CHAPTER - IV
“Cyberspace, as the fifth common space-after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. Deterrence against cyber threats may best be achieved through a global United Nations framework. A cyberspace Treaty, including cybersecurity and cyber crime, should be the framework for peace and security in cyberspace”.

----- By Judge Stein Schjolberg, Norway

The swift expansion of cyberspace and Internet generated new opening for cyber criminal committing crime in the cyber space. They take an opportunity of weaknesses of the countries and assault on the critical information infrastructure of the countries. The effect of cyber crimes and cyberattacks is worth mentioning in terms of lost revenues, loss of sensitive data, and damage caused to equipment. The future advancement and potential of the online information society are in danger from growing threats cyber crimes and cyber attacks. Cybercrime is a global in nature and it creates problems for the global society and it needs a coordination among all stakeholders with their involvement to combat with the cyber crime globally.

The progressive developments of cyber threats against sovereign States, such as massive and co-ordinated attacks against critical information infrastructures, will necessitate a global response. Regional and bilateral agreements may not be sufficient. International Law is necessary to make the global community able to deter the urgent and increasing cyber threats.

506 Stein Schjolberg Chief Judge is an international expert on global harmonisation of cyber crime legislations. He has served as an expert for several international institutions and organizations since 1980. He was in 2007-2008 the Chairman of the High-level-experts Group(HLEG) at the International Telecommunication Union(ITU) in Geneva. See www.cybercrimelaw.net
4. COMPARATIVE STUDY OF CYBER LAWS OF DIFFERENT COUNTRIES IN THE WORLD

4.1- INTERNET AS A UNIVERSAL STANDARD

The Internet was originally invented and designed for research and its founding protocols were designed for in-built redundancy and openness. The Internet was built for research and not for trade and commerce. Its protocols were open and unsecured; it was not designed to hide. Data transmitted over this net could easily be intercepted and stolen; confidential data could not easily be protected. The rapid growth of the computer networks that includes the Internet shifted the focus of a government from research work to the e-commerce. This domestic arena has provided a gateway for criminals and unexpected entrepreneurs to commit the crimes on the net.

Everybody has a legitimate right on the Cyber-space and everyone deserves the right to access to. Due to advent of technology and wide spread use of internet and computers many countries enacted their domestic cyber laws as there are so many problems of cyber crimes and the various countries facing the music of cyber crimes now a days. Due to the rapid growth of the Internet and social networking in cyberspace illustrated that Information and communications technologies are now a part of the everyday life. Whenever anybody searching for travel information or booking railway tickets and doing online reservation for his journey or performing online banking it means that anybody can easily perform these functions at any time and as per the his own convenience either at home or office. Information and communications technologies are therefore turn out to be an essential function of trade and business and in turn commerce and government. With the help of computers and the Internet, businesses and banks are
now enough competent to provide instant services to their customers at an unexpected level of competence\textsuperscript{507}.

Challenges before the governments of the various countries is how to regulate a technology that permits rapid transactions across the continents and hemispheres are uneven across guarded national and jurisdictional borders. This state of affairs points toward the desirability of arrangements at the international level to overcome these procedural barriers.

Every government has played a key role in both the development of information technology and in the efforts to deal with new challenges that arise from its use. Solutions to the new challenges posed by information technology are inherently horizontal in nature and require an inclusive approach to policy development, involving a wide variety of stakeholders both inside and outside government.

Many countries have their own criminal laws which were derived from the legal systems which involve a combination of English law, Roman Dutch law and constitutional law. These laws are disseminated to apply to traditional crimes such as murder, assault, theft and fraud. A problem therefore arises when these outdated procedural laws are tackled with contraventions that arise in the IT environment.

The inadequacy of existing criminal laws to address computer offences has led to the introduction of new legislation to keep abreast with modern technology. Traditionally, crime and punishment were seen to be locally based, regional or national. However, this has changed today with the transnational character of cybercrime posing many problems. The globally connected Internet has made cybercrime a trans-border problem. For many nations, international cybercrime and investigation is more important than purely domestic cybercrime and investigation\textsuperscript{508}.

Law enforcement officials cannot prosecute cyber criminals unless countries have adequate laws in place outlawing such criminal activities. Cybercrime is said to be becoming easier to carry out as society becomes more dependent on the Internet. This increases the risk of a catastrophic attack.

\textsuperscript{507} Roderick Broadhurst and Yao-chung Chang, article ‘Cybercrime in Asia: trends and challenges’ Drafted on 5.1.2012 source: http://ssrn.com/abstract=2118322

\textsuperscript{508} Joseph J. Schwerha, Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from “Cloud Computing Providers
Therefore, the international character of cybercrime calls for international coordination and co-operation to address computer-related offences worldwide. International cybercrime has been viewed as a growing issue by many entities. In order to fight transnational cybercrime, it is widely agreed that there is a need for an international convention that has universal application.

4.2-NEED FOR INTERNATIONAL HARMONIZATION TO FIGHT WITH CYBER CRIME

It is the proven fact that internet operations don’t know any geographical and territorial boundaries. Only for this reason the cyber criminals commit the crime in one country without physically present at the place of crime. The international support and cooperation is required by the countries in the world to tackle the problem of growing cyber crimes for the mutual understanding, United Nation has been done lot of efforts for the member countries to foster co-operations among them to handle the challenges of cyber criminality. Though the response from the member countries is not much encouraging but common consciousness among the concerned countries to prevent the cyber crime the only alternative is the mutual co-operation and trans-border assistance. The ever emergent use of computers and ICT in the world has opened up a range of new activities for crime to take place by using the electronic means on a global scale, irrespective of national and transnational limits. The efficient warfare, investigation and prosecution of such crimes require international cooperation between countries and law enforcement agencies backed by laws, international relations, conventions, directives and recommendations concluding in a set of international guidelines to fight cybercrime. There are many challenges to international cooperation and establishing international guidelines to fight global cybercrime across borders. There is a prerequisite for the harmonization of countries’ criminal laws, the sanction of complex jurisdictional issues and the development of new cooperation procedures to challenge cybercrime. It is necessary to identify the perpetrators across borders anywhere in the world, and to investigate and to secure electronic evidence of their crimes so that they may be

brought to justice in any compliant jurisdiction with fairness and compliance with human rights standards. This is a discouraging task in itself.510.

4.3-ATTEMPTS MADE AT GLOBAL LEVEL TO FIGHT CYBER CRIME
One of the most significant reasons in criminal legislation is the control of criminal offenses. A prospective offender must also in cyberspace be given a clear warning with adequate predictability that certain offences will not be tolerated. And when criminal offences occur, offenders must be punished for the crime explicitly done in order to discourage him or her, and others from such crime. These basic principles are also valid for cybercrimes. Cybercrime, including massive and synchronized cyber assault on the country against critical information infrastructure and terrorist misuse of the Internet, are global crimes. Cyberspace has made a new environment for criminal offenses. Through international organizations fighting against the cyber crimes, pains must be taken to ensure that there is a similarity of provisions in the individual countries. Harmonization of this type may be achieved by means of conventions, recommendations or guidelines. In order to achieve a global harmonization of cybercrime legislation, and a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, a global agreement or Protocol at the United Nations level should be established that includes solutions aimed at addressing the global challenges.
A convention or a treaty is normally a more binding agreement, where countries are parties to the treaty may be held liable under international law for breaches of the agreement. A Memorandum of Understanding (MoU) is normally executed but it is a more loosely agreement. It usually indicates a common line of action between multilateral countries those who are parties to the treaty. A MoU is normally used in situations where parties either do not involve a legal commitment or in circumstances where the countries cannot create a legally enforcement agreement. It is a more formal alternative to a gentlemen’s agreement511. Even if a MoU is not binding under international law, it should be registered in the United Nations treaty database.

The most active UN-institution in reaching harmonization on global cybersecurity and cybercrime legislation is the International Telecommunication Union (ITU) for developing a global agreement or protocol on cybersecurity and cybercrime\(^{512}\)

4.3(A). THE PIONEERS FOR FIGHTING AGAINST THE CYBER CRIME GLOBALLY

Several individuals were engaged in the fight against computer crime as under:

1) **Donn B. Parker (USA)**: was the founder father of the knowledge of computer crime. He was the researcher of computer crime and security from the early 1970. He served as a Senior Computer Security Consultant at the SRI\(^{513}\) International and was the main author of the first basic federal manual for law enforcement in USA: “Computer Crime–Criminal Justice Resource Manual” (1979)\(^{514}\) made for the National Criminal Justice Information and Statistics Service, by the Law Enforcement Assistance Administration LEAA (370 pages) and became soon an encyclopedia

2) **August Bequai (USA)**: was the authors in USA that contributing in the fight against computer crime in those days.

3) **Jay Bloombecker (USA)** He wrote Computer Crime, Lexington Books, USA (1978)

4) **Stein Schjolberg (Norway)**: was a police attorney and prosecutor from 1976. He assisted Interpol from 1979 in the development of knowledge of this new phenomenon.

5) **Ulrich Sieber (Germany)**: - was involved as an academician at the University of Freiburg. He assisted early on many international organisations, such as OECD from 1983 and United Nations. He was later appointed as a professor at the Max Planck University. He has assisted many international organizations: The OECD as a consultant for the guidelines published in 1986, United Nations in 1989, and the Council of Europe for the Organised Crime Report (2004).

6) **H. W. K. Kaspersen (Netherland)**: was another academician, was early involved and became later the “father” of the Council of Europe Cybercrime Convention, through his initiative in 1997.

\(^{511}\) See http://en.wikipedia.org/wiki/MoU/
\(^{513}\) Stanford Research Institute International

4.3(B). INTERNATIONAL HARMONIZATION TO FIGHT WITH CYBER CRIMES

Following are the attempts to fight with cyber crime

1) Council of Europe (1976)
The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. In this conference several categories of computer crime were introduced.515

2) The Ribikoff Bill
In the United States a staff study by the U.S. Senate Government Operations Committee in February 1977 was the first comprehensive initiative on computer crime. The staff study addressed several problems associated with computer programs, and recommended that legislation should be considered that would prohibit unauthorized use of computers. The Chairman of this committee was Senator Abe Ribicoff.516

Later in 1977 Senator Ribicoff introduced the Ribikoff Bill. This Bill was the first proposal for Federal computer crime legislation in the U.S. that would specifically prohibit misuse of computers. The Bill S. 1766 (95th Congress) was cited the “Federal Computer Systems Protection Act of 1977”. The Bill was not adopted, but this pioneer proposal raised awareness around the world as to the potential problems that unauthorized computer usage could cause and the need to define the scope of the topic in order to adequately address the problems in a comprehensive but flexible way.

3) Interpol
Interpol was the first international organization addressing computer crime and penal legislation at a Conference in Paris in 1979. In a presentation on computer frauds it emphasized as follows:

516 Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977
517 Congressional Record, 95th Congress, Vol. 123, No. 111, June 27, 1977
518 Congressional Record, 95th Congress, Vol. 123, No. 111, June 27, 1977
The nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc. between the different countries. International organizations, like Interpol, should give this aspect more attention. In concurrence with this Conference a summary of answers from Interpol member countries on computer crime and penal legislation identified several legislative areas with unsatisfactorily existing penal legislation, such as:

a) Modification and erasure of data, or otherwise affecting data processing with destructive intent,
b) Appropriation or obtaining data belonging to another with intent to gain the perpetrator,
c) Obtaining, without authority, computer services for one's own purpose, using a computer belonging to another,
d) Modification of data with fraudulent intent, or with intent to be used in legal transactions,
e) Disclosure of data without authority.


