CHAPTER 5
INTERNATIONAL LEGAL RESPONSE TO
CYBER TERRORISM

5.1 Introduction

It is the normal tendencies of the human beings to opt/adapt and move towards the destructive side of most innovations and advancements. The most objectives with which the science is working and inventing the various technology is to ease the human lives and provide the opportunities to enrich their lives by using simple, quick and high-quality devices. Current technological developments also are dedicated to the human being serving the same object. But it is evident that human being, anyhow, searched the techniques to use the technologies gifted to them by the science, in destructive ways. Current technological developments presented to us also hold the potential to be used by the terrorists as weapons to destroy the beautiful life of the human being provided by the nature and decorated by the technology itself. Its means that it is not the technological development but the mode of its uses makes it boon or bane for the human being and the world as well¹.

However, since the development in the field of technology is being new, there was lack of the reference as to how the international community can react to destructive use of the technological development. Hence, it is the right time to think and adopt the preventive measure against such use of the technological developments and regulate the terrorist activities regarding the misuse of the same. The instant

research is an attempt to take that next step, and try to analyze whether the available international tool kit is sufficient enough to handle above said problem known to us as ‘cyberterrorism’\(^2\).

The researcher, under the present chapter, have made his effort to analyze the relevancy of the available international legal measure to fight with, and to regulate the cyber terrorism and hence has focused on the legal aspects, rather than discussing the technological options to combat with the same. In the course of which the analysis of existing counter-terror conventions by way of legal interpretation and finding of a better direct way of addressing this threat, via the creation of an explicit regime for the suppression of cyber terrorism consisting of conventional prohibitions, Security Council resolutions and international criminal laws would be the objective of the researcher.

5.2 Cyber Terrorism: A Reality

Cyber terrorism has immerged as a new terror to the world. In the past ten years Information Security Systems received more sophisticated growth, but the same happened with the hackers too. Terrorist groups have been using the Internet for various purposes, such as communicating, propagandizing, recruiting and collecting intelligence\(^3\). The network of computer-mediated communication is ideal for terrorists as communicators: it is decentralized, it is more difficult to subject it to control or restriction and it allows access to anyone who wishes to use it\(^4\). It is so that the cyber-world can be used in a various ways, for example, not only as an indirect tool for executing an attack, but also as a direct weapon.

---

\(^2\) Ibid.


\(^4\) Ibid.
The cyber attacks on websites are one of the ways to use the weapon of cyberspace. For instance, the India-Pakistan dispute over Kashmir, the Israeli-Palestinian conflict and the NATO websites during the crises in Kosovo in the early 90th decade of the 20th century are the instances where such attacks had taken place. Janet J. Prichard & Laurie E. MacDonald in their book has explained these instances. These attacks still do not constitute ‘terrorism’ in the sense that they do not cause physical harm and do not intend to influence the government, as required by the definition of terrorism in the Financing Convention.

The other way the cyberspace is being used as a weapon is the case of cyber terrorism. According to Shlomo Harnoy the cyber terrorism is the use of computer networks in order to harm human life or to sabotage critical national infrastructure in a way that may cause harm to human life. Trachtman has attempted to distinguish among the different types of networks that may be subjected to cyber terrorist attacks, military and civilian defense networks, other governmental networks (Police, Fire), privately or publicly owned networks used to control public utilities and other systems for providing infrastructural services (i.e. Electricity, Water), and public networks used by individual consumers and businesses for communication, education etc.

---

6 This is according to Shlomo Harnoy, Founder, senior VP & Professional manager at SDEMA Group, and Yossi or, VP Information Security at SDEMA Group. The SDEMA Group is an integrated, homeland security solutions partnership specializing in risk mitigation. SDEMA also offers information security service including market forward protection against cyber terrorism. This definition is also accepted in academic literature, see Weimann, Supra Note 3, p. 148; Dorothy E. Denning, “Cyberterrorism”: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000, Available on http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html., Retrieved on 23 June 2013.
Cyber terrorism may be used for disrupting bank data, penetrating Rail Company’s computers, blocking computer communication at an international airport, deleting the voter register 24 hours before an election, and many more. All the above said systems, being service providers, are linked with the Internet in one way or another and therefore are under the risk of invasion. In the present scenario, the Western Societies are dependent in almost every aspect of life upon computer communication. Computer systems control nearly everything required for our daily routines and our emergency plans.

Now the question is whether the cyber terrorism is similar in its characteristics to other forms of terrorism mentioned earlier? Definitely, there are some difference between hijacking an aero-plane on the point of a gun and hijacking it by taking control over the computer system of the aero-plane. In the above demonstrated facts it is crucial to establishing the legal nature of cyber terrorism in combating with it through international legal instruments, which are central to the international community’s fight against terrorism.

As stated above, the elements of physical harm and intention to cause a sense of fear and to influence the decision making process is being exhibited by the terrorism. The cause of physical harm can be attained through disruption of computer systems, such as disabling Traffic light systems, Hospital’s computers, Electric Companies’ computer etc. These acts bring about a sense of fear and uncertainty among the victim population. Hence, the terrorist has not to go through the trouble of getting a gun or a knife onboard an aircraft in order to become a cyberterrorist. They can get the same results sitting in front of a computer screen. The government, ‘do something’ to put control of such activity, being under obligation to the safety and security of the people.
Of course not every Ehud Tenenbaum\textsuperscript{8} is a terrorist just because he intended to break into classified computer networks. As the cyber terrorism requires, the intention element (see Chapter 3) also means there was intention to influence a government’s course of action. Cyber terrorism has several unique characteristics distinguishing it from other kinds of terrorism\textsuperscript{9}. Terrorism is defined as being aimed

\footnotesize\textsuperscript{8}Tenenbaum was born in Ramat HaSharon in 1979. Tenenbaum became widely famous in 1998, when aged 19 years and while he was the head of a small group of hackers, he was arrested for hacking computers belonging to NASA, The Pentagon, the U.S. Air Force, the U.S. Navy, the Knesset, MIT and other American and Israeli universities, the Lawrence Livermore National Laboratory and other federally funded research sites, and the computer of Israeli President Ezer Weizman, as well as attempting to infiltrate the Israel Defense Forces’ classified files. He also hacked into the computers of Palestinian terrorist groups, and claimed to have destroyed the website of Hamas. Tenenbaum installed on some of the servers Packet analyzer software and Trojan horse software. At the time then-US Deputy Defense Secretary John Hamre insisted was “the most organized and systematic attack to date” on US military systems. The military thought that they were witnessing a sophisticated Iraqi ‘information warfare’. In an effort to stop the supposed Iraqi hackers the United States government assembled agents from the FBI, the Air Force Office of Special Investigations, NASA, the US Department of Justice, the Defense Information Systems Agency, the NSA, and the CIA. The government was so worried that the warning and briefings went all the way up to the President of the United States. The investigation, code-named “Solar Sunrise,” eventually snared two California teenagers (screen names Mac and Stimpy) and Tenenbaum, but no Iraqi infowarriors. After their arrest, a subsequent probe led US investigators to Tenenbaum, who was arrested after Israeli police were given evidence of Tenenbaum’s activities. Later, the FBI sent agents to Israel to question Tenenbaum. Before he was sentenced, Tenenbaum served briefly in the Israel Defense Forces, but was released soon thereafter after he was involved in a traffic collision. In 2001, Tenenbaum pleaded guilty, while stating that he wasn’t attempting to infiltrate the computer systems to get a hold of secrets but rather to prove that the systems were flawed. Tenenbaum was sentenced to a year and a half in prison, from which he served only 8 months following the “Deri Law”. After the attack the FBI made a short 18 minutes training video called, Solar Sunrise: Dawn of a New Threat that was sold as part of hacker defense course that was discontinued in September 2004. In 2003, after being freed from prison, Tenenbaum founded his own Information security company called “2XS”. In September 2008, following an investigation by Canadian police and the US Secret Service, Tenenbaum and three accomplices were arrested in Montreal. Tenenbaum was charged with six counts of Credit card fraud, in the sum of approx. US$1.5 million. U.S. investigators suspected Tenenbaum of being part of a scam, in which the hackers penetrated financial institutions around the world to steal credit card numbers. They then sold these numbers to other people, who used them to perpetrate massive credit card fraud. He was later extradited to the United States to stand trial, and was in the custody of the US Marshals for more than a year. In August 2010, he was released on bond after agreeing to plead guilty. In July 2012, after Tenenbaum accepted a plea bargain which may have involved cooperation in the investigation, New York district judge Edward Korman sentenced Tenenbaum to the time already served in prison. Tenenbaum was also ordered to pay $503,000 and given three years’ probation. Recently on November 13 he caught in the case of money laundering.

at a certain target that has great potential damage in terms of human life. The identity of the humans itself does not matter. Cyber terrorism, on the other hand, can hurt a very specific group of people - the population of modern western countries.

