nationality of the forum (2) being domiciled in the forum, (3) being physically present in the forum, or (4) having minimum business contacts with the forum.

This last form of consent to in personam jurisdiction – having minimum business contacts with the forum is generally only used in countries that have a common law tradition (that is, in countries, that inherited their legal system from England). Most of the rest of the countries of the world follow a civil tradition (one derived from legal system of ancient Rome). In Civil law countries, generally, engaging in business in a forum without having a physical presence there, is not enough to establish in personam jurisdiction.

In common law countries, jurisdiction over a person based on minimum business contacts requires a showing that (1) the person purposefully availed itself of doing business in the forum and (2) the person reasonably could have anticipated that it would have to defend its acting there.

An example of a case that applied this minimum business contact criteria to an Internet dispute is Brain Tech Inc. U. Kostiuk, a British Columbia resident, published defamatory information about it on an Internet, bulletin board maintained by a Texas Company. Brain Tech subsequently brought suit in Texas and the Texas Court issued a judgment for damages in Brain Tech’s favour. Brain Tech then sought to have a British Columbia Court issue a judgment enforcing the Texas Court’s judgment. Because Kostiuk was a British Columbia resident and all his assets were there, the Texas judgment was of little effect. A trial court granted Brain Tech its request and Kostiuk appealed, arguing that the Texas Court lacked jurisdiction to hear any dispute between Brain Tech and himself and therefore that its judgment was ineffective. The
British Columbia Court of Appeal agreed. To assume in personam jurisdiction over a nonresident defendant, the court said, a defendant must have "minimum contacts" with the forum, the claim against the defendant must arise out of those contacts and the overall exercise of jurisdiction must be reasonable. With respect to Koustiuk there was no "real and substantial connection" between Texas and the alleged wrong doing. Kostiuk's only connection with Texas was the posting of the allegedly defamatory statement on the bulletin board maintained by the Texas Company. He had no other contacts. Accordingly, the British Columbia Court of Appeal dismissed the trial Courts' judgment.

Although countries that follow the Civil law do not recognize in personam jurisdiction based on minimum business contacts are mostly civil law territory, the European Union recognizes a similar sort of adjudicative jurisdiction. This allows a court in one EU members state to assume in personam jurisdiction over consumer sales involving sellers from other members states.

A recently proposed EU regulation would extend this consumer jurisdiction to Internet transactions. Instead of requiring proof that the seller has directed advertising to, or provided financing for, the consumer, the consumer would only have to show that the seller entered into sales transactions over the Internet in the consumer's state of domicile.

5.1.8 Jurisdiction over property

In rem jurisdiction is the Power to determine the ownership rights of all persons with respect to particular property located within the territory of the forum. For example, legislation way define certain property as being illegal to export (such as encryption software) or as contraband (such as CAD software used in developing missile and nuclear weapons). The ownership of real property (i.e. immovable property, such as land and building) is, determined in an in rem court proceeding. Similarly, if the ownership of personal property (or movable property, such as computers and software) is contested, it would be determined in an in rem court proceeding in the state where the property is physically located.

5.2 The Criminal Justice System And Crime Management

Crime is inevitable in any human Society since some violation of any code of conduct prescribed for the members of a society is bound to occur. Not only is crime
inevitable but, paradoxical as it may found, some sociologists have gone to the extent of saying that crime to some extent, helps in promoting social solidarity among people constituting the society. The inevitability and universality of the phenomenon of crime has been described by Emile Durkheim in the following words:

There is no society that is not confronted with the problem of criminality. Its form changes, the acts thus characterized are not the same everywhere; but, everywhere and always, there have been men who have behaved in such a way as to draw upon themselves penal repressio ......... No doubt it is possible that crime itself will have abnormal forms, as for example, when its rate is unusually high. This excess is indeed undoubtedly morbid in nature. What is normal, simply, is the existence of criminality, provided that it attains and does not exceed, for each social type, a certain level ......... To classify crime among the phenomena of normal sociology is not to say merely that it is inevitable, although regrettable, phenomenon, due to incorrigible wickedness of men, it is to affirm that it is a factor in public health, an integral part of all health societies.

According to Durkheim even a Society composed of persons possessing angelic qualities would not be free from violations of the norms of that society with the result that faults which appear venial to the layman will create there the same scandal that the ordinary offence does in ordinary consciousness.