In 1982 the OECD in Paris decided on appointing an expert committee\textsuperscript{519} to discuss computer-related crime and the need for changes in the Penal Codes. A group of experts met at the OECD in Paris on May 30, 1983: Mme C.M.Pitrat, France, Mr. M. Masse, France, Mr. A. Norman, United Kingdom, Mr. S. Schjolberg, Norway, Mr. B. de Schutter, Belgium, and Mr. U. Sieber, Germany. These" founders " of the harmonization of European computer crime legislation recommended that the OECD should take an initiative. An expert committee was established, and recommended in September 18, 1986 through the ICCP Committee a common denominator between the different approaches taken by the Member countries. As a result of the expert committee proposals, the ICCP-Committee of the OECD highly recommended in 1986

5) The Council of Europe Recommendations of 1989\textsuperscript{520}.

\textsuperscript{519} A group of experts met at the OECD in Paris on May 30, 1983:

\textsuperscript{520} Computer-related crime: Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe On 13 September 1989 and Report by the European Committee on Crime Problems. (Published in Strasbourg 1990)
The Council of Europe appointed in 1985 another expert committees in order to discuss the legal issues of computer–related crime. A summary of the guidelines for national legislatures with liability for intentional acts only, was presented in the Recommendation of 1989.

It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer program and unauthorized reproduction of topography


The participation of both developed and developing nations in international computer-crime initiatives is an encouraging trend. For example, the three associated conferences on computer crime at Wurzburg in October 1992 were attended by delegates from Africa, Asia, eastern and western Europe, Latin America, the Middle East and North America. An adequate response to computer crime requires that both developed and developing nations should encourage regional and international organizations to examine the issue and promote crime prevention programmes on a national level. The draft resolution of the AIDP Colloquium, held at Wurzburg, 5-8 October 1992, contains a number of recommendations, including the following:

1) To the extent that traditional criminal law is not sufficient, modification of existing, or the creation of new offences should be supported of other measures are not sufficient

2) In the enactment of amendments and new provisions, emphasis should be put on precision and clarity.

3) In order to avoid over-criminalization, regard should be given to the scope to which criminal law extends in related areas. Extensions that range beyond these limits require careful examination and justification.

7) The Council of Europe Recommendations of 1995\textsuperscript{521}

The Council of Europe adopted on September 11, 1995, another Recommendation concerning problems of procedural law connected with Information Technology.

---

\textsuperscript{521} Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995,
This Recommendation introduces 18 principles categorized in 7 chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international co-operation

8) 22nd G-7 Summit on Cyber Crime was held at the in Lyon, France (1996)\(^5\)

The 22nd G7 Summit was held at the in Lyon, France between June 27 and 29, 1996. The Group of Seven (G7) was an unofficial forum which brought together the heads of the richest industrialized countries: France, Germany, Italy, Japan, The United Kingdom, The United States & Canada (since 1976) and the President of the European Commission.

Issues which were discussed at this summit included:

- Strengthening Economic And Monetary Cooperation
- Promoting Strong And Mutually Beneficial Growth Of Trade And Investment
- Enhancing Our Approach To Employment Problems
- Implementing A New Global Partnership For Development: An Ambition For The 21st Century
- Enhancing The Effectiveness Of Multilateral Institutions For The Benefit Of Development
- Providing The Necessary Multilateral Support For Development
- Toward Successful Integration Of Countries in transition into the global economy

9) The High Tech Subgroup of the G-8 Group of States.(1998)\(^6\)

The High Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime, developed and established in 1998 (24X7) network of experts to assist in high-tech crime investigation. The goal was to ensure that no criminal receives safe haven anywhere in the world, and that the law enforcement authorities have the technical ability and legal process to find criminals who abuse technologies and bring them to justice. Other countries have joined the network and are participating in the co-operation. The G-8 Group has also agreed upon principles that should apply when law enforcement agents employed by law enforcement agencies are investigating criminal

\(^5\) http://en.wikipedia.org/wiki/22nd_G7summit
\(^6\) G-8 consists of the following States: Canada, France, Italy, Japan, Russia, United Kingdom, Germany and USA. See www.g7.utoronto.ca
offenses and require assistance in other countries. Such principles should be implemented through treaties and through national laws and policies\textsuperscript{524}. Principles on accessing data stored in a foreign state preservation of stored data in a computer system.

**10) G-8 Paris Conference (2000)\textsuperscript{525}**

The Conference to Focus on High-Tech Crime, Seeks to Find International Solutions from 15\textsuperscript{th} to 17\textsuperscript{th} May2000 was held at Paris and arranged by Symantec Corp. (Nasdaq: SYMC), a world leader in Internet security technology, invited to join the U.S. delegation at the G-8 conference to strengthen exchanges between public and private entities, commercial and administrative sectors, and between countries. Delegates at the conference will also conduct threat evaluations on newly developed technologies to identify possible misuse by criminals. The conference is part of an ongoing series of meetings focused on enhancing the abilities of law enforcement to investigate and prosecute high-tech and computer related crime.

**11) DIRECTIVE ON E-COMMERCE OF THE EUROPEAN COUNCIL (2000)\textsuperscript{526}**

The Electronic Commerce Directive, adopted in 2000, sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike. It establishes harmonized rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers. The proper functioning of the Internal Market in electronic commerce is ensured by the Internal Market clause, which means that information society services are, in principle, subject to the law of the Member State in which the service provider is established. In turn, the Member State in which the information society service is received cannot restrict incoming services.


\textsuperscript{525}http://www.symantec.com/region/can/eng/press/2000/n000515.html

\textsuperscript{526}http://ec.europa.eu/internal_market/e-commerce/directive/
12) The Council of Europe at Budapest, Hungary (2001)\textsuperscript{527}

The Council of European Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001. This Convention is a historic milestone in the combat against cybercrime, and entered into force on July 1, 2004. The number of signatures not followed by ratifications are 23 States and the number of ratifications/accessions are 23 States (December 2008). An Additional Protocol on the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of January 2003 has also been adopted. Provisions of procedural law shall apply on any criminal offence committed by means of a computer system, and to the collection on evidence in electronic form of a criminal offence. The provisions contain expedited preservation of stored computer data, production order, search and seizure of stored computer data, real-time collection of computer data.

13) International Conference on E-Security, Cyber Crime and Law (2004)\textsuperscript{528}

The Mahatma Gandhi State Institute of Public Administration, Government of Punjab (MGSIPAP) has organized a two day “Conference on e-Security, Cyber Crime & Law” on 19-20 February 2004 at Chandigarh.

Computer security has become a legal and a technical issue of critical importance for many organizations and the Government. Discussed the legal liabilities arising from security issues, policies and procedures - beyond the “bits and bytes.” The conference was focused on Data Security, Cyber Crimes and Cyber Laws. The Conference was had deliberations on following four Tracks


Track II: Data and Transmission Standards Data Encryption Methods Electronic Fund Transfer and Security of Data Banking and e-Funds Transfer Data Protection & e-Governance

\textsuperscript{527} See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
\textsuperscript{528} http://www.allconferences.com/conferences/2003/
Track III: Detecting Cyber Crime Components of Computer Forensics Preserving Computer Evidence Computer Forensics Practices Adopted by the Police and other Enforcement Agencies

Track IV: Data Protection legislations, policing the cyberspace, role of judiciary in the digital age network security and Law.

An International Cyber Crime Conference was organized by the Computer Crime Research Centre World Anti-criminal Anti-terrorist Forum (WAAF), Zaporozhye State University, with the help of The Transnational Crime and Corruption Center (Tra CCC), Ukraine on May 26-28, 2004. The Cyber Crime Conference deliberations on the following issues:
- Fighting Cyber Crime.
- Fighting Cyber Terrorism.
- Legal Aspects Of Information Security.

15) Asian Pacific Economic Cooperation (APEC) (2004)\textsuperscript{529}
APEC Leaders acknowledged the threat that corruption poses to good governance and economic growth in the Asia-Pacific when they met in Santiago, Chile in 2004. There was a mutual understanding that APEC economies should nurture and sustain good governance, economic development and prosperity by working together to fight corruption and ensure transparency. To advance this work, Leaders endorsed the Santiago Commitment to Fight Corruption and Ensure Transparency and the APEC Course of Action on Fighting Corruption and Ensuring Transparency. The following year an Anti-Corruption and Transparency Experts' Task Force (ACT) was established.

16) ASEAN Regional Forum Bangkok (China) (2004)\textsuperscript{530}
The Association of Southeast Asian Nations (ASEAN) has established high level Ministerial Meeting on Transnational Crime (AMMTC). At the Meeting in Bangkok,

\textsuperscript{530} http://www.nti.org/treaties-and-regimes/association-southeast-asian-nations-asean/
January 8, 2004, a statement included cyber crime was recognized and the need for an effective legal cooperation to enhance the fight against transnational crime. A Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity was signed on October 8, 2003, in Bali, Indonesia. ASEAN and China will pursue the following joint actions and measures: Formulate cooperative and emergency response procedures for purposes of maintaining and enhancing cybersecurity, and preventing and combating cybercrime.

17) Eleventh Congress on Prevention of Crime and Treatment of Offenders (2005)\textsuperscript{531}

The Eleventh Congress was convened at a momentous period in the history of the United Nations Crime Prevention and Criminal Justice programme held in Bangkok on 18-25 April, 2005. The international community had witnessed the entry into force of major international instruments, namely, the United Nations Convention against Transnational Organized Crime and two of its additional protocols (the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and the Protocol against Smuggling of Migrants by Land, Sea and Air supplementing the Convention). In the months following the Eleventh Congress, also the third supplementary Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition and the United Nations Convention against Corruption received the required number of ratifications and entered into force.

18) International Cyber Crime Conference, Brazil (2006)\textsuperscript{532}

Hundreds of computer specialists in fields varying from cyber forensics to digital law met in Brazil to discuss the Internet and Terrorism, among other things. The gathering was the Third International Conference on Cyber Crime, held in Brasilia Nov. 6-9. Icc.org reported on its Web site Nov. 13 that among the law enforcement organizations that sent members to the conference were INTERPOL, EUROPOL, the U.S. Federal Bureau of Investigation, the Canadian Mounted Police, Spain’s Guardia Civil, Australia’s Federal Police, the Federal Police of Brazil, Italy’s Federal Police, Finland’s Federal Police, the Netherlands’ Federal Police, the Federal Police of Mexico, the National

\textsuperscript{531} http://www.asc41.com/UN_congress/undocs.htm

\textsuperscript{532} http://www.4law.co.il/april06.htm
Police of Japan, Canada's Toronto Metropolitan Police, Britain's SOCA-e-crime and the U.S. Departments of Justice and Homeland Security and the U.S. Secret Service. The event was held in conjunction with the First International Conference on Forensic Computer Science. Brazil's Department of Federal Police and the National Institute of Crime Investigation helped sponsor the conference.

19) Seventh International Conference on Cyber Crime New Delhi (India) (2007)

7th International Conference on Cyber-Crime was held on 12 September 2007, New Delhi, India. Shri Shivraj Patil Union Home Minister in his speech has elaborated that the software, computer and Internet – all designed to promote efficient services, higher productivity and greater convenience, reducing the gap in both space and time to bring the world closer. The conference deliberates the message that computer generated terrorist activities and organized crimes through internet should be control.


The 3rd International Conference on Legal, Security, and Privacy Issues in IT Law (LSPI) was held in Prague, Czech Republic under the auspices of the International Association of IT Lawyers, an organization devoted to promoting research and development in the field of Law and with members throughout the world. 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.