As stated above, cyber terrorism hurts computerized infrastructure, on which advanced and advancing societies have come to depend. Thus, different societies are vulnerable to cyber terrorism in different degrees in accordance with their level of dependence on technology and computer networks. The more dependent a state is on electronic communications and information processing networks, the more vulnerable to cyber terrorism it will be\(^\text{10}\). As Richard Clarke put it already in 1999 - “If you are connected you are vulnerable.”\(^\text{11}\)

One might be said that the level of technology advancement also results in better defense systems, which enable states to protect themselves from these kinds of attacks. It is the fact that the India is more exposed to cyber terrorism than Bhutan and hence while assessing the volume of the risk, it remains clear that the cyber terrorists are trying to attack India to become more sophisticated themselves. India, being more at stake and being more dependent on its information security to hold on against a cyber terrorism attack because of having more dependent on its own computerized infrastructure, still, these cat and mouse games between the cyberterrorists and the information security experts are most likely to occur in the India and not in Bhutan.

Unlike a terrorist attack in the physical world which requires recruiting an executor, equipping him with weapons or explosives and making sure he will pass all security checks on his way to the designated location, the a cyber terrorist needs is a good computer and hacking skills that exceed his opponent’s for committing a cyber

\(^{10}\) Weimann, Supra Note 3, p. 148; Trachtman, Supra Note 7, p. 5.

attack. Thus, the cyber terrorism on the other hand, will most likely save these costs and obstacles. Hence, another distinctive feature of cyber terrorism is, its relatively being low costs. In today’s world, being with the potential to acquire the required technical skills and a crash-course “Hacking 101” is not difficult but is so easy and can be easily be found on the Internet\(^\text{12}\) itself.

It is the fact that in spite of all the gloomy predictions of a cyber terrorism doomsday, no single instance of real cyber terrorism has yet been recorded. This fact leads people to think that the prophecies on cyber terrorism are exaggerated\(^\text{13}\). In this regard, several arguments are available which are needed to be considered. Theoretically speaking, non happening of any event does not mean that there is no scope and/or possibility of the happening same in the future. The very perfect and relevant example may the ‘nuclear war’ which even though, fortunately, has not been occurred; the superpowers in the international system have been preparing themselves for the same. In addition, like physical terror cells that hold ‘sleeping agents’ at their enemy’s territory ready to be active on a phone call, so the computer viruses can be programmed to be active as of a certain date in the future, until that time no one will know of their existence.

Shlomo Harnoy and Yossi, both being experts and well known names in the field of counterterrorism, have pointed out that a possible reason as to why there have been no cyber attacks could simply be that terrorist organizations have not yet acquired the technological ability, which is the core factor in cyber terrorism\(^\text{14}\). Assuming that the reason there has, of yet, been no cyber terrorism event is indeed the technological gap between the potential targets and potential terrorist, this calls for immediate action. Technological gaps can be closed, rapidly. Since the most


\(^{13}\) Weimann, Supra Note 3, p. 149.

\(^{14}\) Brenner & Goodman, Supra Note 9, pp. 44-52.
critical infrastructures in Western societies are networked through computers, the potential threat of cyber terrorism is, at least in theory, alarming.\footnote{Weimann, Supra Note 3, p. 148; See Brenner & Goodman, ibid.}

The threat of the cyber terrorism is being taken very seriously for at least a decade by the Governments in Western countries. For instance, the U.S. authorities conducted the first experiment of its kind, designed to check the level of readiness of U.S. computer systems for the next attack. This operation was held in 2002 and was given the symbolic name ‘Digital Pearl Harbor’. The results were startling. The ‘Red Team’ which was supposed to try to hack into computer systems and disrupt their functioning, succeeded in nearly all cases.\footnote{Eric Purchase & Franch Caldwell, “Digital Pearl Harbor: A Case Study in Industry Vulnerability to cyber Attacks”, in: Sumit Ghosh, Manu Malek & Edward A. Stohr (eds.), Guarding Your Business - A Management Approach To Security, Springer, New York, 2004. Red Teams in the United States military were used much more frequently after a 2003 Defense Science Review Board recommended them to help prevent the shortcomings that led up to 9/11.} After this experiment the U.S. government began a campaign of improving readiness for cyber terrorism, both on the technical and legislative level.\footnote{Tara Mythri Raghavan, “Cyberterrorism: An Analysis of the Congressional Response”, J.L. TECH. & POL’Y, 297-312, 2003.}

To adjust their information security systems to a scenario of cyber terrorism, the Israel, vide Government Decision B-84 from 2002 defined critical data systems that will undergo a security upgrade. In Europe, governments have acted not only on a singular basis, such as the establishing of the National Technical Assistance Center in the United Kingdom,\footnote{Clive Walker, “Cyberterrorism: Legal Principle and Law in the United Kingdom”, 110(3) PENN ST. L. REV. 625-665, 2006.} but also in the framework of the European Union. To strengthening the computer security systems, in order to enhance the preparedness for terrorist attacks involving critical infrastructure, in 2005, the European Council adopted the European Program for Critical Infrastructure Protection (EPCIP) as part of its overall fight against terrorism.
Currently there is no single effective international legal instrument which deals specifically with cyber terrorism. Since the threat seems not to be farfetched, it is prudent thinking to try and see what the legal international community has in store for the ‘Day After’. Thus, in the instant chapter and in next\textsuperscript{19} the international response and their efforts and status as well towards the development of the sufficient legal instruments and policies to fight against the, and to face in the event of cyber terrorism, has been taken into consideration by the researcher.

5.3 Status of the Countries on Cyber Law

The journey of legal analysis of the international response to cyber terrorism begins with the examination of the legal framework presently in existence in the form of the conventions, treaties, enactments of respective States etc.. In order to determine the applicability of any of those conventions to cyber terrorism, the foremost step is to ensure that the offenses defined in the convention concerned would not be limited to the execution by physical means. As explained earlier, the current conventions were originally designed to respond to specific manifestations of terrorism, and hence they create specific offenses to suit each scenario, such as aircraft hijackings or hostage situations. Since most of these conventions were drafted when cyber terrorism was considered to be, at most, science fiction, it is not at all certain that they apply to a cyber attack\textsuperscript{20}.

\textsuperscript{19} Chapter 5 and 6 of this Research.

\textsuperscript{20} This can be said with respect to any new method of terrorism that may evolve, for further reading on the criticism of the counter-terrorism conventions and their failure to address new methods of terrorism. See Jennifer Trahan, “Terrorism Conventions: Existing Gaps and Different Approaches”, \textit{8 NEW ENG. INT’L & COMP. L. ANN.} 215, 221-222, 2002.
Table 5.1: The Data of Nineteen Countries with Updated Laws

<table>
<thead>
<tr>
<th>Country</th>
<th>Data Crime</th>
<th>Network Crimes</th>
<th>Access Crimes</th>
<th>Related Crimes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interception</td>
<td>Modification</td>
<td>Theft</td>
<td>Interference</td>
</tr>
<tr>
<td>Australia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Brazil</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Canada</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Chile</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>China</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Denmark</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Estonia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>India</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Japan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Malaysia</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Mauritius</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Peru</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Philippines</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Poland</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Turkey</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>United States</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Statutory provisions of 19 countries, mentioned in above table-1, have been gone through, analyzed including Brazil, Chile, Germany, and other countries. The important and relevant provisions are collected and discussed here below:
5.3.1 Canada


The Section 430 states as:

“1. Every one commits mischief who willfully-

(a) destroys or damages property;
(b) renders property dangerous, useless, inoperative or ineffective;
(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

(1.1) Every one commits mischief who willfully

(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

2. Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.

3. Every one who commits mischief in relation to property that is a
testamentary instrument or the value of which exceeds five thousand dollars.

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.

4. Every one who commits mischief in relation to property, other than property described in sub-section. (3),

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
(b) is guilty of an offence punishable on summary conviction.

5. Every one who commits mischief in relation to data

a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
b) is guilty of an offence punishable on summary conviction.

(5.1) Every one who willfully does an act or willfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
b) is guilty of an offence punishable on summary conviction.

6. No person commits mischief within the meaning of this section by reason only that:
a) he stops work as a result of the failure of his employer and himself to agree on any matter relating to his employment;  
b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree on any matter relating to his employment; or  
c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.

7. No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling house or place for the purpose only of obtaining or communicating information.”

The Data Interception Unauthorized Access, Additional Virus Dissemination

Part IX: Offences Against Rights of Property Possession of device to obtain computer service:

The Sec. 342.2 (1) states as:

“Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section.
a) is guilty of an indictable offence and liable to imprisonment for term not exceeding two years; or

b) is guilty of an offence punishable on summary conviction.”

**Data Theft; Part IX: Offences Against Rights of Property:**

Sec. 322 (1) of the Act runs as:

“(1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent

(a) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it of the thing or of his property or interest in it;

(b) to pledge it or deposit it as security;

(c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or

(d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

(2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved, or begins to cause it to become movable.

(3) Taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.
(4) For the purposes of this Act, the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.

**Computer Related-Fraud; Part X: Fraudulent Transactions Relating to Contracts and Trade**

Section 380 of the Act states:

“(1) Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding ten years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or

b) is guilty

a. of an indictable offence and is liable to imprisonment for a term not exceeding two years, or

b. of an offence punishable on summary conviction, where the value of the subject-matter of the offence does not

(2) Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, with intent to defraud, affects the public market price of stocks,
shares, merchandise or anything that is offered for sale to the public is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.”