The crime is a phenomenon which is of primary concern to every member of the human society. The concern for crimes and criminals is reflected in various forms of curiosity among people. First there is the idle curiosity in certain minds where the object is not so much to understand something seriously about crime but just to get some sort of thrill or kick out of it.

5.2.1 CRIME MANAGEMENT

The object of crime management, is to manage the criminal activities, prevent, cure and eradicate the crimes and to protect the society and to investigate and arresting the offender and place the offender for trial.

The burning truth is that the human society can get rid of the Criminal activities, in the present time forthcoming or distant future. A system of facing and managing crimes has been established through legal rules, administrative frame work and police, the trial of accused and final object is to convict the accused to save the society from terror of criminal activities.

The various wrongful activities done by members of the society have been divided into two broad groups for the convenience of attention, persuasion, trial and remedy. The broader part has been named as civil wrong and the other part the crime or offence. “Writers on English legal history have often mentioned that in early law there was no clear distinction between criminal and civil offences – There is indeed no fundamental or inherent difference between a crime and a tort. Any conduct which harms an individual to some extent harms society, since society is made up of individuals. The difference is one of degree only7.

The system of crime management includes preventive measures, surveillance and censuring potential offenders, recorded offenders and their associates. The present work deals with the control and management of cyber crimes only, being a rapidly growing concern in the cyber space. The issue of cyber crime, being a part of the crime generally is also directly connected to the traditional crime management with need of scientific and sophisticated means and equipments, such as concept of crime, principles of criminal liability procedural can, partly with substantive law, law enforcing authorities, judicial approach to trial and punishment, reformation and correction.

The Information Technology Act 2000 has also dealt with the subject of cyber crime. And the policy of crime management under IT Act has divided the subject in two broad groups u/s 43 under Chapter IX and other u/s 65 to Sec. 75 under Chapter XI. “Though the focus of the Act is not on cyber crimes as such the Act defines certain defenses and penalties that deal with acts and omissions falling under the term cyber crimes. Chapter XI of the Act deals with offences and Chapter IX deals with penalties and adjudication.

Chapter IX brings a welcome changes in the minds of law makers as, may be for the first time Indian Parliamentarians have come out of their obsession with the idea of ‘criminalization’ as the sole means of regulating human conduct and upholding societal peace and tranquility and introduced civil liabilities as an alternative8.

N. Kamath has stated that “The Crime management under the IT Act largely depends on the existing crime management infrastructure and the criminal law. And the Act has made some necessary and relevant changes in law of Evidence and the

8. Supra I – P. 12.
Indian Penal Code, though, however, with some deviations of procedural law in relation to the entry, search or arrest u/s 80. "It was this provision for search without warrant in public places that caused a stir during the discussions on the Bill just prior to passing it into law. However the provision was passed untouched the provision of a clause of such nature is clearly to try through quick preventative action to control the misuse of public Internet access system such as those found at cyber cases. It may be noted that there can be no search of this nature of private homes or offices and the provisions of the code of criminal procedure, as they stand, will be applicable to such a case."

The Information Technology Act 2000 enacted following U.N. Model law face global challenge of cyber-offences also deals with particular branch of crimes. The Information Technology Act, 2000 providing to prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislation.

The IT Act, 2000 imposes criminal liability on offences such as Tampering with Computer Source document (u/s 65), Hacking with Computer System u/s 66, and also publishing of information which is obscene in electronic form (u/s 67), and accessing a protected computer (u/s 70).

5.3 CONVENTION ON CYBER CRIME

The Convention on cyber crime was opened at Budapest on 23 November, 2001 for signatures. It was the first ever-international treaty on Criminal offences committed against or with the help of computer networks such as the Internet.

The Convention deals in particular with offences related to infringement of copyright, computer – related fraud, child pornography and offences connected with network security. It also covers a series of procedural powers such as secretes of and interception of material on computer networks. Its main aim as set out in the preamble is to pursue “a common criminal policy aimed at the protection of society against cyber crime inter alia by adopting appropriate legislation and fostering international cooperation”.

5.4 STRATEGY FOR PREVENTION OF COMPUTER CRIME

In light of proliferation of computer technology, the impacts of computer crime have become enormous. Hence a multi pronged strategy is required to fight the menace to its

logical end. The two main dimensions of the strategy are, systemic methodology and legal deterrents.

5.4.1 (a) **Systemic Methodology**

Computer crime is a form of criminal offence that pervades through transnational borders. Concerted international co-operation is required to effectively address this crime.