21) International Conference on Terrorism and Organized Crimes (2008)

An International Conference on Terrorism and Organized Crimes was held in Anaheim (USA) on August 25, 2008. There was deliberations in the conference on International & Domestic Terrorism Trends, Weapons of Mass Destruction, Organized Crime (Russian, Asian, Euroasian, Armenian, Italian, and Israeli), Human Smuggling &
Trafficking, Regional Updates on Gangs, Identity Theft, Drug Trafficking, International Money-Laundering, Dangerous Mail, and Computer Forensics

22) Conference on Cyber Security Protective Strategies (2009)\textsuperscript{536}

An International Conference on Cyber Security and Protective Strategies was held on November 2-3, 2009 in Gatineau (Quebec). A Cyber security threats are increasing, which has implications for businesses, governments, and community organization. member countries and emphasized the need for further cooperation and coordination to fight cyber criminality.

23) International Conference on Digital Forensics and Cyber Crime (2009)\textsuperscript{537}

Digital Forensics and Cyber Crime - First International ICST Conference, ICDF2C 2009, Albany, NY, USA, September 30-October 2, 2009, Revised Selected Papers on the field of digital forensics is becoming very important for law enforcement, network security, and information assurance. This is a multidisciplinary area that encompasses multiple fields, including: law, computer science, finance, networking, data mining, and criminal justice. The applications of this technology are far reaching including: law enforcement, disaster recovery, accounting frauds, homeland security, and information warfare.

24) Fifth Annual Conference on Cyber Crime, Council of Europe (2010)\textsuperscript{538}

Fifth Annual Conference was held in Strasbourg on March 25, 2010. The Council of Europe has called for a worldwide implementation of its Convention on Cybercrime to fight the growing problem of economic crime on the web. During the fifth annual CoE conference on cybrecrime in Strasburg this week, participants spoke in favour of greater international cooperation in sharing existing tools, instruments, best practices and initiatives. The conference also heard calls for improved co-operation between law enforcement and industry (ISPs, IT firm and national CETS). The conference also considered the security and privacy implications of greater use of cloud-based technology, making a number of recommendations.

\textsuperscript{536} http://sso.conferenceboard.ca/Libraries/CONF_PDFS_PUBLIC/09-0170.sflb
\textsuperscript{537} http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=5123&copyownerid=3167
\textsuperscript{538} http://www.theregister.co.uk/2010/03/26/cybercrime_conference/

Twelfth United Nations Congress on Crime Prevention and Criminal Justice was held at Salvador, Brazil, 12-19 April 2010. This Crime Congress marked the fifty-fifth anniversary of United Nations congresses on crime prevention and criminal justice. The agenda of the Twelfth Congress was focused on: children, youth and crime; smuggling of migrants; trafficking in persons; money-laundering; and cybercrime. The deliberations were held in-depth as under:

- Establishing firmly the criminal justice system as a central pillar in the rule-of-law architecture;
- Highlighting the pivotal role of the criminal justice system in development;

Emphasizing the need for a holistic approach to criminal justice system reform to strengthen the capacity of criminal justice systems in dealing with crime.

26) Fourth International Conference on Cyber Law (August 2010)\(^{539}\)

The 4th International Conference on Cyber law was held at Virginia (US) on 18-20 August 2010. During the conference, academics and members of the judiciary have exchanged ideas and discussed most recent topics focusing on Cyber law. The deliberations were on bringing together leading academics from all over the world, the conference will explore comparative approaches to intellectual property and discuss privacy, information technology and other Cyber law issues.

*****

\(^{539}\) http://www.cyberlaw-conference.org/
4.4. CYBERCRIME LEGISLATION OF THE VARIOUS COUNTRIES IN THE WORLD

4.4.1. WESTERN EUROPE

1) Austria
Cyber crimes are dealt with the provisions of Austria’s Cyber Crime Act 2001, which came into effect on 2001.

2) Belgium
In November, 2000, the Belgian Parliament adopted new legislation ‘Loi sur la criminalité informatique’ which would insert a series of new articles, dealt with computer crime, into the Belgian Criminal Code.

3) Denmark
The Danish Penal Code also known as The Danish Criminal Code is the codification of and the foundation of criminal law in Denmark.

4) Finland
Cyber Crimes are dealt with the provisions of Finnish Penal Code.

5) France
Cyber crimes are dealt with French penal code (1994) No cyber law enacted.

6) Germany
Cyber crimes are governed by the provisions of German Criminal Code in Germany.

7) Greece
The Cyber crimes are governed by the provisions of Greek Penal Code in Greece.

8) Iceland
The Cyber crimes are governed by the provisions of Iceland Penal Code in Iceland.

---

9) Ireland
In Ireland Cyber crimes are governed by the provisions of Regulation on Unsolicited Communications 2008

10) Italy
In Italy the Cyber Crimes are dealt with the provisions of “Legge Anticriminalità” enacted in 2008

11) Luxembourg
Luxembourg Penal Code makes it an offense either to fraudulently gain access to a computer system or to alter, suppress or modify data contained in such a way to govern the cyber crimes in Luxemburg

12) Malta
On January 8, 2001, the Parliament enacted the Electronic Commerce Act, which adds a new section, entitled “Computer Misuse”, to the Maltese Criminal Code to facilitate to govern the cyber crimes in Malta.

13) The Netherlands
The Netherlands Criminal Code is enacted to control the cybercrimes in the Netherland

14) Norway
The Cyber crimes are governed by the provisions of Norway Penal Code in Iceland

15) Portugal
Criminal Information Law of August 17, 1991 in the name & style “Lei 109/91-Lei da Criminalidade Informatica” is enacted in the Portugal to control the cyber crime

16) Spain
Cyber crimes in Spain are dealt with Spanish Penal Code, Article 197, McConnell International, Cyber Security Legislation. Now the new enactment came into existence since 2010 in the name and style as Royal Decree 3/2010
17) **Sweden**

In Sweden, cyber crimes are governed by “The Data Act 1973” (as amended with effect from January 1, 1989)

18) **Switzerland**

Cyber crimes in Switzerland are governed by the provisions of the Swiss Penal Code.

19) **United Kingdom**

The Cyber law to control cyber crimes in United Kingdom’s is the Computer Misuse Act of 1990 and Regulation of Investigatory Power Act 2000

20) **Romania**

The Cyber law to control cyber crimes in Romania is Provisions on Preventing and Fighting Cybercrime 2003

### 4.4.2. RUSSIA AND EASTERN EUROPE

Countries of Central and Eastern Europe have generally made less progress in reforming their legal systems to incorporate cybercrime, though Russia stands as an exception\(^{541}\).

1) **Albania**

Cyber crimes in Albania are governed by the provisions of The Criminal Code of the Republic of Albania,

2) **The Federation of Bosnia and Herzegovina**

The criminal code of The Federation of Bosnia and Herzegovina is enacted to dealt with the cyber crimes in Bosnia and Herzegovina

3) **Bulgaria**

The Bulgarian criminal code has established crimes involving computers in two separate categories; crimes against intellectual property and general economic crimes.

---

4) **Czech Republic**
The cyber crimes in Czech Republic are governed by the provisions of “The Criminal Code of Czech Republic”

5) **Estonia**
The cyber crimes in Estonia are governed with the provisions of “The Criminal Code of Czech Republic” Estonian Penal Code

6) **Hungary**
Hungary’s only cybercrime-specific penal legislation is a provision criminalizing computer fraud with Penal Code of Hungary.

7) **Latvia**
The cyber crimes in Latvia are governed by the provisions of Criminal Law of Latvia

8) **Poland**
The Polish Penal Code criminalizes the cyber crimes in Poland.

9) **Russia**

10) **Slovenia**
There is no special legislation dealing with computer crime in force in Slovenia. Cyber crimes are governed by the provisions of Slovene Criminal Procedure Code in Slovenia

11) **Yugoslavia**
Yugoslavia has enacted several laws attempting to address cyber crimes. These include laws on the information system of the government agencies and organization of FRY (“Official Gazette of FRY” No.59/98) and laws on the protection of personal data (“Official Gazette of FRY”, No. 24/98).
4.4.3. NORTH AMERICA 542

1) Canada
Canada criminalizes a number of computer-related offenses, including computer mischief; data theft; invasion of privacy; computer fraud; and hacking/cracking and virus dissemination are governed by Canadian Criminal Code.

2) United States of America
Cybercrime legislation has been adopted at both the state and federal levels. Cyber crimes in USA are dealt with the Federal Computer Fraud and abuse Statute and Related Federal Criminal Laws2008, and Child Online Protection Act (COPA)

4.4.4. SOUTH AND CENTRAL AMERICA AND THE CARRIBBEAN

1) Argentina
Cyber crimes in Argentina is governed by the cyber law of Argentina “Ley 26.388/2008 - Delitos Informaticos”2008 and the Argentina Penal Code

2) Barbados
Barbados has not enacted any specific cyber crime legislation543.

3) Brazil
On July 14, 2000, amendments to Brazil’s Penal Code were enacted, to go into effect ninety days after the date the amendments were published. The amendments created two new offenses: the “entry of false data” into an information system; and the unauthorized modification or alteration “of the information system or computer program by an employee”. On August 8, 2001, “Project de Lei da Camara n. 84/1999,” was enacted specifically targeted at cybercrimes

4) Chile
Chile’s Law on Automated Data Processing Crimes no. 19223, published June 7, 1993 criminalizes espionage on automated systems nomenclature as “Ley 19223/1993-Ley Reletiva a Delitos Informaticos”

543 Director of Public Prosecutions of Barbados
5) Costa Rica
The cyber laws in Costa Rica are governed by the provisions of the Costa Rican Penal Code.

6) Cuba
Cyber crimes in Cuba are governed by the provisions of the Penal Code of Cuba.

7) Ecuador
Ecuador’s penal code does not speak of cybercrime. There are no criminal laws in Ecuador which prohibit “computer crimes” such as computer trespass, vandalism, or interception of computer communications.

8) El Salvador
There are no laws on the books in El Salvador which prohibit the alteration, interception, or destruction of computer information. Computer systems are not defined nor referenced within El Salvadorian criminal law. Despite the lack of substantive law relative to computer crime in El Salvador, training courses on the subject have been started and are in progress in the Office of the Attorney General of the Republic.

9) Mexico
Cyber crimes are controlled by the provisions of Mexican Federal Penal Code in Mexico.

10) Nicaragua
Cyber crimes in Nicaragua are governed by the provisions of the Nicaragua Penal Code as Nicaragua had no cybercrime specific laws in place.

11) Panama
Cyber crimes are controlled in Panama by the provisions of The Criminal Code of the Republic of Panama. In the Republic of Panama there are no specifically defined and punishable crime relating to computer crime.

12) Peru
In April of 2000, Peru added two computer crime provisions to its Penal Code. The provisions criminalize the unauthorized use of a computer system and damaging, altering or destroying data or computer programs.
13) Trinidad and Tobago
The cyber crimes of Trinidad and Tobago are controlled by the provisions of The Computer Misuse Act, 1999.

14) Venezuela
Venezuelan criminal law does penalize the unauthorized interception and transmission of computer data and information by Ley Especial Contra los Delitos Informaticos the cyber law of Venezuela

4.4.5. ASIA 544
1) Bangladesh
Bangladesh’s responses to a United Nations survey on cybercrime law indicate that it has not adopted cybercrime-specific penal legislation. Cybercrimes in Bangladesh are dealt with Penal Code of Bangladesh

2) Burma (Myanmar)
Cyber crimes are governed by the Computer Science Development Law enacted in September 1996. This legislation includes titles, definitions, and objectives for computer development within Burma (Myanmar)

3) People’s Republic of China
The bulk of China’s cybercrime provisions are contained in its “Computer Information Network and Internet Security, Protection and Management Regulations”, which were promulgated to “strengthen the security and the protection of computer information networks and of the Internet, and to preserve the social order and social stability.”