Section 381 is about the punishment for the crime committed under Sec. 380:

“Everyone who makes use of the mails for the purpose of transmitting or delivering letters or circulars concerning schemes devised or intended to deceive or defraud the public, or for the purpose of obtaining money under false pretences, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.”

5.3.2 Czech Republic

Czech-Criminal Code, 1961; Secs. 182 and 257a

Sec. 182 Damaging and Endangering the Operation of a Public Utility

(1) Whoever intentionally endangers the operation of-

(a) public telecommunications facility, a post office or a public transport facility;
(b) facility preventing the leaking of contaminating substances;
(c) a power or water-supply facility;
(d) public facility for the prevention of fire, flood or other natural disasters;
(e) a submarine cable or pipeline;
(f) a defensive or protective facility against air and other similar
attacks or their consequences; or

(g) any other similar public facility

shall be punished by imprisonment for a term of up to three years or a pecuniary penalty.

(2) An offender shall be sentenced to imprisonment for a term of from one to six years if:

(a) he causes a breakdown in the operation of a public utility by an act under sub-provision (1); or

(b) he commits such act during a state defence emergency.

Sec. 257a Damaging or Misusing Data Carrier Record

(1) A person who, with intent to cause damage or some other detriment to another or obtain unjust benefit for himself or another person, gains access to a data carrier and:

(a) uses such data without authorization;
(b) destroys, damages or renders useless the data on such carrier; or
(c) interferes with the hardware or software of a particular computer,

shall be punished by a term of imprisonment of up to one year, by prohibition of a (specific) activity, by a pecuniary penalty or forfeiture of a (specific) thing.

(2) An offender shall be sentenced to a term of imprisonment of from
six months to three years if:

(a) he commits an act under sub-provision (1) as a member of an organized group, or
(b) by such act he causes substantial damage or acquires substantial benefit for himself or another person.

(3) An offender shall be sentenced to a term of imprisonment of from one to five years if, by an act under sub-provision (1), he causes large-scale damage or acquires a large-scale benefit for himself or another person.

5.3.3 Denmark

The Danish Criminal Code, 1930 contains the following provisions that are applicable in relation to computer crime:

**Computer Fraud**

**Sec. 279 a** - Any person who, for the purpose of obtaining for himself or for others an unlawful gain, unlawfully changes, adds or erases information or programs for the use of electronic data processing, or who in any other manner attempts to affect the results of such data processing, shall be guilty of computer fraud.

**Sec. 285(1)** - The offences referred to in [i.a. Section 279 a] of this Act shall be punished with imprisonment for any term not exceeding one year and six months,

**Sec. 286(2)** - The penalty for computer fraud may, where the offence is of a particularly aggravated nature or where a large number of such offences
have been committed, be increased to imprisonment for any term not exceeding eight years.

Sec. 287 (1) - If any of the offences dealt with in [i.a. Sections 279 a] of this Act is of minor importance because of the circumstances under which the punishable act was committed, because of the small value of the objects appropriated or of the loss of property sustained or for any other reason, the penalty shall be a fine. In further mitigating circumstances, the penalty may be remitted.

5.3.4 Estonia

Estonian Criminal Codes, 2001 - Chapter 13-Offences against Property, Division-1, Sub-Division-2

Sec. 206. Interference in Computer Data

(1) Illegal alteration, deletion, damaging or blocking of data or programmes within computer systems, or illegal uploading of data or programmes into computer systems is punishable by a pecuniary punishment or up to 3 years’ imprisonment.

(2) The same act, if committed against a computer system of a vital sector or if significant damage has been caused thereby is punishable by a pecuniary punishment or up to 5 years’ imprisonment.

(3) An act provided for in sub-section (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

---

[RT I 2008, 13, 87 - entry into force 24.03.2008]
Sec. 207. Hindering of Operation of Computer System

(1) Illegal interference with or hindering of the operation of a computer system by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to 3 years imprisonment.

(2) The same act, if significant damage is caused thereby or the operation of a computer system of a vital sector or the provision of public services is hindered thereby is punishable by a pecuniary punishment or up to 5 years imprisonment.

(3) An act provided for in sub-section (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

Sec. 208. Dissemination of spyware, malware or computer viruses

(1) Dissemination of spyware, malware or computer viruses is punishable by a pecuniary punishment or up to 3 years imprisonment.

(2) The same act, if committed:

1) at least twice; or

2) causing significant damage is punishable by a pecuniary punishment or up to 5 years imprisonment.

(3) An act provided for in sub-section (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

---

22 Ibid.
(4) A court may, pursuant to the provisions of Sec. 83 of this Code, apply confiscation of an object which was the direct object of the commission of an offence provided for in this section.

Chapter 15 - Offences against the State, Division-3 - Offences against State Power;

Sec. 237. Acts of Terrorism\textsuperscript{23}

(1) Commission of a criminal offence against international security, against the person or against the environment, against foreign states or international organizations or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent or interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose to force the state or an international organization to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organization, or to seriously terrorize the population is punishable by 5 to 20 years’ imprisonment or life imprisonment.\textsuperscript{24}

(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.

\textsuperscript{23} RTI 2007, 16, 77 entry into force 01.01.2008.
\textsuperscript{24} RTI 2009, 19, 114 - entry into force 06.04.2009.
(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Sec. 832 of this Code.\textsuperscript{25}

Sec. 237(1). \textbf{Terrorist Organization}\textsuperscript{26}

(1) Membership in a permanent organisation consisting of three or more persons who share a distribution of tasks and whose activities are directed at the commission of a criminal offence provided in Sec. 237 of this Code as well as forming, directing or recruiting members to such organisation is punishable by 5 to 15 years’ imprisonment or life imprisonment.

(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.

Sec. 237(2). \textbf{Preparation of and incitement to acts of terrorism}\textsuperscript{27}

(1) Organization of training or recruiting persons for the commission of a criminal offence provided in Sec. 237 of this Code, or preparation for such criminal offence in another manner as well as public incitement for the commission of such criminal offence is punishable by 2 to 10 years’ imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution.

\textsuperscript{25} RTI 2007, 2, 7 - entry into force 01.02.2007.
\textsuperscript{26} RTI 2007, 13, 69 - entry into force 15.03.2007.
\textsuperscript{27} Ibid.
Sec. 237(3). Financing and support of act of terrorism and activities directed at it

(1) A person who finances or knowingly supports in another way the commissioning of a criminal offence provided for in Ss. 237, 2371 or 2372 of this Code, as well as a terrorist organisation or a person whose activities are directed at the commission of a criminal offence provided in Sec. 237 of this Code, and makes available or accumulates funds knowing that these may be used in full or in part to commit a criminal offence provided for in Ss. 237, 2371 or 2372 of this Code, shall be punished by 2 to 10 years’ imprisonment.

(2) The same act, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution.

(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of Sec. 832 of this Code.

5.3.5 Japan

Japan Computer Crime Act; Japan Penal Code, 1907 - Chapter XVII Crimes of Counterfeiting of Documents

Article 161-2 Unauthorized Creation of Electromagnetic Records

(1) A person who, with the intent to bring about improper
administration of the matters of another person, unlawfully creates without due authorization an electromagnetic record which is for use in such improper administration and is related to rights, duties or certification of facts, shall be punished by imprisonment with work for not more than 5 years or a fine of not more than 500,000 yen.

(2) When the crime prescribed under the preceding paragraph is committed in relation to an electromagnetic record to be created by a public office or a public officer, the offender shall be punished by imprisonment with work for not more than 10 years or a fine of not more than 1,000,000 yen shall be imposed.

(3) A person who, with the intent prescribed for in paragraph (1), puts an electromagnetic record created without due authorization and related to rights, duties or certification of facts into use for the administration of the matters of another shall be punished by the same penalty as the person who created such an electromagnetic record.

(4) An attempt of the crime prescribed under the preceding paragraph shall be punished.

Chapter XXXV - Crimes against Credit and Business

Article 233 Damage to Credit; Obstruction of Business

A person who damages the credit or obstructs the business of another by spreading false rumors or by the use of fraudulent means shall be punished by imprisonment with work for not more than 3 years or a fine of not more than 500,000 yen.
Article 234 Forcible Obstruction of Business

A person who obstructs the business of another by force shall be dealt with in the same manner as prescribed under the preceding Article.

Article 234-2 Obstruction of Business by Damaging a Computer

A person who obstructs the business of another by interfering with the operation of a computer utilized for the business of the other or by causing such computer to operate counter to the purpose of such utilization by damaging such computer or any electromagnetic record used by such computer, by inputting false data or giving unauthorized commands or by any other means, shall be punished by imprisonment with work for not more than 5 years or a fine of not more than 1,000,000 yen.

5.3.6 Malaysia

Computer Crimes Act, 1997 - Unauthorized Access to Computer Material - Unauthorized Access with intent to commit or facilitate commission of further offence

Section 4 states as

“A person shall be guilty of an offence under this section if he commits an offence referred to in section 3 with intent-

(1) (a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or

(b) To facilitate the commission of such an offence whether by
himself or by any other person.

(2) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorized access is secured or on any future occasion.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Unauthorized modification of the contents of any computer

Section 5 of the Act runs as

“(1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

(2) For the purposes of this section, it is immaterial that the act in question is not directed at-

(a) any particular program or data;
(b) a program or data-of any kind; or
(c) a program or data held in any particular computer.