International collaborations and exchange of technology pertaining to data security should be vigorously encouraged.

It has become imperative to develop concepts/guidelines (manual) for computer security. The implementation of such manual at all levels within an organization and between organizations, should be made mandatory. Such guidelines/manual when earnestly implemented, hold greater prospects of success than, enacting new legislations for data protection. It should be made obligatory on the part of companies/ institutions to provide in their annual reports, a confirmation to the effect that data security standards as prescribed by the manual have been adopted.

A transaction oriented system need permit only ‘read only’ or ‘inquiry only’ access. This offers a greater degree of protection than a system offering access for programming.

5.4.2 (b) **Legal Deterrents**

Demarcation of the activities which constitute offences which are non-offences.

Amendment of the domestic Criminal Law (of all countries), based on an international understanding to meet the requirement of prevention of computer related crime.

Effective prosecution, inter-alia, by adopting the existing criminal procedure law and related provisions.

The formulation and adoption of a procedure for the investigation of computer crime is cardinal to the effective translation into action, of any new piece of legislation or amendment /supplementation of existing law. The guidelines/rules should spell out the procedural aspects relating to search of the premises, seizure of incriminating documents/materials, the duty of witnesses etc.

In addition to the above considering the fast changing nature of computer-related crime, it is desirable to adapt the guidelines and classification suggested by the Organisation for Economic Co-operation and Development (OECD) with necessary amendments to suite national requirements11.

5.4.3 **INVESTIGATION**

It is the duty of every state to prosecute and set the law in motion and bring the criminals in the court of law for punishment.

The code of criminal procedure, 1973 gives to the police unfettered power to investigate all cases where they suspect that a cognizable offence has been committed.

5.5 **CYBER CRIME CELL**

A Cyber Crime cell was started at corps of Detective – Head Quarters, Bangalore to deal with Cyber Crime. The Cyber Crime cell started functioning at Corps of Detectives – Head Quarters, Bangalore from 21-10-1999. The Cyber crime cell was declared as cyber crime police station on 13th September 2001.

The cyber crime police station shall have jurisdiction in respect of all the offences, committed under The Information Technology Act, 2000 (Central Act No. 21 of 2000) or offences relating to Intellectual Property Rights (Source Internet).

5.5.1 **Working of Cyber Crime Police Station**

The cyber crime police station has a strength of four Deputy Superintendents of Police and four police Inspectors assisted by supporting staff. There is one legal adviser of the rank of Deputy Director of prosecution assisting the police officers on legal issues. Depending upon legal and technical requirement, assistance from outside experts is also taken. Functioning of cyber crime police station is supervised by Superintendent of Police
t.

5.6 **Professional efforts of International Criminal Police Organization (Interpol)**

Many international organizations quality for professional organizations, because their goals and activities are focused on certain specific issues; those organizations include Interpol, the International Telecommunications Union etc. However professional efforts here primarily mean substantial actions in the field of cyber security protection and cyber crime prevention. Although some other organizations also greatly contribute to coordinating cyber security protection, their emphasis is not necessarily on the law. By this standard this section only analyzes the actions of the International Criminal Police Organization (Interpol). As an international law enforcement organization with 184 members, Interpol started to tackle Computer Crime very early; coordinating law enforcement agencies and legislations in regard to which Interpol made efforts to improve counter-cyber crime capacity at the international level. A 1981 survey of members on cyber criminal law recognized dilemmas in application of existing legislation
t.

12. Source – [www.google.com](http://www.google.com)

13. Schjolberg & Tingrett, 2004
Based on the recognition of the legal gaps between countries, and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonization. Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-South Pacific and European Working parties on Information Technology crime. Besides these groups, a steering committee for Information Technology Crime was established in order to harmonize the different regional working–party initiatives. Considering the already harmonized legislation as the prerequisite for the co-ordinate law enforcement, the African working party agreed upon “the project on legislation and comparative law existing in the Africa with a view to having more African states co-signing and/or ratifying the Council of Europe Cyber crime Convention”. Apparently, legal harmonization is one of Interpol’s important task in working towards an effective law-enforcement environment. In regard to law enforcement, Interpol has provided a technical guide in cyber crime detection investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European working party on Information Technology Crime compared with the substantive and procedural law harmonization of today’s convention on cyber crime, the manual developed a technological law-enforcement model to improve the efficiency of combating cyber crime.