4) Hong Kong
Cyber crimes are controlled by the provisions of Telecommunication Ordinance and the Crimes Ordinance of Hong Kong.

5) India
India’s cybercrime legislation is set out in “The Information Technology Act, 2000”. The offenses are set out in Chapter XI of the Act. The Act was further amendment in 2008 and now termed as Information Technology Amendment Act 2008.

6) Japan
Japan has a cyber law namely “Law No.128 of 1999 –Unauthorized Computer Access Law” In April of 2002, Japanese officials announced that they intended to put forward legislation which would criminalize the online transmission of child pornography.

7) Malaysia
Malaysia’s cybercrime legislation is contained in the “Computer Crimes Act 1997.”

8) Mauritius
Mauritius’ cybercrime legislation is the product of its “Information Technology Act 1998”. Section 4 of the Act amended the Mauritius Criminal Code to add two new offenses: a data protection and security offense; and computer misuse.

9) Pakistan
Pakistan enacted the Prevention of Electronic Crimes Ordinance, 2008(Ordinance No. IX) in 2008 and all the crimes related to cyber space are governed with this Act.

10) Philippines
The Republic of the Philippines adopted the “Electronic Commerce Act” which, among other things, created several new cyber-offenses. The act was enacted after six weeks after the dissemination of the “Love Bug” virus.

11) Singapore
Singapore’s cybercrime legislation appears in the Computer Misuse Act which was adopted in 1998 which dealt with the cybercrimes in Singapore.

12) South Korea
South Korea has two methods of implementing computer crime laws. They have established numerous articles within their criminal code, which went into effect on July 1, 1996, and they have implemented the Promotion of Utilization of Information and Communications Network Act, which went into effect on July 1, 1999.
13) Taiwan
In 1997, Taiwan amended its Criminal Code to include prohibitions directed at several varieties of cybercrime. The cyber crimes in Taiwan are dealt with the provisions of Taiwan’s Criminal Code

14) Vietnam
Vietnam has recently enacted new legislation to prosecute Internet related crimes. Included in the new legislation is Article 41 which addresses administrative breaches of regulations, Article 224 of the Penal Code of Vietnam. Hence the crimes related to cyber space are governed with Penal code of Vietnam

15) Shri Lanka
Cyber Crimes in Shri Lanka are governed by the provisions of computer Crime Act 2007

16) Thailand
Cyber Crimes in Thailand are governed by the provisions of computer Crime Act 2007

4.4.6. NORTH AFRICA AND THE MIDDLE EAST

1) Egypt
The cyber crimes are governed by the provisions of the Penal Code of Egypt.

2) Iran
The cyber crimes are governed by the provisions of Penal Code of Iran.

3) Israel
Israel’s cybercrime legislation appears in its Computers Law, 5755, which has been in effect since 1995. The Computers Law creates the following offenses: disrupting or interfering with the operation of a computer; disseminating “specious information” or “specious output”; unauthorized programs.

4) Jordan
Jordan had no cybercrime specific laws in place. Subscribers to Internet services are explicitly required to abide by the laws applicable in Jordan, especially pertaining to publications, limitations on opinions expressed, and all the relevant Jordanian laws.
5) Kazakhstan
Kazakhstan currently had no cybercrime specific laws in place. The cyber crimes in Kazakhstan are governed by the provisions of penal code of Kazakhstan.

6) Lebanon
The cyber crimes in Lebanon are governed by the provisions of Penal Code of Lebanon.

7) Morocco
Morocco currently had no cybercrime specific laws in place, but that an “inter-ministerial commission sponsored by the Prime Minister” was “working on security issues.”

8) Oman
Rules and regulations of an ISP entitled GTO prohibit unauthorized or unlawful gaining or trying to gain access to any computer systems or networks through the use of the ISP services and any unlawful activities which are contrary to the social, cultural, political, religious or economical values of the Sultanate of Oman.

9) Saudi Arabia
All communications are routed through a state proxy-server, which blocks access to sites deemed unacceptable for religious, moral, national security, or other reasons set out by the state.

10) Sudan
Sudan had no cybercrime specific laws in place. Cyber crimes in Sudan are governed by the provisions of Penal code of Sudan.

11) Syria
No specific Cyber Laws are in Syria. Cyber Crimes are governed by the existing penal code of Syria. The Syrian Electronic Army (S.E.A.), “a group of hackers who support President Bashar al-Assad of Syria to control cyber crimes in Syria

12) Tunisia
Tunisia has not enacted any specific cyber crime legislation. All cyber crimes are dealt with the penal code of Tunisia

13) Turkey
Cyber crimes in Turkey are governed by the provisions of Internet Law of Turkey
14) United Arab Emirates
UAE is governed by The Federal Law No. (5) of 2012 on - The Prevention of Information Technology Crimes to control the cyber crimes in UAE

4.4.7. **SUB-SAHARAN AFRICA**

1) **Gambia**
Cyber crimes in Gambia are governed by the provisions of the Information and Communication Act 2009 of Gambia

2) **Kenya**
Kenya Communications (Amendment) Act 2008 is dealing with the cyber crimes in Kenya

3) **Lesotho**
Currently Lesotho had no cybercrime specific laws in place. Cyber crimes are dealt with the provisions of penal code of Lesotho

4) **Nigeria**
Cyber crimes are dealt with the provisions of Nigerian Cybercrime and Cyber secuirty Act 2004”, in Nigeria

5) **South Africa**
Cyber crimes are dealt with the provisions of Electronic Communications and Transactions Act 2002

6) **Zambia**
Cyber crimes are dealt with the provisions of Computer Misuse and Crimes Act 2007

7) **Zimbabwe**
Cyber crimes are dealt with the provisions of Penal code of Zimbabwe as it had no cybercrime specific laws in place

8) **Antigua and Barbuda**
Cyber crimes are dealt with the provisions of The Computer Misuse Act 2006

9) **Bermuda**
Cyber crimes are dealt with the provisions of The Computer Misuse Act 2006
10) Cameroun
Cyber crimes are dealt with Cyber sécurité et la Cybercriminalité au Cameroun

11) Tonga
Cyber crimes are dealt with the provisions of The Computer Crimes Act 2003

12) Uruguay
Cyber crimes are dealt with the provisions of Ley n. 17.838 - Proteccion de Datos Personales para ser Utilizados en Informes Comercialesy Accion de Habeas Data

4.4.8. AUSTRALIA, NEW ZEALAND AND THE PACIFIC ISLANDS

1) Australia
Cyber crimes are dealt with the provisions of Cyber Crime Act 2001

2) Fiji Islands
The Fiji Islands have not enacted any specific cyber crime legislation. 7

3) New Zealand
Cyber Crimes are dealt with the provisions of New Zealand was drafting a Crimes Amendment Act
4.5-COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE OFFENCES AGAINST E-BANKING

Different countries have enacted their cyber legislations to control the cyber crimes in the different categories usually committed against banking. Following are the cyber crimes under different categories and enactment of different countries to control those crimes.

4.5.1. COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE OFFENCES OF UNAUTHORIZED ACCESS AND UNAUTHORIZED DISRUPTION TO COMPUTERS & COMPUTERS PROGRAMMES

The offences against banking of the nature of criminal liabilities are further categories as under:-

a) **Unauthorized Access** to Computers and Computer Programs

b) **Unauthorized Disruption** to Computers and Computer Programmes i.e.
   i) Viruses, ii) Worms, iii) Trojan Horses, iv) Distributed Denial of Service and Bot Software

1) THE COUNCIL OF EUROPEAN UNION

The Council of European Union Convention has the following enactment to curb and control the cyber crimes of illegal access, illegal interception, data intrusion, system interference and misuse of computer devices. Also unauthorized disruption to computers and computer programmes are controlled with the following provisions as under:-

**Section 1 - Substantive criminal law**^545^  
*Offences against the confidentiality, integrity and availability of computer data and systems*

**Article 2 - Illegal Access**

*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of*

---

obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 3 - Illegal Interception**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electro magnetonic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article 4 - Data Interference (Intrusion)**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally to damage, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

**Article 5 - System Interference**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

**Article 6 - Misuse of Devices**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   a) The production, sale, procurement for use, import, distribution or otherwise making available of:

   - a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5

   - a computer password, access code, or similar data by which the whole or any part of
a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2-5, and b) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2) AUSTRALIA

Australia has the following enactment to hold down and control the cyber crimes of unauthorized access to or modification of restricted data. Also unauthorized disruption to computers and computer programmes are controlled with the following provisions as under:-


Unauthorized access to or modification of restricted data

1. A person is guilty of an offence if:
   a) The person causes any unauthorized access to, or modification of, restricted data;
   b) The person intends to cause the access or modification; and
   c) The person knows that the access or modification is unauthorized; and
   d) One or more of the following applies:
      (i) The restricted data is held in a Commonwealth computer;
      (ii) The restricted data is held on behalf of the Commonwealth;
      (iii) The access to, or modification of, the restricted data is caused by means of a telecommunications service.

Penalty: 2 years imprisonment.

2. Absolute liability applies to paragraph (1)(d)

3. In this section: restricted data means data.
   a) Held in a computer; and
   b) To which access is restricted by an access control system associated with a function of the computer

3) AUSTRIA
Austria has the following enactment to control the cyber crimes of willfully obtained unlawful access, intentionally transmit data in violation of the data secrecy clause, *Use data contrary to a legal judgment or decision and intentionally delete data*. Unauthorized disruption to computers and computer programmes are also controlled with following provisions as under:-

**Privacy Act 2000, effective as of January 2000**

**Section 10: Administrative Penalty Clause**

Provided that the offence does not meet the statutory definition of a punishable action within the relevant jurisdiction of the court nor is threatened by a more severe punishment under a different administrative penalty clause, a minor administrative offence shall be pronounced with a fine of up to S260.000. Parties who

1. **Willfully obtain unlawful access** to a data application or willfully maintain discernable, unlawful, and deliberate access or
2. **Intentionally transmit data in violation of the Data Secrecy Clause** (15), especially data that were entrusted to him/her according to 46 and 47, for intentional use for other purposes or
3. **Use data contrary to a legal judgment or decision**, withhold data, fail to correct false data, fail to delete data or
4. **Intentionally delete data** contrary to, Section 7.

4) BELGIUM
Following four main offences relating to forgery, computer fraud, hacking and sabotage are treated as criminal offences by the Belgian Parliament with effect from February 2001. The four main offences i.e. computer forgery, computer fraud, hacking and sabotage are made criminal offences. Unauthorized disruption to computers and computer programmes are controlled with the following provisions

**Computer Hacking**

**Article 550(b) of the Criminal Code**

---

547 [www.oecd.org](http://www.oecd.org) › Austria
548 [www.cybercrimelaw.net/Belgium.html](http://www.cybercrimelaw.net/Belgium.html)
1. Any person who, aware that he is not authorized, accesses or maintains his access to a computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of (Belgium franc 5,200-5m) or to one of these sentences. If the offence specified above is committed with intention to defraud, the term of imprisonment may be from 6 months to 2 years.

2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to a term of imprisonment of 6 months to 2 years and to a fine of (Belgium Franc 5,200-20m) or to one of these sentences.

3. Any person finding himself in one of the situations specified and who either: accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or makes any use whatsoever of a computer system, or causes any damage, even unintentionally, to a computer system or to data which is stored, processed or transmitted by such a system, may be sentenced to a term of imprisonment of 1 to 3 years and to a fine of (Belgium Franc 5,200-10m) or to one of these sentences.

4. The attempt to commit one of the offences specified is sanctioned by the same sentences as the offence itself.

5. Any person who, with intention to defraud or with the intention to cause harm, seeks, assembles, supplies, diffuses or commercializes data which is stored, processed or transmitted by a computer system and by means of which the offences specified may be committed, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of (Belgium Franc 5,200-20m) or to one of these sentences.