(3) For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary.

(4) A person guilty of an offence under this section shall on conviction
be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

Wrongful Communication

Section 6 provides

“(1) A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate,

(2) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

5.3.7 Phillipines

Electronic Commerce Act, 2000 (Republic Act No. 8792)

Section 30 - Extent of Liability of a Service Provider

Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of the electronic data message or electronic document for which the person or party acting as a service provider as defined in Section 5 merely provides
access if such liability is founded on -

(a) The obligations and liabilities of the parties under the electronic data message or electronic document;

(b) The making, publication, dissemination or distribution of such material or any statement made in such material, including possible infringement of any right subsisting in or in relation to such material: Provided, That

(i) The service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material;

(ii) The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and

(iii) The service provider does not directly commit any infringement or other unlawful act and does not induce or cause another person or party to commit any infringement or other unlawful act and/or does not benefit financially from the infringing activity or unlawful act of another person or party: Provided further, That nothing in this Section shall affect -

a) Any obligation founded on contract;

b) The obligation of a service provider as such under a licensing or other regulatory regime established under written law: or

c) Any obligation imposed under any written law;
d) The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any material, or to preserve evidence of a violation of law.

Sec. 33 Penalties

The following Acts shall be penalized by fine and/or imprisonment, as follows:

a) Hacking or cracking
b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

c) Violations of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those
laws;

d) Other violations of the provisions of this Act shall be penalized with a maximum penalty of one million pesos (P 1000,000.00) or six (6) years imprisonment.

5.3.8  Spain

Spanish Penal Code, 1884;

TITLE X, Felonies against privacy, the right to personal dignity and the inviolability of the dwelling,

Chapter I - On Discovery and Revelation of Secrets

Article 197 of the Act provides that

1. Whoever, in order to discover the secrets or to breach the privacy of another, without his consent, seizes his papers, letters, electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal, shall be punished with imprisonment of one to four years and a fine of twelve to twenty-four months.

2. The same penalties shall be imposed upon whoever, without being authorized, seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telemetric files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without
being authorized, accesses these by any means, and whoever alters or uses them to the detriment of the data subject or a third party.

3. Whoever, by any means or procedure and in breach of the security measures established to prevent it, obtains unauthorised access to computer data or programs within a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years.

When, pursuant to the terms established in Article 31 bis, a legal person is responsible for the offences included in this Article, the punishment of a fine from six months to two years shall be imposed thereon. Pursuant to the rules established in Article 66 bis, the Judges and Courts of Law may also impose the penalties established in sub-Sections b) to g) of Section 7 of Article 33.

4. A sentence of imprisonment shall be imposed from two to five years if the data or facts discovered, or the images captured to which the preceding numbers refer, are broadcast, disclosed or ceded to third parties. Whoever, being aware of their unlawful origin and without having taken part in their discovery, perpetrates the conduct described in the preceding Section shall be punished with imprisonment from one to three years and a fine of twelve to twenty-four months.

5. Should the acts described in Sections 1 and 2 of this Article be perpetrated by persons in charge of or responsible for the files, computer, electronic or telemetric media, archives or records, a
sentence of imprisonment of three to five years shall be imposed on them, and if they disclose, communicate or reveal reserved data, the upper half shall be imposed.

6. Likewise, when the acts described in the preceding Sections concern personal data that reveal the ideology, religion, belief, health, racial origin or sexual preference, or when the victim is a minor or incapacitated, the penalties imposed shall be those foreseen in the upper half.

7. If the acts are perpetrated for profit-making purposes, the penalties shall be imposed as foreseen in Sections 1 to 4 respectively of this Article in the upper half. If they also affect the data mentioned in the preceding Section, the punishment to be imposed shall be that of imprisonment from four to seven years.

8. Should the acts described in the preceding Sections be committed within a criminal organization or group, the higher degree penalties shall be applied respectively.

Chapter IX- On Damages: Article 264

1. Whoever, by any means, without authorization and in a serious way, were to erase, damage, deteriorate, alter, suppress, or make data, computer programs or electronic documents pertaining to others inaccessible, when the result produced is serious, shall be punished with a sentence of imprisonment of six months to two years.
2. Whoever, by any means, without being authorised and in a serious way, were to hinder or interrupt operation of a computer system pertaining to another, introducing, transmitting, damaging, erasing, deteriorating, altering, suppressing or making computer data inaccessible, when the result produced is serious, shall be punished, with a sentence of imprisonment of six months to three years.

3. The penalties imposed shall be higher by one degree to those respectively stated in the previous two Sections and, in all cases, the punishment of a fine ranging from one to ten times the amount of damage caused, when any of the following circumstances concur in the conduct described:

1. When committed within the setting of a criminal organisation;

2. When special damage has been caused or general interest has been affected;

4. When, pursuant to the terms established in Article 31 bis, a legal person is responsible for the offences included in this Article, it shall have the following penalties imposed thereon:

   a) Fine of two to four times the damage caused, if the offence committed by a natural person has a punishment of imprisonment foreseen exceeding two years;

   b) Fine of two to three times the damage caused, in the rest of the cases.

Pursuant to the rules established in Article 66 bis, the Judges and
Courts of Law may also impose the penalties established in Sub-Sections b) to g) of Section 7 of Art. 33.

**Article 270 provides the Punishment**

Punishment consisting of imprisonment from between six months and two years or a fine of between six and twenty-four months [sic] will be imposed on an individual who, with intent to profit and to the detriment of third party, reproduces, plagiarizes, distributes or publicly communicates either wholly or in part, a literary, artistic or scientific work or the transformation, interpretation or artistic execution thereof contained in any medium or communicated by any means, without the authorization of the holders of the corresponding intellectual property rights or successors thereof.

The same punishment will be imposed on any individual who intentionally imports, exports or stores copies of such works or productions or executions without the authorization-specified above.

The same punishment will be imposed in the event of the manufacture, circulation and possession of any medium specifically designed to facilitate the unauthorized suppression and neutralization of any technical device used to protect computer programs.
5.3.9 Turkey

PART II: Felonies on Information Technology

Article 525/a - (Annexed by Code 3756 Art. 21, 06.06.1991)

Whoever obtains programs or data or another component from an automatic data processing system illegally, shall be punished by imprisonment for one year to three years and a heavy fine of 1,000,000 to 15,000,000 liras. Whoever uses, transfers or copies programs, data or another component in an automatic data processing system, with the purpose of harming anybody, shall suffer the punishment in the above mentioned paragraph.

Article 525/b - (Annexed by Code 3758 Art. 22, OS.06, 1991)

Whoever destroys or changes or deletes or prevents from operating or ensures incorrectly operating an automatic data processing system or data or another component, completely or partially, for the purpose of harming anyone or deriving a benefit for himself or anybody else, shall be punished by imprisonment for two years to six years and a heavy fine of 5,000,000 to 50,000,000 liras.

Whoever derives a legal benefit for himself or anybody else, using an automatic data processing system, shall be punished by imprisonment for one year to five years and a heavy fine of 2,000,000 to 20,000,000 liras.

Article 525/c - (Annexed by Code 3756 Art. 23, 06.06.1991)

Whoever puts data or other components into an automatic data
processing system or alters existing data or other components, in order to generate a counterfeit document for the purpose of using as evidence in jurisprudence, shall be punished by imprisonment for one year to three years. Whoever uses knowingly the abovementioned-altered one shall be punished by imprisonment for six months year to two years.

**Article 525/d** - (Annexed by Code 3756 Art. 24, 06.06.1991)

Whoever violates the Article 525/a and 525/b by virtue of performing or while performing his profession, shall also be disqualified from holding the public office subject to offense or performing his profession or trade subject to offense for six months to three years, in addition to punishment prescribed in the Articles mentioned.

### 5.3.10 United Kingdom

**Computer Misuse Act 1990**

**Section 1- Unauthorized Access to Computer Material.**

“(1) A person is guilty of an offence if-

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; 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 offence under this section need not 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 offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Section 2 - Unauthorised access with intent to commit or facilitate commission of further offences.

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

(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences-

(a) for which the sentence is fixed by law; or

(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions 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).

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

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

(5) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;
(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Telecommunications Act, 1984

Section 43 - Improper use of public telecommunication system

(1) A person who-

(a) sends, by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

(b) sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system,

shall be guilty of an offence and liable on summary conviction to imprisonment for a term not exceeding six months or a fine not exceeding level 5 on the standard scale or both.

Sub-section (1) above does not apply to anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990).
5.3.11 United States of America

Computer Fraud and Abuse Act of 1986 (CFAA),

USC, Title 18, Crimes, Part I - Crimes,

Chapter 47 - Fraud and False Statement

Sec. 1029 Fraud and related activity in connection with access devices

“(a) Whoever-

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

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

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

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

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;
(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of-

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

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

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

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

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as
provided in sub-section (c) of this section.