Along with efforts in law enforcement on cyber crime Interpol also takes distinct action to prevent cyber crime, cooperating with credit-card companies to combat payment fraud by building a data base on Interpol’s Web Site (Police Commissioners Conference Electronic Crime Working Party, 2000, P-64). As one of the necessary cooperation projects at the international level of law enforcement, cyber crime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition Interpol is making efforts to establish a network to for harvesting information relating to activities on the Internet\textsuperscript{14}.

\textsuperscript{14} Supra 12.
5.7 TECHNOLOGY, REGULATION AND LAW ENFORCEMENT

Technology and law enforcement have a mixed relationship. Sometimes technology provides benefits to law enforcement, at other times it provides benefits to criminals, and most often it does some of both. Fingerprinting, for example, is a technology that is usable by law enforcement but not by criminals. But in most cases technology will be usable both by criminals to commit crime and by either law enforcement or private citizens to fight crime, and so will offer mixed benefits.

Law enforcement is generally at the mercy of technology. Society does not prohibit the use of automobiles simply because they can be used for criminal purposes. Indeed, it is somewhat uncommon to regulate the use of technology solely based on concerns over law enforcement's ability to investigate crimes – the benefits of technology are too great to restrict it in most cases. Instead, law enforcement often depends upon regulation imposed for multiple purposes.\footnote{Douglas Thomas and Brian D. Loader - Cyber crime Law enforcement. Security and Surveillance in the information age – Edn. 2000 Routledge. P. 141-142.}

5.7.1 EFFECTIVE LAW ENFORCEMENT IS COMPLICATED

Effective law enforcement is complicated by the transnational nature of cyber space. Mechanisms of cooperation across national boarders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations.

\footnote{Sec www.cert.org.}

Although the following organizations also track reported incidents, global statistics have yet to be compiled: the National Infrastructure protection Center (NIPC), www.nipc.gov, the Computer Security Institute (CSI), www.coesi.com and the Internet Fraud Complaint Center, www.iffcctbi.gov.

\footnote{Victims of recent attacks include: Yahoo, CNN Interactive, Amazon.com.eBay, Datek online, E-Trade, ZD Net and Buy.com.) originating an attack from almost any computer in the World, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.}
Six weeks after the Love Bug attack, the Philippines outlawed most computer crimes as part of a comprehensive e-commerce statute. In order to prevent a repeat of the catastrophe that prompted this action, however, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise enforceable laws that will effectively deter all but the most determined cyber criminals.

5.8. **International impetus of criminal law reform in combating cyber crime**

Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cyber crimes. It is therefore, important to have international legal instruments ready to serve anti-crime efforts.

The international harmonizing efforts to fortify the legal battle against cyber crime, categorizing the actions into four aspects: professional law enforcement efforts, regional efforts, multi-national efforts, and global international efforts. The other important measures, the promotion of security, awareness at both international and national levels, the harmonization of legislation, coordination and cooperation between law-enforcement agencies and direct anti-cyber crime actions.

5.8.1 **FROM DOMESTIC LEGISLATION TO INTERNATIONAL HARMONIZATION**

People usually are impressed by illusory overlap between Internet space and international space. The globally connected Internet has made cyber crime a trans-border problem. The international dimension\(^{17}\), “trans-national dimension”\(^{18}\) or global dimension\(^{19}\) of cyber crime is universally perceived. While law is always territory-based the tool, the scene, the target, and the subject of cyber crime are all boundary independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. International coordination and cooperation are necessary in figuring offences commonly prohibited by every country. Many international organizations have been making efforts harmonize actions within their forums.

---

5.9 Professional efforts of International Police Organization (Interpol)

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cyber security protection and cyber crime prevention. Although some other organizations also greatly contribute to coordinating cyber security protection, their emphasis is not necessarily on the law.

As an international law-enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations in regard to which Interpol made efforts to improve counter-cyber crime capacity at the international level.

Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-south Pacific and European Working Parties on Information Technology Crime. Besides these groups, a steering Committee for Information Technology Crime was established in order to harmonize the different regional working party initiatives.

In regard to law enforcement, Interpol has provided a technical guidance in cyber crime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime. Compared with the substantive and procedural law harmonization of today's convention on cyber crime, the Manual developed a technological law-enforcement model to improve the efficiency of combating cyber crime.