6. Any person who orders or incites one of the offences specified to be committed may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of (Belgium France 5,200-40m) or to one of these sentences.

7. Any person who, aware that data has been obtained by the commission of one of the offences specified, holds, reveals or divulges to another person, or makes any use whatsoever of data thus obtained, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of (Belgium France 5,200-20m) or to one of these sentences.
5) BRAZIL
Brazil has the following enactment to curb and control the cyber crimes regarding entry of false data comes under the category of unauthorized access to computers. Also unauthorized disruption to computers and computer programmes are controlled with the following provisions as under:-

Law no. 9,983 of July 2000\(^{549}\) has been adopted covering provisions Entry of False Data into the Information System.

**Art. 313-A.** Entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the information system or the data bank of the Public Management for purposes of achieving an improper advantage for himself or for some other person, or of causing damages. Penalty-imprisonment for 2 to 12 years and fines. Unauthorized Modification Or Alteration Of The Information System. **Art. 313-B.** Modification or alteration of the information system or computer program by an employee, without authorization by or at the request of a competent authority. Penalty-detention for 3 months to 2 years and fine. The penalties are increased by one-third (one terco) until one-half if the modification or alteration results in damage to the Public Management or to the individual

6) CANADA
Canada has the following enactment to hold back and control the cyber crimes of unauthorized access to computers and unauthorized disruption to computers and computer programmes are also controlled with the following provisions as under:-

**Canadian Criminal Code\(^{550}\)**

Section 342.1 states:

1. Everyone who, fraudulently and without color of right,  
   a) Obtains, directly or indirectly, any computer service,  
   b) By means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system.  
   c) Uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation

\(^{549}\) [www.cybercrimelaw.net/Brazil.html](http://www.cybercrimelaw.net/Brazil.html)  
to data or a computer system, or

d) Uses, possesses, traffics in or permits another person to have access to a computer
password that would enable a person to commit an offence under paragraph (a), (b) or
(c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding
ten years, or is guilty of an offence punishable on summary conviction.

7) DENMARK

Canada has the following enactment to curb and control the cyber crimes of
unauthorized access and unauthorized disruption to computers and computer
programmes to computers as under:-

Penal Code Section 263551:
Any person who, in an unlawful manner, obtains access to another person’s information
or programs which are meant to be used in a data processing system shall be liable to a
fine, to simple detention or to imprisonment for a term not exceeding 6 months.
If an act of the kind described in subsection 1 or 2 is committed with the intent to
procure or make oneself acquainted with information concerning trade secrets of a
company or under other extraordinary aggravating circumstances, the punishment shall
be increased to imprisonment for a term not exceeding 2 years.

8) GERMANY

Germany has the following enactment to curb and control the cyber crimes related to
data espionage, alteration data and computer sabotage as under:-

German Criminal Code552
Penal Code Section 202a. Data Espionage:
1. Any person who obtains without authorization, for himself or for another, data which
are not meant for him and which are specially protected against unauthorized access,
shall be liable to imprisonment for a term not exceeding three years or to a fine.
2. Data within the meaning of subsection 1 are only such as are stored or transmitted
electronically or magnetically or in any form not directly visible.

552 www.gesetze-im-internet.de/englisch_stgb/
Penal Code Section 303a: Alteration of Data

1. Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.

(2) The attempt shall be punishable.

Penal Code Section 303b: Computer Sabotage

1. Imprisonment not exceeding five years or a fine shall be imposed on any person who interferes with data processing which is of essential importance to another business, another's enterprise or an administrative authority by: committing an offense under section 300a(1) or destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier.

(2) The attempt shall be punishable

9) JAPAN

Japan has the following enactment to seize and control the cyber crimes unauthorized computer access by various ways. Likewise Also unauthorized disruption to computers is controlled with the following provisions as under:-


Article 3. No person shall conduct an act of unauthorized computer access.

2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:

a) 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 persons 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 the authorized user for that identification code);

b) An act of making available a restricted specific use by making in operation a specific

553 www.cybercrimelaw.net/Japan.htm
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);

c) An act of making available a restricted specific use by making 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, any information or command that can evade the restriction concerned.

**Article 4.** 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 computer’s 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.

**Article 8.** A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:

1. A person who has infringed the provision of Article 3, paragraph 1;

**Article 9.** A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

10) **SOUTH AFRICA**

South Africa has the following enactment to curb and manage the cyber crimes related to unauthorized access of data as under:-

The Electronic Communications and Transactions Act Of July 31 2002 (Act No. 25, 2002)  
**Chapter XIII, Cyber Crime**

Unauthorized access to interception of or interference with data.
Sec.86.1. Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

2. A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

3. A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item to contravene this section, is guilty of an offence.

4. A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

5. A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence. Penalties

Sec.88. 1. A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), Sec80 (5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

2. A person convicted of an offence referred to in sections 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.

11) SWITZERLAND

Switzerland has the following enactment to curb and control the cyber crimes of unauthorized access to data processing system as under:-

Penal Code Article 143bis\textsuperscript{555}. Unauthorized access to data processing system.

\textsuperscript{555} www.admin.ch/ch/e/rs/3/311.0.en.pdf
Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.

12) UNITED KINGDOM

United Kingdom has the following enactment to curb and control the cyber crimes as described in the above paragraphs as under:-

**Computer Misuse Act 1990**

**Unauthorized access to computer material:**

1. A person is guilty of an offense if
   a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer,
   b) The access he intends to secure is unauthorized, and
   c) He knows at the time when he causes the computer to perform the function that that is the case.

2. The intent a person has to have to commit an offense under this section need not to be directed at:
   a) Any particular program or data,
   b) A program or data of any particular kind, or
   c) A program or data held in any particular computer.

3. A person guilty of an offense under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

A person is guilty of an offense under this section if he commits an offense under section 1 above (the unauthorized access offense) with intent

a) To commit an offense to which this section applies; or

b) To facilitate the commission of such an offense (whether by himself or by any other person); and the offense he intends to commit or facilitate is referred to below in this section as the further offense.

This section applies to offences

a) For which the sentence is fixed by law; or
b) For which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates Courts Act 1980).

It is immaterial for the purposes of this section whether the further offense is to be committed on the same occasion as the unauthorized access offense or on any future occasion.

A person may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible.

A person guilty of an offense under this section shall be liable
a) On summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and
b) On conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

A person is guilty of an offense if -

a) He does any act which causes an unauthorized modification of the contents of any computer; and
b) At the time when he does the act he has the requisite intent and the requisite knowledge.

For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any and by so doing -

a) To impair the operation of any computer;
b) To prevent or hinder access to any program or data held in any computer;
c) To impair the operation of any such program or the reliability of any such data.

The intent need not be directed at
a) Any particular computer;
b) Any particular program or data or program or data of any particular kind;
c) Any particular modification or a modification of any particular kind.

For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorized.
It is immaterial for the purposes of this section whether an unauthorized modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

For the purposes of the Criminal Damage Act 1971 a modification of the contents of a Computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

A person guilty of an offense under this section shall be liable
a) On summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
b) On conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

13) USA
USA has the following enactment to curb and control the cyber crimes of fraud & related activity, as under:-


Fraud and related activity in connection with computers.

Whoever-

1) Having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained 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 defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit

\textsuperscript{557}www.law.cornell.edu/uscode/
or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
   (A) 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 (15 USC. 1681 et seq.);
   (B) Information from any department or agency of the United States; or
   (C) Information from any protected computer if the conduct involved an interstate or foreign communication;

3) Intentionally, without authorization to access any nonpublic 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 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 that use by or for the Government of the United States;

4) Knowingly and with the intent to defraud, accesses a protected 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 and the value of such use is not more than $ 5,000 in any one-year period;

5) i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
   ii) Intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage; or
   iii) Intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)-
i) Loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least USD 5,000 in value;
ii) The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
iii) Physical injury to any person;
iv) A threat to public health or safety; or
v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; password or similar information through which a computer may be accessed without authorization, if
A) such trafficking affects interstate or foreign commerce; or
B) such computer is used by or for the Government of the United States;
7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State or of an intelligence agency of the United States.

United States has a statute to prevent hacker to intrude the computer without the permission.

Section 1030(a) (4) of title 18 of the United States Code states in full:
“Whoever ... knowingly and with intent to defraud, accesses a protected 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.”
14 FRANCE
France has the following enactment to curb the cyber crimes of unauthorized access to the computers as under:-

Article 323-1 of the French penal code (1994) *Unauthorized access to the computer*

Article 323-1 of the French penal code (1994) contains the following provision:

“*Fraudulently obtaining or maintaining access to the whole or part of a system for automated data processing is punishable by [imprisonment and a fine]*”.

15) THE NETHERLANDS

The Netherlands has the following enactment to control the cyber crimes of intentionally unlawfully intrusion into a computer system as under:-

Article 138-a) of the penal code of the Netherlands for unauthorized access to the computer a have the following provisions:

A person who intentionally unlawfully intrudes into a computerized device or system for storing or processing data or a part of such a device or system is guilty of computer intrusion and liable to a term of imprisonment of not more than six months or a fine of the third category, where he: thereby breaches any security, or gains access by technological means, with the help of false signals or a false key, or by assuming a false capacity. Computer intrusion is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently copies the data stored in a computerized device or system, to which he has gained access unlawfully, and records such data for his own use or that of another.

16) INDIA

India has the following enactment to curtail and control the cyber crimes of hacking and, spreading Viruses, Worms and Trojans as under:-

The Information Technology Act, 2000 (ITA 2000) and Amendment Act 2008 (ITAA)

---

558 www.frenchlaw.com/criminal_law.htm  
559 www.ejcl.org/143/art143-10.pdf
**Section 66. Hacking with computer system.**

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

2. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

**Legal remedy available for spreading Viruses, Worms and Trojans In India**

Legal remedy is available under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 and under Section 268 of Indian Penal Code, 1860. Spreading of Virus offence is cognizable offence with bailable and compoundable with a permission of the court before which the prosecution of such offence is pending. It can be trialed before any magistrate.

**CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHER COUNTRIES.**

Total sixteen enactments of the different countries and their provisions related to unauthorized access and unauthorized disruption to computers & computers programmes are examined. The enactments of the various countries examined in this regards are found to be the legislations to control offences related with unauthorized access and unauthorized disruption to computers & computers programmes. In India these offences are dealt with the provisions of Information Technology Act 2000 and its Amendment i.e Information Technology Act 2008 vide Section 66 of the IT Act 2000 and Section 43[c] and 43[e] of IT Amendment Act 2008. Also Section 268 of Indian Penal Code 1860 is also applicable to these offences.

The cutting of certain elements of the effects of hacking under the existing Section 66 and putting the same under Section 43 make no legal or pragmatic sense.

The Information Technology Act talks about unauthorized access but it does not talk about maintaining integrity of customer transactions. The act does not lay down any

---

560 wwww.mondaq.com/.../An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes...
duty upon banks to protect the details of customers and clients. U.K has a data protection law which was enacted 10 years back of the enactment of Indian law under which banks or any person holding sensitive information may be held liable for damages if it fails to maintain adequate security protection in respect of data. Section 268 of the Indian Penal Code throw light on the public nuisance which is an offence against the public either by doing a thing which tends to annoy the community in general, or by neglecting to do anything which the common good requires. It cannot be disputed that viruses and worms are perfect examples of public nuisance and the person launching them can be prosecuted under this section. Online privacy is not protected; only Section 43 (penalty for damage to computer or computer system) talks about it in some extent but doesn’t hinder the violations caused in the cyberspace.