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

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

(c) Penalties.-

(1) The punishment for an offense under sub-section (a) of this section is-

(A) in the case of an offense that does not occur after a conviction for another offense under this section-

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

(ii) if the offense is under paragraph (4), (5), (8), or (9) of sub-section (a), a fine under this title or imprisonment for not more than 15 years, or both;
(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure - The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for sub-section (d) of that section.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section-

(1) the term ‘access device’ means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);
(2) the term ‘counterfeit access device’ means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term ‘unauthorized access device’ means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) the term ‘produce’ includes design, alter, authenticate, duplicate, or assemble;

(5) the term ‘traffic’ means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6) the term “device-making equipment” means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;

(7) the term ‘credit card system member’ means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

(8) the term ‘scanning receiver’ means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument;

(9) the term ‘telecommunications service’ has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47
(10) the term ‘facilities-based carrier’ means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and

(11) the term ‘telecommunication identifying information’ means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.

(f) 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, or any activity authorized under chapter 224 of this title. For purposes of this sub-section, the term ‘State’ includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(g) (1) It is not a violation of sub-section (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that sub-section for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining
telecommunications service provided by another facilities-based carrier without the authorization of such carrier.

(2) In a prosecution for a violation of sub-section (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose.

(h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under sub-section (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if-

(1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and

(2) the person transports, delivers, convey, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.
Section 1030  Fraud and Related Activity in Connection with Computers

(a) 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 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 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 U.S.C. 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 defence, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any 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 sub-section (c) of this section.

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

(c) The punishment for an offense under sub-section (a) or (b) of this section is-

(f) 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 sub-division of a State or of an intelligence agency of the United States.

Anti-Terrorism Act, 1990, USC, Title 18, Chapter 113b - Terrorism

Section 2332a Acts of Terrorism Transcending National Boundaries

Prohibited Acts-
(1) **Offenses**- Whoever, involving conduct transcending national boundaries and in a circumstance described in sub-section (b)-

(A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or

(B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States;

in violation of the laws of any State, or the United States, shall be punished as prescribed in sub-section (c).

(2) **Treatment of threats, attempts and conspiracies**

Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under sub-section (c).

(b) **Jurisdictional Bases.**

(1) **Circumstances**- The circumstances referred to in sub-section (a) are-

(A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense;

(B) the offense obstructs, delays, or affects interstate or foreign commerce, or would have so obstructed, delayed, or affected
interstate or foreign commerce if the offense had been consummated;

(C) the victim, or intended victim, is the United States Government, a member of the uniformed services, or any official, officer, employee, or agent of the legislative, executive, or judicial branches, or of any department or agency, of the United States;

(D) the structure, conveyance, or other real or personal property is, in whole or in part, owned, possessed, or leased to the United States, or any department or agency of the United States;

(E) the offense is committed in the territorial sea (including the airspace above and the seabed and subsoil below, and artificial islands and fixed structures erected thereon) of the United States; or

(F) the offense is committed within the special maritime and territorial jurisdiction of the United States.

(2) Co-conspirators and accessories after the fact

Jurisdiction shall exist over all principals and co-conspirators of an offense under this section, and accessories after the fact to any offense under this section, if at least one of the circumstances described in subparagraphs (A) through (F) of paragraph (1) is applicable to at least one offender.

(c) Penalties-

(1) Penalties- Whoever violates this section shall be punished-
(A) for a killing, or if death results to any person from any other conduct prohibited by this section, by death, or by imprisonment for any term of years or for life;

(B) for kidnapping, by imprisonment for any term of years or for life;

(C) for maiming, by imprisonment for not more than 35 years;

(D) for assault with a dangerous weapon or assault resulting in serious bodily injury, by imprisonment for not more than 30 years;

(E) for destroying or damaging any structure, conveyance, or other real or personal property, by imprisonment for not more than 25 years;

(F) for attempting or conspiring to commit an offense, for any term of years up to the maximum punishment that would have applied had the offense been completed; and

(G) for threatening to commit an offense under this section, by imprisonment for not more than 10 years.

(2) **Consecutive Sentence**

Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section; nor shall the term of imprisonment imposed under this section run concurrently with any other term of imprisonment.

(d) **Proof Requirements** - The following shall apply to prosecutions under this section:
(1) **Knowledge** - The prosecution is not required to prove knowledge by any defendant of a jurisdictional base alleged in the indictment.

(2) **State law** - In a prosecution under this section that is based upon the adoption of State law, only the elements of the offense under State law, and not any provisions pertaining to criminal procedure or evidence, are adopted.

(e) **Extraterritorial Jurisdiction** - There is extraterritorial Federal jurisdiction-

1. over any offense under sub-section (a), including any threat, attempt, or conspiracy to commit such offense; and

2. over conduct which, under section 3, renders any person an accessory after the fact to an offense under sub-section (a).

(f) **Investigative Authority** - In addition to any other investigative authority with respect to violations of this title, the Attorney General shall have primary investigative responsibility for all Federal crimes of terrorism, and any violation of section 351 (e), 844(e), 844 (f)(1), 956 (b), 1361, 1366 (b), 1366 (c), 1751 (e), 2152, or 2156 of this title, and the Secretary of the Treasury shall assist the Attorney General at the request of the Attorney General. Nothing in this section shall be construed to interfere with the authority of the United States Secret Service under section 3056.

(g) **Definitions** - As used in this section-
(1) the term ‘conduct transcending national boundaries’ means conduct occurring outside of the United States in addition to the conduct occurring in the United States;

(2) the term ‘facility of interstate or foreign commerce’ has the meaning given that term in section 1958 (b)(2);

(3) the term ‘serious bodily injury’ has the meaning given that term in section 1365 (g)(3);

(4) the term ‘territorial sea of the United States’ means all waters extending seaward to 12 nautical miles from the baselines of the United States, determined in accordance with international law; and

(5) the term ‘Federal crime of terrorism’ means an offense that-

(A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and

(B) is a violation of-

(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), sub-section (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnapping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and
weapons of mass destruction threats to the United States) 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnapping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the
United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a foreign terrorist organization), or 2340A (relating to torture) of this title;

(ii) sections 92 (relating to prohibitions governing atomic weapons) or 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C.2122 or 2284);

(iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49; or

(iv) section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).

The EEA criminalizes the theft or misappropriation of trade secrets by computer or other means. The first section specifically addresses the theft of trade secrets/economic espionage with the intent to benefit foreign
governments. The second section addresses the theft of trade secrets/economic espionage more generally. This Act further broadens the federalization of crimes that were historically the province of individual states. Offenses may result in up to fifteen years of imprisonment and/or fines up to $10 million, as well as forfeiture of the property or proceeds thereof.

Mail and Wire Fraud Statutes, 1999

USC, Title 18, Crimes and Criminal Procedure, Part I - Crimes, Chapter - 63 Mail Fraud and other Fraud Offenses

Section 1341 Frauds and Swindles

“Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be
delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in Section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.”

Section 1342  Fictitious Name or Address

“Whoever, for the purpose of conducting, promoting, or carrying on by means of the Postal Service, any scheme or device mentioned in Section 1341 of this title or any other unlawful business, uses or assumes, or requests to be addressed by, any fictitious, false, or assumed title, name, or address or name other than his own proper name, or takes or receives from any post office or authorized depository of mail matter, any letter, postal card, package, or other mail matter addressed to any such fictitious, false, or assumed title, name, or address, or name other than his own proper name, shall be fined under this title or imprisoned not more than five years, or both.”

Section 1343  Fraud by Wire, Radio, or Television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises,
transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

Section 1345 Injunctions against Fraud

(a) (1) If a person is-

(A) violating or about to violate this chapter or section 287, 371 (insofar as such violation involves a conspiracy to defraud the United States or any agency thereof), or 1001 of this title;

(B) committing or about to commit a banking law violation (as defined in section 3322 (d) of this title); or

(C) committing or about to commit a Federal health care offense;

the Attorney General may commence a civil action in any Federal court to enjoin such violation.

(2) If a person is alienating or disposing of property, or intends to alienate or dispose of property, obtained as a result of a banking
law violation (as defined in section 3322 (d) of this title) or a Federal health care offense or property which is traceable to such violation, the Attorney General may commence a civil action in any Federal court-

(A) to enjoin such alienation or disposition of property; or

(B) for a restraining order to-

(i) prohibit any person from withdrawing, transferring, removing, dissipating, or disposing of any such property or property of equivalent value; and

(ii) appoint a temporary receiver to administer such restraining order.

(3) A permanent or temporary injunction or restraining order shall be granted without bond.

(b) The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

So Mail and Wire Fraud Statutes have wide-ranging application to
computer and internet crime. Under these acts, it is illegal to use the mails, interstate, or foreign communications to devise or further fraudulent schemes for obtaining money or property. These statutes, while not primarily regarded as cybercrime statutes, have application to many of the prosecutions for cybercrime. These statutes outlaw any computer-aided or enabled theft. Penalties include fines up to $1 million, and/or imprisonment for up to thirty years.

5.3.12 India

Information Technology Act, 2000

During the discussion of the 2006 Bill, the Standing Committee felt that sufficient interest was not given to the concept of cyber crime and cyber terrorism in the proposed amendments. The Department of Information Technology (DIT) had taken a stand that necessary amendments can be carried out in the Act which will be in tune with the provisions of the Indian Penal Code and Criminal Procedure Code. The Standing Committee, in contrast opined that the age old penal provisions in India are not sufficient to support changes to incorporate cyber crime as a crime with imprisonment for a longer time and with highest fine. The Standing Committee recommended that the DIT formulate stringent, strong and adequate laws to curb cyber terrorism in the country.