Along with efforts in law enforcement on cyber crime, Interpol also takes distinct actions to prevent cyber crime, cooperating with credit card companies to combat payment fraud by building a database on Interpol's website20. As are of the necessary cooperation projects at the international level of law-enforcement, cyber crime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish a network for harvesting information relating to activities on the Internet.

5.10 Regional efforts

There are many regional international organizations, with a narrow or broad coverage of states more or less making efforts to maintain cyber security and harmonize international measures to combat cyber crime.

(i) The Asia-Pacific Economic Co-operation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cyber security and to tackle the risks brought about by Cyber crime (APEC 2003). The APEC has conducted a capacity building project on cyber crime for member economies in relation to legal structures and investigative abilities where the advanced APEC economies support other member-economies in training legislative and investigative personnel.

The U.S. proposed the judge and prosecutor cyber crime capacity Building project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (Judges and Prosecutors).

(ii) The Council of Europe (COE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s. In 1981, the Council of Europe implemented the convention for the protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January, 1981), which was revised according to the Amendment to Convention ETS No. 108.

In 2004 Conference on Cyber crime, the Council of Europe called for “wide and rapid: access to and “effective implementation” of the convention, raising awareness in the highest political level and encouraging cooperation between public and private sectors.

On the 2005 Conference on Cyber crime, the Council of Europe expressed concern about the fast increasing threats and serious social and economic results of cyber crime including terrorist activity on the Internet, noting that most cyber crime is international cyber crime, recognized the need for effective and compatible laws and took to enable cooperation, and encouraging access to the Convention on Cyber crime.
In 2006, the Council of Europe launched a project against Cyber crime, intended to grant assistance to the development of national legislation in line with the provision of the convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5, contact points in international cooperation.

(iii) The European Union

The EU took a series of actions to tackle cyber crime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cyber crime field.

In 1995, the European parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on protection of Individuals with regard to the processing of personal data and on the Movement of such data. Section VIII of the Directive specifically deals with confidentiality and securing of processing of personal data.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the processing of personal Data and the protection of privacy in the Telecommunications sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the Member States’ provision to attain on equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2). On 27 November 2001, a plenary session took place in Brussels of the EU Forum on cyber crime, organized by the EC, and where the primary discussion was about the retention of traffic data (EU Forum on Cyber crime, 2001).

In April, 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on Attacks against information Systems, and this proposal constitutes the case of the Decision of 24 February 2005. The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Commission further considered the future possibility of “Specific protection measures” to broadband networks.
(iv) The Organization of American States (OAS):

As other regional organizations, the organization of American States (OAS) with 35 member states is also highly concerned about the issue of cyber crime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americans (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cyber crime and protecting the Internet. Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cyber crime (The Group of Experts) in March 1999. The Group of Experts has been devoted to analyzing cyber crimes, to inspecting the domestic cyber crime law, and to a finding ways of cooperating in the Inter-American System of containing cyber crime.

The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA III) has urged member states to take steps to endorse cyber crime law; harmonize cyber crime laws to make international cooperation possible. The meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA V) has recommended that member states evaluate the availability of implanting the principles of the convention on Cyber crime, and consider the possibility of acceding to that conservation.

In 2004, the Fourth Plenary Session of the Organization of the American States General Assembly passed the resolution on Adoption of a Comprehensive Inter-American Strategy to combat Threats to Cyber Security: A Multi-dimensional and Multi-disciplinary Approach to Creating a Culture of Cyber Security, "proposing that "An effective cyber security strategy must recognize that the security of the network of information systems that comprise the Internet requiring a partnership between government and industry.

5.11 MULTI-NATIONAL EFFORTS

(i) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related
Within the Commonwealth’s 563 member countries the “Model Law” has had a wide influence on domestic legislation. Through this model law, the Conservation on cyber crime has become one of the legislative choices in substantive Criminal law, covering the offences of illegal access, interfering with data interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the convention on cyber crime, the Model Law also covered the problem of dual criminality by stating that the act applied to an act done or an omission made by a national of a state outside its territory, if the person’s conduct would also constitute an offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in the convention on cyber crime.

Another focus of the Commonwealth is on mutual assistance in law enforcement between Commonwealth member States and between Commonwealth member states and non-commonwealth member states. In the 2005 Meeting of Commonwealth : Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures for improving domestic law enforcement and trans-national assistance and encouraged member states to sign, ratify, accede to and implement the convention on Cyber crime as a basis for mutual legal assistance between Commonwealth member States and non-Commonwealth States.