Due to numerous Laws dealing with the subject they create the confusion to their applicability, and none of the Law deals with the subject specifically in total. Therefore it gives the impression that Indian enactment are not sufficient enough to control of cyber crimes like unauthorized access and unauthorized disruption to computers & computers programmes i.e. spreading viruses and worms against e-banking in India. However the IT Act appears sufficient in all respect but it is not efficient and sufficient to tackle the problems of such crimes as compared to the enactments of the other countries.

4.5.2. COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE OFFENCES OF CYBER TERRORISM

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.\(^{561}\)

\(^{561}\) http://en.wikipedia.org/wiki/Cyberterrorism
1) USA

USA has the following enactment to control the cyber crimes of Cyber Terrorism as under:-

Section 814 of “The Patriot Act”

This section amends section 1030(a) (5) of title 18, United States Code. The amended section punishes any person who causes unauthorized damage to a protected computer by either:

(i) Knowingly causing the transmission of a program, information, code, or command, or
(ii) Intentionally and unauthorized accessing a protected computer

This section applies only in cases where the conduct of the accused causes:

(i) Loss to one or more persons during any 1-year period aggregating at least $5,000 in value, or
(ii) The actual or potential modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, or
(iii) Physical injury to any person, or
(iv) A threat to public health or safety, or
(v) Damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Section 816 of The Patriot Act is titled Development and Support of Cyber Security Forensic Capabilities.

This section empowers the Attorney General to establish adequate regional computer forensic laboratories and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability to:

1) Provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyber-terrorism),
2) Provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer related crime (including cyber-terrorism),
3) Assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime,

www.asianlaws.org › Library › Cyber Laws
4) Facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer related crime with State and local law enforcement personnel and prosecutors, including the use of multi jurisdictional task forces, and
5) Carry out such other activities as the Attorney General considers appropriate

2) UNITED KINGDOM
As per The Terrorism Act, 2000, the term terrorism includes the use or threat of action that is
i) Designed seriously to interfere with or seriously to disrupt an electronic system
ii) Designed to influence the government or to intimidate the public or a section of the public, and
iii) Made for the purpose of advancing a political, religious or ideological cause.

3) EUROPE
The Council of European Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001. This Convention is a historic milestone in the combat against cybercrime, and entered into force on July 1, 2004. Provisions of procedural law shall apply on any criminal offence committed by means of a computer system, and to the collection on evidence in electronic form of a criminal offence. Under this Convention, states are required to establish a number of defined offenses, including crimes against the confidentiality, integrity and availability of computer systems, their processing capacity and their data content (articles 2-6). These provisions require states to prohibit most types of cyber-terrorism. Under the Convention, each member state is required to establish laws that will enable it to intercept, preserve, search and seize data on its networks. These include real-time monitoring of traffic data (article 20) and interception of content data (article 21). Article 22 of the Convention provides that each party shall extend its jurisdiction over offences committed in its territory or by its nationals.

4) INDIA
In India Cyber Terrorism was not defined by Information Technology Act 2000. Section 66 of IT Act 2000 was applied only of the act is done "Dishonestly" or "Fraudulently". In
ITAA2008, this clause has been re written with significant changes. Applies to all contraventions listed in Section 43. Fine increased to Rs 5 lakh. Section 66FITAA2008 introduced for the new offence i.e. Cyber Terrorism. This Section 66provides life sentence, though definition is not considered comprehensive. Section 69 of the Information Technology Act is a strong legislative measure to counter the use of encryption by terrorists. This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource. Any person who fails to assist the Government agency in decrypting the information sought to be intercepted is liable for imprisonment up to 7 years. By ITAA2008, two more sections were introduced i.e. 69A to enable blocking of websites and 69B provides powers for monitoring and collecting traffic data etc. Prevention of Terrorism Act 2002(POTA) also applies in the case of physical Terrorist Attack.

CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHERS
The enactments and their provisions related to the offences of cyber terrorism in USA, United Kingdom, Europe and India are examined.
In USA offences related to cyber terrorism are dealt with the Patriot Act. US PATRIOT Act stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act. The act covers 1) Enhancing domestic security against terrorism, 2) Enhanced surveillance procedures, 3) International money laundering abatement and anti-terrorist financing act of 2001, 4) Removing obstacles to investigating terrorism, 5) Strengthening the criminal laws against terrorism
In United Kingdom the specific Act was enacted as Terrorism Act, 2000.

In Europe, conference in Budapest, Hungary was held on November 23, 2001 and under this Convention, states are required to establish a number of defined offenses, including crimes against the confidentiality, integrity and availability of computer systems, their processing capacity and their data content (articles 2-6). These provisions require states to prohibit most types of cyber-terrorism.
In India Cyber Terrorism was not defined by Information Technology Act 2000. Section 66 of IT Act 2000 was applied only of the act is done "Dishonestly" or "Fraudulently". In ITAA2008 The clause has been re written with significant changes. Applies to all contraventions listed in Section 43. Fine increased to Rs 5 lakh. Section 66Fof ITAA2008 introduced for the new offence i.e. Cyber Terrorism. Section 66F of ITAA 2008 provides life sentence, though definition is not considered comprehensive. Similarly, two new section were introduced i.e. 69A to enable blocking of websites and 69B provides powers for monitoring and collecting traffic data etc. Patriot Act of USA covers in the definition of "Cyber Terrorism" to include "Propaganda, technical assistance for hosting, Phishing, Spamming etc. But this not included in Indian Act. Whatever stated above it reveals that the enactment on cyber terrorism in USA having the edge over the enactment of Indian cyber laws.

4.5.(3). COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE OFFENCES OF IDENTITY THEFT

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, usually as a method to gain access to resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.563

1) USA

The USA has the following enactment to control the cyber crimes of identity theft as under:-

Federal Trade Commission-Assumption Deterrence Act, June 1998 564

a) The term document-making implement means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;
b) The term identification document means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;
c) The term 'false identification document' means a document of a type intended or commonly accepted for the purposes of identification of individuals that is not issued by or under the authority of a governmental entity; and appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization

d) The term means of identification means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any
- name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- unique electronic identification number, address, or routing code;
- telecommunication identifying information or access device.
e) The term personal identification card means an identification document issued by a State or local government solely for the purpose of identification;
f) The term produce includes alter, authenticate, or assemble;
g) The term transfer includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of
such identification document, false identification document, or document-making implement on an online location where it is available to others.

2) EUROPEAN UNION

The European Union has the following enactment to control the cyber crimes of identity theft as under:-

Council Directive 95/46 EC 1995-Data Protection\textsuperscript{565}

\textit{a}) Personal data shall mean any information related to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

\textit{b}) Processing of personal data (processing) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Council of Europe Committee of Experts on Crime in Cyber-Space, Convention on Cyber-crime 2001\textsuperscript{566}

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

\textit{a}) Any input, alteration, deletion or suppression of computer data;

\textit{b}) Any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

3) JAPAN

Japan has the following enactment to control the cyber crimes of identity theft as under:-

\textsuperscript{565} https://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm

\textsuperscript{566} cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf
Japanese Privacy Act -2003\textsuperscript{567}

The Basic Principles of the Japanese draft law require:

\begin{itemize}
\item[a.] use of personal information for a clearly defined purpose and within the scope necessary for the achievement of that purpose;
\item[b.] the use of lawful and proper means to acquire personal information;
\item[c.] maintenance of the accuracy and currency of personal data
\item[d.] the implementation of appropriate measures to maintain the security of personal information;
\item[e.] allowing individuals access to their personal information
\end{itemize}

\textbf{4) INDIA}

The provisions of Information Technology Act, 2000 and Information Amendment Act,2008

There is no specific provision related to Identity Theft in Information Technology Act. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity is used for Identity Theft:

\textbf{Section 43}: This section makes adequate provision for unauthorized access to his personal/private data for the purpose of Identity theft\textsuperscript{568}.

\textbf{Section 66}: The account of the victim is fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server and attempt the data theft. Thus, this act is squarely covered and punishable u/s 66 IT Act\textsuperscript{569}.

\textbf{Section 66A}: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000\textsuperscript{570}.

\textbf{Section 66C}: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000\textsuperscript{571}.

\textsuperscript{567} https://www.huntonprivacyblog.com/tag/japan
\textsuperscript{568} IT ACT 2000 and ITAA2008
\textsuperscript{569} ibid
\textsuperscript{570} ibid
\textsuperscript{571} ibid
Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted.

Section 420 IPC which related to Cheating: Because phishers use false and fraudulent websites, URL Links to deceive people into disclosing valuable personal data, phishing schemes which is used later to swindle money from victim account. Thus, it is an offence of cheating punishable u/s 420 IPC.

Section 120-B IPC which relates to Criminal Conspiracy: There is also criminal conspiracy between various persons perpetrating the crime, like the persons who open the beneficiary account or who receive the funds in their account in conspiracy with the fraudster. Thus, Section 120-B IPC which relates to criminal conspiracy is also applicable.

Section 468 IPC which relates to Forgery: - Website which is in the nature of electronic record to cheat the gullible bank customers is punishable u/s 468 IPC.

Section 471 IPC which relates to Fraud: - Further fraudulently or dishonestly use as genuine, the fake website in the nature of electronic record is punishable u/s 471 IPC

CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHER COUNTRIES

Total four enactments of the different countries and their provisions related to Identity Theft are examined. The enactments of the various countries examined in this regards are found to be the legislations to control offences related with Identity Theft. In Japan specific enactment i.e. Japanese Privacy Act -2003 is there to prevent the Identity Theft. European Union also having the enactment to prevent the data theft. USA also having the specific laws to protect the Identity Theft. Theft of identity has become an increasing problem; the scam operates by obtaining information about a victim, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document

572 ibid
obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as "Social security numbers, PAN numbers" are also valuable to the identity theft. Unfortunately for the banks, identity thieves have been known to take out loans and disappear with the cash, quite content to see the wrong persons blamed when the debts go bad.

In India these offences are dealt with the provisions of ITA 2000 and ITAA 2008 vide section 43, section 66, 66(A),(C),and 66(D). Similarly Section 420 IPC which relates to cheating, Section 120(B) IPC which relates to criminal conspiracy, Section 468 IPC which relates to forgery and Section 471 IPC relates to fraud. The IT Act, 2000 does not have any specific provision to deal with Identity theft. Due to numerous Laws dealing with the subject they create the confusion to their applicability. Therefore it gives the impression that Indian enactments are not sufficient enough to control of cyber crimes like Identity Theft. On the basis of the above our analysis is that the existing cyber laws are inadequate and insufficient to control the cyber crimes like Identity as there is a massive growth in cyber crime incidents.

4.5.4. COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE OFFENCES OF SPAM

Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, and spreading malware.573

1) AUSTRALIA

Australia has the following enactment to control the cyber crimes of spam as under:

SPAM (CONSEQUENTIAL AMENDMENTS) ACT 2003 No. 130, 2003 574

The Spam Act was amended by Spam (Consequential Amendments) Act were enacted by the assent of Australian Parliament in 2003. The Acts starts its operation in April 2004.

2) CANADA

Canada has the following enactment to control the cyber crimes of Spam as under:

573 http://en.wikipedia.org/wiki/Email_spam
(1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).

(2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

(3) Subsections (1) and (2) do not apply where compliance therewith might

(a) Result in the collection of inaccurate information; or

(b) Defeat the purpose or prejudice the use for which information is collected.