It was brought to the notice of the Committee that much needed focus was not given to the issue of cyber terrorism in the 2006 Bill. There was no single provision in the whole of the Information Technology Act when the country was battling against the heinous crime of terrorism during the Mumbai attacks of November 26, 2008. The question put to the Department was if having any legislation dealing with crimes like morphing, cyber terrorism and other
simple cyber crimes punishable with the highest fine and imprisonment will help curb the spread of such offences. The Department was of the view that morphing would anyway be covered under sections 43 and 66 of the Information Technology, (Amendment) Act, 2006. The Department of Information Technology also took the view that cyber terrorism should be made an offence punishable with imprisonment for a term of 10 years and with fine in line with section 120 B and section 121 of the Indian Penal Code. The Standing Committee, however, noted that the term ‘cyber terrorism’ had not been defined anywhere in the IT Act, 2000 or in the 2006 Bill. Ultimately, many of the concerns of the Standing Committee were addressed in the 2009 Amendments.

The 2009 Amendments have created a new offense of cyber terrorism which is punishable with life imprisonment.

Section 2. Definitions

(1) In this Act, unless the context otherwise requires,

(a) “Access” with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(i) “Computer” means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;
(j) “Computer Network” means the interconnection of one or more Computers or Computer systems or Communication device through-

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(k) “Computer Resource” means computer, communication device, computer system, computer network, data, computer database or software;

(l) “Computer System” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(o) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
(p) “Digital Signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(r) “Electronic Form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(t) “Electronic Record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) “Function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) “Indian Computer Emergency Response Team” means an agency established under sub-section (1) of section 70 B

(v) “Information” includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)

(ze) “Secure System” means computer hardware, software, and procedure that -

   (a) are reasonably secure from unauthorized access and misuse;

   (b) provide a reasonable level of reliability and correct operation;
are reasonably suited to performing the intended functions; and

adhere to generally accepted security procedures;

Section 3 Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, “Hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “Hash Result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.
(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Section 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network-

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)

(j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

(i) “Computer Contaminant” means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) “Computer Database” means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) “Computer Virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) “Damage” means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) “Computer Source Code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

**Section 43A. Compensation for failure to protect data (Inserted vide ITAA 2008)**

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes
wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008)

Explanation: For the purposes of this section,-

(i) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) “sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in
force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, “Computer Source Code” means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Section 66. Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

a) the word “dishonestly” shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word “fraudulently” shall have the meaning assigned to it in section 25 of the Indian Penal Code, 1860.

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Section 66C. Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D. Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E. Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section-

(a) transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) capture, with respect to an image, means to videotape, photograph, film or record by any means;
(c) private area means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) publishes means reproduction in the printed or electronic form and making it available for public;

(e) under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that-

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

**Section 66F. Punishment for Cyber Terrorism**

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iv) introducing or causing to introduce any Computer Contaminant;
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 72. Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register,
correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**Section 75. Act to apply for offence or contraventions committed outside India**

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

The discussion of the legal provisions of various countries shows that world is very much concern abbot the terrorist use of the internet and computers. It also shows that except few countries, all the countries are not taking cyber terrorism seriously. Only some have used the term cyber terrorism in their Statues. It is a matter of concern about the threat of cyber terrorism.

### 5.4 International Initiatives and Conferences to Address Cyber Terrorism

Since early history of human population and societies have been changing in characteristics, depending on their way of life like prominent jobs, tools, and
communication, in the early ages it was gathering, hunting, agricultural, industrial, and now the age of Information Society “most of the people work with information related jobs, instead of dealing directly with physical objects”, for each kind of these societies it has also is related offences and crimes. The rapid development of computer and internet technology in last decades, the problem of cyber terrorism has emerged as a global concern. Because of its destructive nature it becomes an alarming issue for the legal fraternity to get effective weapons and means to eliminate cyber terrorists. It has created an entirely new set of problems for law enforcement agencies all over the world. Cyber terrorism brought back the cold war situation again. The United Nations and European Union always played and are playing significant roles to prevent and control the menace. Internet has no territorial boundaries which enable the cyberterrorists to target the other nations without being physically there. The issue of cyber terrorism therefore gets greater international support and cooperation.

Every national or international Incident Response and Security Team should be assigned a global role for tracking the trends in cyber crime and terrorist activities by establishing linkages with the international organizations. However, there are certain essential pre-requisites for the computer security incident response teams to succeed in solving international cyber terrorism. A common terminology in respect of identification of the criminal’s modus operandi, the technical details of the crime, and identification of the targets should exist between the parties involved in the investigation. Absolute understanding should also exist on the common and conflicting societal issues surrounding the crime. The technical competence of all the parties involved in investigating the crime should be known. There should also be complete agreements on how the different types of crimes are to be handled. This

---


provides the best approach in handing the issues of cyber terrorism and cybercrime internationally. This approach is dependent on the international agreements of treaties between the governments of participating countries, as they assist in formal identification and prosecution of perpetrators of cyber crimes and terrorism. There should be an international extradition treaty among all the UN member nations, without any exceptions, in respect of cyber criminals. This would prove to be a very strong deterrent to the potential criminals\textsuperscript{31}.

The realm of any legislation is limited to the national boundaries, whereas the Internet has a global presence. Many countries are facing a challenge in regulating the activities in borderless cyberspace. The global nature of the Internet enables the criminals to easily hide their identity and commit crimes beyond the national borders, without being physically present at the scene of crime. If a hacker in New Delhi attacks the VSNL server, the cyber trail of this crime could force the investigating agency to seek the help of law enforcement agencies of far away countries like USA, England and Australia to pin him down. Though the case may initially seem to be of local nature, still the electronic trail takes the agency through many countries, because the hacker could have utilized the service providers in New York, London and Melbourne to hack the VSNL server at Delhi. The electronic-trail may involve cooperation of different countries, friendly and hostile. Valuable data would be lost or damaged by the time the co-ordination with the international agencies is established and the trial is conducted.

The extra-territorial jurisdiction of the new Indian cyber law is also applicable to any offence committed outside India by any person, irrespective of his nationality, provided the offence involves a computer, or a computer network located in India. This provision of the IT Act 2000 cannot be easily implemented, as our country, does

not have extradition treaty with many countries, where the hacker may reside.

Many international conferences held on the common concern of cyber terrorism. Few of them are below.

5.4.1 **International De Droit Ponel Conference in Germany (1992)**

The Association Internationale De Droit Ponel (ADIP) held the collegiums on ‘Computer Crime and Other Crimes against Information Technology’ in Wartzburg (Germany). Its report stated that only 5% computer crimes were being reported to police. The factors contributing to non-disclosure of cyber crimes\(^{32}\), according to this report, were as follows:

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

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

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

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

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

Though, this conference was not directly related to the cyber terrorism, even the issues discussed then were directly and indirectly related to the cyber menace. So the international community has started discussing terrorist aspect of the internet.

\(^{32}\) The undisclosed cyber crimes are referred as ‘dark figures’ by criminologists.
5.4.2 Twenty-Second G-7 Summit on Cyber Crime (1996)

The member nations\textsuperscript{33} at the G-7 Summit on Anti-terrorism held in Leon (France) in July, 1996 resolved to accelerate mutual consultations and cooperation through appropriate bilateral and multi-lateral meetings on encryption that allows, when necessary, lawful government access to data and communications in order to prevent or investigate acts of cyber terrorism while protecting the privacy of legitimate communications\textsuperscript{34}. The focus of deliberation was on protection of security of information systems, privacy of personal data and protection of intellectual rights of the people.

5.4.3 International Ministerial Conference

In July 1997, the International Ministerial Conference on global information networks was held in Bonn. This Conference brought every member State under one umbrella of information and communication technology. World Wide Web users, International Organizations and Information Technology Industries came together for the protection of net users and to evolve standards of functioning systems and self-regulations.

5.4.4 The Justice and Home Affairs Council

The Justice and Home Affairs Council also came forward to establish practical cooperation between countries worldwide at the investigative and procedural stages., this end the G-8 Senior Level Group on the transnational organ crime was investigating mechanisms to determine, identify prosecute cyber terrorism and other

\textsuperscript{33} The group of G-7 countries consisted of Canada, France, Germany, Italy, Japan, UK and USA.

computer-related crimes\textsuperscript{35}. In 1997, the European Commission, and the European Police forces initiatives to control illegal content on the internet, reporting, investigating cross border links, exchange of information, to reconcile national laws and to co-operate investigations\textsuperscript{36}.

\textbf{5.4.5 G-8 Hi-Tech Crime Working Group (1998)}

In the year 1998, in March to prevent and control the hi-Tech crime G-7 had taken initiatives and the United Kingdom (UK) came forward to combat cyber crimes. G-8 countries are the largest group of industrialized countries in the world. In December 1997 G-8 Conference was held at FBI headquarter of the Justice Ministers of the G-8 countries.