(ii) The Group Of Eights (G 8)

Since the mid-1990s, the Group of Eight (G 8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax summit 1995, the Group of seven recognized “that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime”. The group released 40-point set of “recommendations to combat Transnational organized crime efficiently” at the G 7/ P 8 Lyon Summit. The recommendations urged the states to increase the level of criminalization,

prosecution, investigation and international cooperation, while acknowledging in their entirely human-rights protection. The Group of Eight Meeting of the Justice and Interior Ministers of December 1997 responded to the increased international movement of criminals, organized crimes and terrorists and their use of the ICT.

At the subsequent Summits, the Group of Eight repeatedly expressed their concern about cyber criminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society adopted the principle of international collaboration and harmonization of cyber crime. “In order to maximize the social and economic benefits of the information society” the Group of Eight agreed on principles and approaches for the protection of privacy, the free flow of information and the security of transactions. The charter recognized that the security of the information society necessitated coordinated action and effective policy responses.

(iii) The Organization for Economic Cooperation and Development (OECD)

With its 30 member-countries, the OECD addressed computer security for several decades. In 1983 an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal law reform (Schjolberg & Hubband, 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage. The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002.

5.12 Global International Efforts by the United Nations (UN).

There are numerous global organizations, nevertheless, the UN is capable of being identified as the only global organization that forms a forum of its 191 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to contain domains. Compared with regional organizations, the UN does not limit its activities to certain states. The actions of the UN have unique advantages in coordinating international positions.
In 1990, the General Assembly of the UN adopted the Guidelines concerning Computerized Personal Data Files. It proposed to take appropriate measures to protect the files against both natural and artificial dangers.

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by Schjdberg and Hubbard (2005), checking Resolutions 55/63 (2000) and 56/121 (2001) on combating the Criminal Misuse of Information Technology, the value of the group of Eight principles.

In Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse.

a. To ensure the elimination of safe havens for cyber criminals;

b. To coordinate cooperation in the investigation and prosecution of cyber crime;

c. To exchange information for fighting cyber crime;

d. To train and equip law-enforcement personnel to address cyber crime;

e. To protect the security of data and computer systems from cyber crime;

f. To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

g. To ensure mutual assistance regimes for the timely investigation of cyber crime and the timely gathering and exchange of evidence;

h. To remind the general public of the requirement to prevent and combat cyber crime;

i. To design information technologies to help to prevent and detect cyber crime;

j. To take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight cyber crime.

The General Assembly invited states to consider the measures in their endeavour to fight the criminal misuse of information systems, and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session.22

22. Susan W. Brenner Professor of Law & Technology, University of Dayton School of Law, Dayton, Ohio, Website: http://www.cybercrimes.net, P. 81, Source: Internet.
Cyber crime posses great challenges:

Cyber crime posses great challenges for law enforcement and for society in general. To understand why this is true, it is necessary to understand why and how, cyber crime differs from traditional terrestrial crime.

One characteristic of cyber crime is its disrespect for national boundaries. As a report issued several years ago noted, effective law enforcement is hampered by the "transnational nature of cyber crime. Mechanisms of cooperation across national borders to solve and prosecute crimes and complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes".\(^\text{23}\).

Concluding Comments:

In the new millennium, national boundaries have little meaning in cyberspace. The infrastructure and communication and information technology that makes up cyberspace is global in nature. Because of this global nature of cyberspace, the existing vulnerabilities are open to the world and to anyone, anywhere, who has sufficient capability to exploit them. The only way to protect the world is to have a sound knowledge of cyber crime and to pay heed to warnings from cyber security experts.

One reason for the increasing alarm is the apparent lack of effective legislation against cyber crime and India has to tighten its legislative framework in this regard. The country hardly has any cyber crime legislation. The I.T. Act, contains some laws to tackle cyber crimes, but enforcing them seems to be extremely difficult. The Internet Service Providers(ISPs) that are a good source for information about the activities of their subscribers will often keep these records and log files confidential.

\(^{23}\)Supra 20 – p. 81.
The four aspects of action to curve cyber crimes are professional law enforcement efforts, regional efforts, multi-national efforts, and international efforts. The other important measures are the promotion of security, awareness at both international and national levels, the harmonization of legislation, co-ordination and co-operation between law-enforcement agencies and direct anti-cyber crime actions.