3) EUROPEAN UNION

European Union has the following enactment to control the cyber crimes of Spam as under:-


---

\(^{575}\) http://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html

\(^{576}\) europa.eu › ... › Information society › Current general legal framework


\(^{578}\) www.refworld.org/docid/3ddcc6364.html

4) JAPAN
Japan has the following enactment to control the cyber crimes of Spam as under:-

Law for Appropriate Transmission of Specified Emails (Law No.26 of 2002).
The Act on Regulation of the Transmission of Specified Electronic Mail
(Act No. 26 of April 17, 2002)

Only the original Japanese texts of Acts and regulations have legal effect, and the translations are to be used solely as reference material to aid in the understanding of Japanese Acts and regulations. The Government of Japan shall not be responsible for the accuracy, reliability or currency of the legislative material provided on this Website, or for any consequence resulting from use of the information on this Website. In July 2002 MPHPT established a body Japan Data Communications Association to determine the appropriateness of sending specified e-mail messages.

5) IRELAND

6) NEW ZEALAND
New Zealand has the following enactment to control the cyber crimes of Spam as under:-

---

579 eur-lex.europa.eu › EUROPA › EUR-Lex Home
eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX...en:HTML
580 ibid
581 ibid
582 www.dataprotection.ie/docs/LAW-ON-DATA-PROTECTION/795.htm
**Privacy Act 1993 - New Zealand Legislation**

This Act may be cited as the Privacy Act 1993. (Except as provided by section 31(2), this Act shall come into force on 1 July 1993.

In this Act, unless the context otherwise requires,—

action includes failure to act; and also includes any policy or practice agency—

(a) means any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department; but

(b) Does not include—

(i) The Sovereign; or

(ii) The Governor-General or the Administrator of the Government; or

(iii) The House of Representatives; or

(iv) A member of Parliament in his or her official capacity; or

(v) The Parliamentary Service Commission; or

(vi) The Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; or

(vii) In relation to its judicial functions, a court; or

(viii) In relation to its judicial functions, a tribunal; or

(ix) An Ombudsman; or

(x) A Royal Commission; or

(xi) A commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; or

(xii) A commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; or

(xiii) In relation to its news activities, any news medium; or

(xiv) An inquiry to which section 6 of the Inquiries Act 2013 applies collect does not include receipt of unsolicited information

---

7) REPUBLIC OF KOREA
Republic of Korea has the following enactment to control the cyber crimes of Spam as under:-

**Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (Republic of Korea) - [2005] PrivL Res 2**[^584].

1) Any information and communications service provider shall protect the personal information of users, and contribute to the protection of the rights and interests of such users and to the enhancement of its information utilization capability by rendering the information and communications services in a safe and sound manner.

2) Every user shall endeavor to help a sound information society take hold.

3) The Government may assist the organizations of information and communications service providers and the organizations of users in carrying out their activities designed to protect the personal information and the youth in the information and communications networks. Korea Spam Response Center was constituted within the KISA (Korea Information Security Agency), an agency of the Ministry of Information and Communication with the specific authority to deal with problems regarding spam.

8) USA
USA has the following enactment to control the cyber crimes of Spam as under:-

**Controlling the Assault of Non-Solicited Pornography and Marketing Act**-117 Stat. 2699 Public Law 108- 187[^585]

In 2003, Congress passed a federal anti-spam law, the CAN-SPAM Act, which became effective on January 1, 2004. In enacting the law, Congress determined: (1) there is a substantial governmental interest in regulation of commercial electronic mail on a nationwide basis;

(2) Senders of commercial electronic mail should not mislead recipients as to the source or content of such e-mail; and

(3) Recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

[^584]: [http://www.worldlii.org/int/other/PrivLRes/2005/2.html](http://www.worldlii.org/int/other/PrivLRes/2005/2.html)

The Act does not ban spam outright. Instead, it establishes requirements for those who send commercial e-mail, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.

The Act has the displacing effect of state laws that specifically address spam, but not state laws that are not specific to email, such as trespass, contract or tort law, or other state laws to the extent they relate to fraud or computer crime.

9) UNITED KINGDOM
United Kingdom has the following enactment to control the cyber crimes of Spam as under:-

Privacy and Electronic Communications Regulations
Privacy and Electronic Communications Regulations (PECR) is an implementation of the European Union (EU) e-Privacy Directive in the United Kingdom. PECR regulations restrict the processing and sharing of personal traffic data and location data and provide for access to users’ personal data in the interest of national security. The information commissioner has the power to audit the measures taken by a provider of public electronic communications services to comply with personal data breach notification and recording requirements.

10) INDIA
India has the following enactment to control the cyber crimes of Spam as under:

Spamming Laws in India\textsuperscript{586}
As of today, the Indian government has yet to come out with a legislation that directly addresses the issue of spam. The Information Technology Act, 2000 (IT Act 2000) does not contain any provision regulating the act of spamming though it does regulate obscenity, which covers publishing, transmitting or causing to be published in electronic form any material which is lascivious, or appeals to the prurient interest. The Spam cases indirectly booked under Section 43 of Information Technology Act 2000.

However, as of today in India, legal remedy is available under CAUSE (Coalition Against Unsolicited Commercial Email) India is available. It is a non-profit advocacy

\textsuperscript{586} http://www.lawyersclubindia.com/articles
group that works to reduce the amount of unsolicited commercial email, or spam via legislation. CAUCE India was formed in the late 1990s

**CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHERS**

USA and the European Union have already enacted anti spam legislation. In the United States spam is legally permissible according to the CAN-SPAM Act of 2003 provided it follows certain criteria. If the spam fails to comply with any of these requirements, then it is illegal. Article 13 of the European Union Directive on Privacy and Electronic Communications (2002/58/EC) provides that the EU member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed. The major failure of the amendments of ITAA2008 is that they have not dealt with the entire issue pertaining to spam in a comprehensive manner. Spam is not mentioned in the IT Amendment Act2008. India has not given any importance to the issues and problems of spam.

In India, there is no enactment on spam to control the problems of spam. This make India a paradise as far as spam is concerned. The various global surveys indicates that India find the place in the top ten nations from where spam originates.

**4.5.5.COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE INCIDENTS OF DIGITAL OR ELECTRONIC EVIDENCE**

Most electronic records are generally admitted in the court. The digitization and emerging use of ICT has a huge impact on procedures for the collection of evidence and its use in court. Prior to the amendment by ITAct, 2000, the definition of ‘Evidence’ in section 3 of the Indian Evidence Act, 1872 was as follows.

“Evidence” means and includes:

(3) All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under enquiry, such statements are called oral evidence.

(4) All documents produced for the inspection of the Court, such documents are called documentary evidence

---

587 Section 3 of the Indian Evidence Act, 1872
The aforesaid definition has now been amended by the IT Act, 2000 which reads as 588:

(3) All statements which the court permits or requires to be made before it by Witnesses, in relation to matters of fact under enquiry; such statements are Called oral evidence

(4) All documents including electronic records produced for the inspection of the court, such documents are called documentary evidence.

1) EUROPEAN UNION

European Union has the following enactment on the Digital and Electronic Evidences as under:-

Convention on Cyber-crime, 2001589

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a) the criminal offences established in accordance with articles 2-11 of this Convention;

b) other criminal offences committed by means of a computer system; and

c) the collection of evidence in electronic form of a criminal offence.

3. a) Each Party may reserve the right to apply the measures referred to in Article 20

588 IT Act 2000
589 www.magnin.org
only to offences or categories of offences specified in the reservation, provided that the
range of such offences or categories of offences is not more restricted than the range of
offences to which it applies the measures referred to in Article 21. Each Party shall
consider restricting such a reservation to enable the broadest application of the
measure referred to in Article 20.

b) Where a Party, due to limitations in its legislation in force at the time of the adoption
of the present Convention, is not able to apply the measures referred to in Articles 20
and 21 to communications being transmitted within a computer system of a service
provider, which system is being operated for the benefit of a closed group of users, and
does not employ public communications networks and is not connected with another
computer system, whether public or private, that Party may reserve the right not to
apply these measures to such communications. Each Party shall consider restricting
such a reservation to enable the broadest application of the measures referred to in
Articles 20 and 21.

Section 1 – General principles
Article 23 – General principles relating to international co-operation
The Parties shall co-operate with each other, in accordance with the provisions of this
chapter, and through application of relevant international instruments on international
cooporation in criminal matters, arrangements agreed on the basis of uniform or
reciprocal legislation, and domestic laws, to the widest extent possible for the purposes
of investigations or proceedings concerning criminal offences related to computer
systems and data, or for the collection of evidence in electronic form of a criminal
offence.

Article 25 – General principles relating to mutual assistance
1. The Parties shall afford one another mutual assistance to the widest extent possible
for the purpose of investigations or proceedings concerning criminal offences related to
computer systems and data, or for the collection of evidence in electronic form of a
criminal offence.

Article 35 – 24/7 Networks
1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week
basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a) Provision of technical advice;
b) Preservation of data pursuant to Articles 29 and 30; and
c) Collection of evidence, giving of legal information, and locating of suspects.

2. a) A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b) If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:
   a) The effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
   b) The exchange of information on significant legal, policy or technological developments pertaining to cyber-crime and the collection of evidence in electronic form;

2) USA

USA has the following enactment on the computer evidence as under:-

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002⁵⁹⁰.

The Fourth Amendment states:
The right of the people to be secure in their persons, houses, papers, and effects,
against unreasonable searches and seizures, shall not be violated, and no Warrants
shall issue, but upon probable cause, supported by Oath or affirmation, and particularly
describing the place to be searched, and the persons or things to be seized. According
to the Supreme Court, a “‘seizure’ of property occurs when there is some meaningful
interference with an individual’s possessory interests in that property, “

The United States requests that pursuant to the preclusion of notice provisions of 18
U.S.C. § 2705(b), [EMAIL PROVIDER] be ordered not to notify any person (including
the subscriber or customer to which the materials relate) of the existence of this warrant
for such period as the Court deems appropriate. The United States submits that such an
order is justified because notification of the existence of this Order would seriously
jeopardize the ongoing investigation. Such a disclosure would give the subscriber an
opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee
or continue his flight from prosecution

3) INDIA

India has the following enactment on electronic and digital evidence as under:-
Admissibility of Electronic Record under Information Technology Act, 2000\textsuperscript{591}
The Information Technology Act granted a comprehensive permission for records
produced as an evidence should not to be denial to the legal effect of the document
being produced in the electronic form as long as they are available for future response.
The Act amends the definition of ‘evidence’ to include “all documents including
electronic records produced for the inspection of the court.”\textsuperscript{592}
Further, the IT Act provides that “where any law provides that information or any other
matter shall be in writing or in the typewritten or printed form, then, notwithstanding
anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-
(a) Rendered or made available in an electronic form; and

\textsuperscript{591} Information Technology Act 2000
\textsuperscript{592} Indian Evidence Act, 1872; Section 3
(b) Accessible so as to be usable for a subsequent reference.\textsuperscript{593}

It also describes the manner in which the electronic document is to be proved in law.\textsuperscript{594}

**Section 3A of Information Technology (Amendment) Act, 2008\textsuperscript{595}** provides as under:

**Electronic Signature:** (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which--

(a) Is considered reliable; and
(b) May be specified in the Second Schedule

**Section 42 of the Information Technology (Amendment) Act\textsuperscript{596}** requires every subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure

**Proof of Digital Signature:** Under section 36 Information Technology (Amendment) Act\textsuperscript{597}, a Certifying Authority while issuing a Digital Signature Certificate shall certify, *inter alia* that,-

(ca) the subscriber holds a private key which is capable of creating a digital signature;
(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber

**Under Section 67A of Indian Evidence Act, 1872\textsuperscript{598},** the Court shall presume, unless contrary is proved, that the information listed in an Electronic Signature Certificate (which includes digital signature certificate) is correct.