The United States Attorney General Janet Reno said “Criminals no longer are restricted by national boundaries…… If we are to keep up with cyber crimes, we must work together as never before.”\textsuperscript{37}

The news conference released their report for the following areas where these major nations have agreed to collaborate:

i. to assign number of properly trained and equipped law enforcement personnel to investigate high-tech crimes;
ii. to improve ways to control attacks on computer networks;
iii. to prosecute criminals in the country where they are found, when extradition is impossible;

\textsuperscript{36} Ibid.
iv. to preserve key evidence on computer networks;
v. to review the legal codes in each nation to ensure that appropriate crimes for computer wrong doing are prescribed;
vi. to ensure that the language makes it easier to investigate the crimes;
vii. for cooperation with the private sector to develop new ways to detect and prevent computer crimes;
viii. to increase efforts to use new communication technologies, such as, video teleconferencing to obtain testimony from witnesses in other nations.

5.4.6 Paris Cyber Crime Conference (2000)

A 3-day Cyber Crime Conference was held in Paris in May, 2000 which was attended by nearly 300 delegates including judges, police officials, diplomats, legal experts, leading businessman and industrialists from G-8 countries. The conference stressed on the desirability of a global law to tackle the hackers, software pirates, crooks and virus attackers who were making the life of internet users miserable. The members unanimously agreed that there was a need for an international convention to deliberate on cyber crime related issues and urgency of setting up an International Criminal Tribunal having global jurisdiction to deal with cyber crime and criminals. It was further resolved that the nature of cyber crime demands that the concerned countries should actively cooperate and coordinate in the investigation and prosecution of these hi-tech crimes regardless of their territorial boundaries. There should be prompt exchange of evidence in case of cross-country cyber crimes. Therefore, all efforts should be made by the member nations to initiate measures for security of networks on priority basis.

38 Similar issues were also discussed in the 66th U.N. General Assembly Annual Conference of the Interpol held in New Delhi in October, 1997.
5.4.7 European E-Commerce Directive, 2000

The European community has adopted the Directive on Electronic Commerce\(^{40}\) containing set of rules which lay down the standards that will apply to various online intermediaries for their involvement in illegal or infringing material put on their internet facilities by third parties.

There are different types of storage by an intermediary namely, mere conduit, proxy catching and hosting\(^{41}\). The member states cannot impose upon online intermediaries an obligation to monitor the information which they transit or store, nor can member states require intermediaries to seek facts or circumstances indicating illegal activity\(^{42}\). The priority of the European Commission during 2000-07 has been responding to the threat posed by cyber crime in various forms such as phishing, Trojan horses and spamming which affect all economic sectors and call for urgent actions. The Commission has laid greater stress on development of research and development as also the legal and economic initiatives to enhance information security.

5.4.8 European Committee on Crime Problems

In the year 2000, on 22nd December the European Committee on Crime Problems and Committee of Experts on Crime in Cyberspace adopted a draft Convention on cyber crimes with due regards to:


\(^{41}\) European E-Commerce Directive, 2000; Article 13 distinguishes between 3 types of storage as follows:
   a. Storage for the purpose of carrying out transmissions is known as ‘conduits’.
   b. Storage for the purpose of making more efficient the transmission of information onwards is called ‘proxy caching’.
   c. Storage of information provided by a subscriber is known as ‘hosting’.

\(^{42}\) Ibid., Article 15.
(i) common criminal policy for the protection of society against cyber crimes,
(ii) globalization, digitalization and convergence of computer networks,
(iii) preservation of evidence in computer network,
(iv) international cooperation to combat cyber crime,
(v) to adopt necessary measures to deter activities against confidentiality integrity and availability of computer system, networks and data,
(vi) to adopt necessary measures to deter against computer misuse to control cyber crimes,
(vii) to achieve above objectives every member State has to facilitate detection, investigation and prosecution of cyber crimes at national and international level,
(viii) to ensure a proper balance between the interests Of law enforcement and respect for fundamental human rights as established by the European Councils Convention for the protection of Human Rights and Fundamental Freedoms and in the year 1966 the United Nations International Convention on Civil and Political Rights; freedom of expression, freedom to seek, receive and impact information and ideas of all kinds, right to privacy conferred by the Council of European Convention for the protection of individuals with regard to automatic processing of personal data in the year 1981.

To combat cyber terrorism and other cyber crimes the European Council in its draft Convention 2000 adopted certain principles and substantive as well as procedural laws which were also proposed to be followed by all the nations some of these objectives are mentioned below. Under s. 1 it prohibits

1) illegal and unauthorized access, alteration, deletion of computer, computer system and computer network;
2) computer-related crimes;
3) content-related cyber crimes;
4) cyber hacking, fraud, forgery pornography and directed all the nations for cooperation and to adopt extradition policy to help in investigation, detection and prosecution of cyber crimes.

But, the Convention does not specifically mention the word cyber terrorism. However, indirectly we can find it under content related crimes and other cyber crimes when these will be in the nature of causing terror in the mind of general people at large. The convention also proposed to be cordial and co-operative to combat the situation adopting uniform legal system.

5.4.9 European Convention on Cyber Crime, Budapest (November 2001)

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe’s observer states Canada and Japan.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8th November 2001. It was opened for signature in Budapest, on 23rd November 2001 and it entered into force on 1st July 2004. As on November 2013, 41 states have ratified the convention; while a further 11 states had signed the convention but not ratified it.

On 1st March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivates by racism or xenophobia.
i. Objectives of the Convention

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and lawful interception⁴³.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

The Convention aims principally at:

1. Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;
2. Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form;
3. Setting up a fast and effective regime of international cooperation.

The following offences are defined by the Convention: illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-

time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans-border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24 x 7 network for ensuring speedy assistance among the Signatory Parties.

The Convention is the product of four years of work by European and International experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. Currently, cyber terrorism is also studied in the framework of the Convention.

ii. Accession by other Non-European States

The Convention was signed by Canada, Japan, the United States, and the Republic of South Africa on 23rd November 2001, in Budapest. As of November 2013, the non-European states that have ratified the treaty are Australia, Dominican Republic, Japan, Mauritius, and the United States. On October 21, 2013, The Foreign Ministry of Colombia through a press release stated the Council of Europe invited Colombia to adhere to the “Convention of Budapest”. Colombia has not acceded to the convention.

5.4.10 Internet Treaty by Council of Europe (2001)

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

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

(ii) Need for a change in certain substantive and procedural laws that have not kept pace with the changing technology, creating legal challenges to effective prosecution of criminals operating in cyberspace

(iii) Infrastructural needs to enhance the capability and ability of law enforcement agencies to keep pace with changing technology with emphasis on training the people to fight cyber criminality.

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

The treaty of Council of Europe suggested measures which could control cyber crime activities at the global level. The treaty was entitled ‘International Convention on Cyber Crime’ and it was focused on the following three major issues:

i. harmonization of national laws, which defines cyber crimes

ii. laying down definite investigation and prosecution procedures to cope up with global networks

iii. establishment of a rapid and effective system of international cooperation for combating cyber criminality.

Council of Europe (CoE) is a 43 Nations Alliance with US, Canada & Japan as the participating observers.

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

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

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

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

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

5.4.12 ASEAN Regional Forum (2004)

The Association of South East Asian Nations (ASEAN) held a high level ministerial meeting on trans-national crimes in Bangkok (China) on January 8, 2004 recognizing the need for an effective legal cooperation to combat the growing menace of cyber crime in the south east region of Asia. The statement issued by the ASEAN Regional Forum on July 2006 reiterated its resolve to give a thorough fight against
the growing menace of cyber space crime by extending common cooperation in legal and other areas of mutual concern. The theme of the discussion was various issues and challenges involved in the investigation of cyber crimes and measures to be taken to curb this ever growing evil.\(^45\)


In the Eleventh Congress on Prevention of Crime and Treatment of Offenders held in Bangkok on 18-25 April, 2005, the participants reviewed the global picture of cyber crimes and discussed priority concerns for prevention of these crimes. It was realized that the existing national laws were inadequate to check the constantly rising graph of cyber crimes at the international level. Therefore, there was need for bilateral, regional and international cooperation in crime prevention and strengthening of the criminal justice system by the participating nations.\(^46\)


International Cyber Crime Conference was held in Brazilia, during November 6-9, 2006 was the 3\(^{rd}\) major international meet in which hundreds of computer experts participated to deliberate on computer crime related issues and measures to prevent them. The issues taken up for deliberation included electronic and online crime, crime task force model for 21\(^{st}\) century, crucial infrastructure protection program, cyber security, underground hacking activities, criminal file sharing on internet, cyber crime in international context and need for greater international cooperation in cyber crime investigation and extradition of cyber criminals.

5.4.15 Seventh International Conference on Cyber Crime (2007)


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

The focus in the conference was on computer generated terrorist activities and organized crimes through internet which the criminals have found to be a lucrative means to generate huge proceeds of time. It was generally agreed that online child pornography, trafficking in contrabands and e-commerce frauds are showing a rising trend and the acts of vandalism and cheating were increasingly frustrating the e-governance efforts. Therefore, the need of the time demands quick response to the Interpol references and bilateral requests, liberal sharing of forensic technology and more cross-country training exchange programmes besides, timely alert to tackle the cyber crime menace effectively47.