**Section 65B (1) of Indian Evidence Act, 1872\textsuperscript{599}** reads as under:

“Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer

\textsuperscript{593} The Information Technology Act, 2000; Section 4
\textsuperscript{594} Section 65 A and section 65 B of the Indian Evidence Act, introduced by the IT Act, 2000 amending provisions
\textsuperscript{595} Sec.3A ITAA,2008
\textsuperscript{596} Section 42 of the Information Technology (Amendment)Act
\textsuperscript{597} Section 36 Information Technology (Amendment) Act
\textsuperscript{598} Section 67A of Indian Evidence Act
\textsuperscript{599} Sec65B of Indian Evidence Act,1872
output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.”

**Sec79A-Central Government to notify Examiner of Electronic Evidence**

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence

**CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHER COUNTRIES**

The enactments and their provisions related to digital or electronic evidence in Europe, USA and India are examined.

In Europe there is an enactment for electronic evidence. As per the European Convention on Cyber-crime, 2001 criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence. Article 23 dealt with the international co-operation whereas Article 25 of the Act dealt with mutual assistance. Article 35 dealt with assistance is available on 24X7 basis. For investigations or proceedings concerning criminal offences related to computer systems and data, Article 46 dealt with the consultation of the parties for exchange of Information.

In USA, the fourth amendment to “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002” talks about the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The United States requests that

---

600 Sec.79 A of Indian Evidence Act, 1872
pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), [EMAIL PROVIDER] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate.

In India recording of evidence for satisfying the object of the Evidence Act that the evidence be recorded in the presence of the accused. Since computer generated evidence is a recent development, till date Indian law has not issued the guidelines in this regard. The UK and USA law are referred in this regard. References to the UNCITRAL Model Law on Electronic Commerce are also made. There is no major initiative in India on common repositories of electronic evidences by which in the event of any dispute (including civil) the affected computer may be handed over to a common trusted third party with proper software tools, who may keep a copy of the entire disk and return the original to the owner, so that he can keep using it at will and the copy will be produced as evidence whenever required.

Information Technology Act Section 3A of Information Technology (Amendment) Act, 2008 provides about the Electronic Signature as an evidence. Section 42 of the Information Technology (Amendment) Act provides proof of Digital Signature. Section 67A, Section 65B (1) and Sec79A of Indian Evidence Act, 1872 dealt with Electronic Signature Certificate, Electronic record to be deemed as original and by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence respectively. Hence Information Technology Act is not competent enough to delat with the problems of evidence in electronic or digital forms.

4.5.(6). COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH THE JURISDICTIONAL ISSUES.

1) INDIA

1) Personal jurisdiction:- No rule of procedure of foreign law is recognised. The Code provides general provisions regarding jurisdiction on the basis of pecuniary limit, subject matter and territory. Sections 16 to 20 of the Code regulate the issue of territorial jurisdiction for institution of suits.
2) Jurisdiction of Civil Courts in India
In India, civil court’s jurisdiction can be broadly classified in the categories 1) Pecuniary, 2) Subject Matter and 3) Territorial

3) Jurisdiction of courts and the Information Technology Act 2000
Traditional principles cover two aspects. One is the place where the defendant is residing and another where the incident occurred. However in the context of the Internet, both these are difficult to establish with certainty.

4) Legal provisions of ITA2000 & ITAA 2008 applicable in jurisdictional Issues
a) Section 13 (3), 13(4) and 13(5) of ITAA2008 :- The aforesaid sub-section (3), (4) and (5) of section 13, being deeming provisions shall apply only for the purpose of the IT Act, whereas for the application of the concept of cause of action, under our civil law, only the places from where the parties actually interact by dispatch and receipt of electronic record shall be considered in all cases.

b) Section 75 of IT Act 2000:- This section is invoked for offences or contraventions committed outside India

c) Foreign judgment applicable in India:- Indian civil Procedure Code provides that a foreign judgment is conclusive on matters directly adjudicated upon between the parties

2) European Union
The Brussels Convention has been the controlling document for jurisdictional issues.
1) A offender who is the resident of European Union country may be sued in that country.
2) In online contracts, a offender may be sued in that country where the contract has been taken place. Place of performance of the obligation may be the place where he may be sued
3) In the case of cyber torts, the miscreant may be sued where the event occurred.
4) If the contracts by not involving a consumer may opt for the dispute resolution

3) USA
There are two types of Jurisdictional issues in USA
1) General Jurisdiction :- These jurisdiction are of the personal nature and apply only when there is valid contract between the parties
2) **Specific Jurisdiction**: The jurisdiction in this case of the specific nature and it applied over the specific thing and place and the claim of jurisdiction should be reasonable.

3) **Rem-Jurisdiction** :- *In this type of jurisdiction the claim of jurisdiction is over the things and not over the persons*

4) **The Hague Convention** :- The Hague Convention on Jurisdiction and Foreign Judgments in Civil & Commercial Matters, art. 7(2), June 2001 over the Jurisdiction matter. The Hague Convention agreed upon that US courts would be required to enforce a foreign judgment against a US resident

4) **INTERNATIONAL CONVENTIONS ON JURISDICTIONAL PROBLEM.**

Following are the International Conventions on jurisdictional problem as under:-

1) European Convention on Cyber Crimes,
2) Convention on Cyber Crimes by G7 Groups
3) Convention on Cyber Crimes G8 groups etc.

In every convention jurisdictional problems have been highlighted and also respective cyber legislation of the states.

**CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHER COUNTRIES**

In India, no rule of procedure of foreign law is recognised. Sections 16 to 20 of the Code regulate the issue of territorial jurisdiction for institution of suits. Jurisdiction of Civil Courts in India classified in three categories i.e. pecuniary, subject matter and territorial. ITA2000 & ITAA 2008 applicable in jurisdictional Issues a) Section 13 (3), 13(4) and 13(5) of ITAA2008. Section 75 of IT Act 2000 is invoked for offences or contraventions committed outside India. Indian civil Procedure Code provides that a foreign judgment is conclusive on matters directly adjudicated upon between the parties.

**IN USA**, General Jurisdiction, Specific Jurisdiction, Rem-Jurisdiction are applicable while deciding the disputes of Jurisdiction
In European Union, the Brussels Convention has been the controlling document for jurisdictional issues. International Conventions on jurisdictional problem are referred while deciding the issue namely 1) European Convention on Cyber Crimes, 2) Convention on Cyber Crimes by G7 Groups and 3) Convention on Cyber Crimes G8 groups etc. Whatever stated in the foregoing paragraph IT Act is well equipped to settle the jurisdictional issues at par with the other countries.

4.5.(7).COMPARATIVE STUDY OF THE ENACTMENTS OF THE VARIOUS COUNTRIES RELATED WITH EXTRATERRITORIAL JURISDICTION AND EXTRADITION OF OFFENDERS.

The whole trouble with the jurisdiction of internet is there are so many parties involved in the crime are residing in various parts of the world who do not have real connection with each other. Cyberspace has no geographical boundaries and it establishes communications with anybody who can have access to any website. Therefore a single transaction may involve the laws of at least three jurisdictions:
1) The laws of the state/nation in which the user resides, 2) The laws of the state/nation that apply where the server hosting the transaction is located, and 3) The laws of the state/nation which apply to the person or business with whom the transaction takes place.

1) EUROPEAN UNION

Budapest Convention on Cyber-crime

Principles relating to extradition

Article 24 – Extradition

1.a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

1.b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the

---

601 conventions.coe.int/Treaty/en/Treaties/Html/185.htm
European Convention on Extradition, applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7.a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

7.b) The Secretary General of the Council of Europe shall set up and keep updated a
register of authorities so designated by the Parties. Each Party shall ensure that the
details held on the register are correct at all times.

2) AUSTRALIA
Extradition (Cybercrime) Regulation 2013\(^{602}\)
Select Legislative Instrument No. 3, 2013, Quentin Bryce, Governor General of the
Commonwealth of Australia, acting with the advice of the Federal Executive Council,
make the following regulation under the *Extradition Act 1988*. This regulation
commences on 1 March 2013. This regulation is made under the *Extradition Act 1988*.
*Section 55* of the *Extradition Act 1988* (the *Extradition Act*) provides, in part, that the
Governor-general may make regulations, not inconsistent with the *Extradition Act*,
prescribing all matters required or permitted by the *Extradition Act* to be prescribed, or
necessary or convenient to be prescribed, for carrying out or giving effect to the
*Extradition Act*.
*Subsection 11(1A)* of the *Extradition Act* provides that the regulations may provide that
the *Extradition Act* applies in relation to a specified extradition country subject to the
limitations, conditions, exceptions or qualifications as are necessary to give effect to a
multilateral extradition treaty in relation to the country. *Subsection 11(1C)* provides that
this may be achieved by applying the *Extradition Act* to the country subject to the treaty.

3) KOREA
Extradition (Republic of Korea) Order 2002\(^{603}\)
**Article 1-Obligation to extradite**
Each Party agrees to extradite to the other, in accordance with the provisions of this
Treaty, any person who is wanted for prosecution, trial, or the imposition or enforcement
of a sentence in the Requesting Party for an extraditable offence

---


**Article 2-Extraditable offences**
For the purpose of this Treaty, extraditable offences are offences which are punishable under the laws of both Parties by deprivation of liberty for a period of at least one year or by a more severe penalty.

**Article 3-Mandatory refusal of extradition**
When the Requested Party determines that the offence for which extradition is requested is an offence of a political nature.

**Article 4-Discretionary refusal of extradition**
When the offence for which extradition is sought is regarded under the law of the Requested Party as having been committed in whole or in part within its territory.

4) **India**
1) In India the Extradition Act, 1962
In India the Extradition Act, 1962 regulates the surrender of a person to another country or the request for arrest of a person in a foreign land.

2) Under the Information Technology Act, 2000
Section 75 of the Act, deals with extraterritorial application of the law,

**CRITICAL ANALYSIS OF INDIAN ENACTMENTS AS COMPARED TO OTHERS**

In **European Union**, *Principles relating to extradition* vide Article 24 – *Extradition as per* Budapest Convention on Cyber-crime

In **Australia**, extradition is governed by Section 55 *subsection11(A) under* Extradition (Cybercrime) Regulation 2013. This regulation is made under the *Extradition Act 1988*

In **Korea**, extradition is governed by Extradition (Republic of Korea) Order 2002

The **Indian Extradition Act, 1962** specifies that any conduct of a person in India or in a foreign state that is mentioned in the list of extradition offence and is punishable with minimum one year of imprisonment qualifies for extradition request. The process has to be initiated by the central government. We have extradition treaties with only 31 countries. In the case of countries with which India does not have such a treaty, the central government can by notified order treat any convention to which India and the foreign country is a party as the extradition treaty providing for extradition with respect to the offences specified in that convention. If the extradition request has come from two
or more countries then the government has the rights to decide which of them is the fittest for the request. Since 2002 India has extradited 42 fugitive criminals who were handed over by the foreign countries to India.

**Under the Information Technology Act, 2000,** Section 75 of the Act, deals with extraterritorial application of the law, the section states that the provisions of the Act will apply to Any person irrespective of nationality and an offence or contravention committed outside India Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies. Moreover, it is important to note that India at present does not have a proper extradition law to deal with crimes that have been committed over the Internet. To address this issue, India should become a signatory to the Convention of cyber crimes treaty and should ratify it. Recently India has signed cyber crimes related treaties with 19 countries to attain legal compatibility.

Whatever stated in the foregoing paragraphs it will be fair enough to say that the measures taken by the Government of India are not sufficient to curb and control cases of extraterritorial jurisdiction. Though the Government has provided the statute to deal beyond the territorial boundaries but it has not given any framework for its execution. Unless there is no international co-operation and legal harmony between the countries there is no use of drafting such legal provision to control the cyber crime are not effective.