5.4.16 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. It deliberated on problems of international and domestic terrorism, misuse of weapons of mass destruction, organized crime, human smuggling and trafficking, identity theft, online drug trafficking international

monetary laundering, e-commerce, cyber frauds and computer forensics. The focus of the conference was on the extensive use of forensics in cyber crime investigations and involvement of computer experts in the process of investigation.

5.4.17 Third International Conference on Security and Privacy Issues in Information Technology (2008)

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

5.4.18 Conference on Cyber Security Protective Strategies (2009)

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

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

A Conference on Emerging Security Information Systems and Techniques was held on June 18-23, 2009 in Athens (Greece) to review the initiatives taken by participating countries to strengthen their intelligence security informatics.
5.4.19 Conference on Terrorism and Cyber Security (San Lorenzo de El Escorial, Spain, April 16-17, 2009)

This event brought together national and international experts to share their experience in combating the use of the Internet for terrorist purposes and ensuring the protection of the Internet and critical infrastructure from cyber attacks by terrorists. The Conference offered participating States a valuable insight into how to better implement existing policies and standards in these fields. It was also intended as a discussion-oriented forum for exchanging information, experiences, ideas, and innovative approaches.

5.4.20 International Conference on Digital Forensics and Cyber Crime (2009)

The International Conference on Digital Forensics and Cyber Crime was held in Albany (New York, US) from September 30 to October 2, 2009 and it deliberated that a uniform pattern of forensic mechanism should be evolved to tackle the digital related cyber crimes48. This conference was preceded by the Conference on Digital Forensics Security and Digital Law which was held in Pretoria (South Africa) on July 22-24, 2009. It deliberated that the confidential information transmitted through internet and computer system needs to be protected against cyber attacks. The cyber criminals generally resort to spoofing to fish out data and digital informatics. Cyber crimes involving digital copying or piracy specially need a comprehensive digital protection. The need to upgrade digital law providing both civil and criminal liabilities for violation of digital forensics is also an area of paramount concern to facilitate investigation of crimes involving digital violations.

5.4.21 Fifth Annual Conference on Cyber Crime, Council of Europe (2010)

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

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

There was general agreement on the part of participants that legislative reform underway to prevent and control cyber crimes and ensure e-security should sustain. The majority of participants expressed a view that many countries have the global capacity to initiate measures to combat web-based crimes, therefore, there was need to enhance trust in information and communication technology. Primacy should, however, be on protection of privacy and confidentiality, which are subjected to cyber attacks to clinch data pertaining to financial, commercial, technical or defence related computer program. The delegates shared common concern for strengthening of e-security by extending legal protection to database and digital information in view of the fact that internet jurisdiction involves the presence of multiple parties across the globe whose place of residence and cause of action shrouds in uncertainty and defies specific infringement and remedial actions

5.4.22 UN Congress on Crime Prevention (April 2010)

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

5.4.23 The 5th International Conference on Network and System Security
(September 6-8, 2011 Milan, Italy)

The attack systems of cyber terrorists have become more easy-to-use, sophisticated and powerful, interest has greatly increased in the field of building more effective, intelligent, adaptive, active and high performance defense systems which are distributed and networked. The conference covered research on all theoretical and practical aspects related to network and system security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability and sustainability of computer networks and systems NSS 2011 was the next event in a series of highly successful events of Network and System Security. Previous editions were held in: Melbourne, Australia, (2010); Gold Coast, Australia, (2009); Shanghai, China (2008); and Dalian, China (2007).

5.4.24 Octopus Conference Cooperation against Cybercrime (6 - 8 June, 2012, Council of Europe, Strasbourg, France)

In the three days long conference, many experts from the computer and allied areas participated. There was a great concern on the Budapest conference and its outcomes and the emerging trends in the cyber zone.

i. All were agreed on major capacity building effort is needed to assist countries worldwide to curb the menace of cybercrime and this will facilitate cooperation between international organisations to provide best possible services to societies in all regions of the world.

ii. Cybercrime affects core interests and development opportunities of societies so curbing cybercrime will enhance human rights and the rule of law.

iii. Official development aid should increasingly be made available for technical assistance against cybercrime so the confidence and trust in information and communication technologies remains.
5.4.25 Workshop on Effective International Cooperation in the area of Cybercrime Investigation and Prosecution (May 20th, 2013)

The Ministry of Foreign Affairs of Japan hosted Workshop on Effective International Cooperation in the area of Cybercrime Investigation and Prosecution in Tokyo on 20 May, 2013. The workshop is hosted by the Government of Japan to share with the countries in the Asia Pacific region Japan’s experience leading up to the conclusion of the Cybercrime Convention (Japan concluded the Cybercrime Convention last July and it came into force in Japan last November). The objective is to exchange views with the countries in the Asia Pacific region on cybercrime investigation and prosecution and to promote an effective international cooperation.

Government experts from 16 countries in the Asia Pacific region and (UNODC), (UNAFEI), Interpol and the Council of Europe also attended this workshop. Cybercrime easily transcends national borders, international cooperation is crucial in tackling this crime, and that utilizing the existing frameworks and assisting capacity building of national criminal justice systems are very useful in promoting effective international cooperation.

5.4.26 Multidisciplinary Conference on Cyber Terrorism - Final Report

The Cyber terrorism Project was established at Swansea University, UK in 2011 by academics working in the School of Law, College of Engineering, and Department of Political and Cultural Studies. The project has four primary objectives:

i. To further understanding amongst the scientific community by engaging in original research on the concept, threat and possible responses to cyber terrorism.

ii. To facilitate global networking activities around this research theme.

iii. To engage with policymakers, opinion formers, citizens and other stakeholders at all stages of the research process, from data collection to dissemination.

iv. To do the above within a multidisciplinary and pluralist context that draws on expertise from the physical and social sciences.

Findings of the project

i. It is clear that cyberspace opens considerable potential opportunities for terrorist activities, including communication, fund-raising and attacks. It remains an open question whether terrorist uses of the Internet constitute an evolutionary or revolutionary dynamic. This question hinges, in part, on one’s view of how the Internet differs to earlier technologies.

ii. There are multiple constraints on terrorist engagements with cyberspace. First, the feasibility of the terrorist activities listed above varies considerably with some requiring very little technical knowledge and others necessitating a high level of expertise. In addition to this are further constraints such as financing and the comparative desirability of more traditional attacks for reasons of visibility or knowhow.

iii. A range of legal and political instruments are available within national and international bodies with which to confront the challenge of cyber terrorism. However, these instruments are limited by different factors including: different strategic cultures and capabilities across countries; the language and construction of existing legal instruments such as the ‘use of force’ requirement in international law; and, sensitivities towards sharing information and data.

51 Ibid.
iv. Distinguishing between different types of cyber-threat is challenging, in part, because motives and behaviour in this realm are difficult to identify and monitor.

v. The value of existing models and methods of deterrence to confront challenges such as cyber terrorism is unproved, at best.

vi. Efforts to address threats such as cyber terrorism raise considerable ethical as well as political, legal and technical challenges.

vii. Cyber terrorism has a discursive existence as well as a ‘material’ one. How this phenomenon is framed or constructed in media and political language matters greatly.

viii. The disciplinary backgrounds and commitments of academics are not incidental within debate on the definition of cyber terrorism. In part, this is because of different views of the purposes of definition itself: to ensure effective communication between researchers and/or policymakers; to facilitate cooperation across jurisdictional boundaries; to distinguish terrorism from crime and war; or, to impose limits on investigative and prosecutorial powers.

International conferences/congresses/workshops held from time to time shows the concern of global community and its efforts to control and curb cyber terrorism. However, many States have also enacted their own domestic legislation on cyber laws as under given, this is not final but only the few countries concern on cyber crimes.

5.5 Conclusion

New multimedia technology and internet have become part of our daily life in contemporary society and have made life easier, quicker and cheaper. Computers are not only useful for communication and information processing but also useful for typing, editing, drawing, copying, printing, musical purposes,
microwave, door keys, remote car driving, to use as remote control, in the form of wireless, mobile phone and so on with ever increasing utility around human society.

Such tremendous utility of Information and Communication Technology (ICT) encouraged the terrorists and other deviants in society to use it sometimes as their tool and sometimes as targets to fulfill their ends. Internet became a way which may be called superhighway or information way (I-Way) for war. That is why one can call it a war as cyber war or net war in I-Way. Pakistan, China attack against India and the USA through I-Way are cyber war.

Terrorists very easily attack through this superhighway in cyber world on their targets. Cyber terrorism became one of the complex challenges in contemporary global scenario. There is great need of intensive study, research and protest against this dangerous national and international evil in society.

Cyber terrorism is a kind of cyber threat using new technology. It is national as well as international challenge. Warfare is one way of cyber terrorism by which one nation attacks other nations through information way (I-way). That may be called as net war. International terrorists attack using websites and controlling network i.e., Al-Qaida’s websites http://www.mojahedoon.net which has link with Osama Bin Laden, attack on Indian Parliament on 13th December 2001 by making false gate pass from internet, on 11th September 2001 attack on WTO and Pentagon controlling network of airway, on 16th December 2005 electronic mail threat to attack Indian Parliament and US consulate are examples of cyber terrorism in India.

As the above discussed, many countries have enacted their national laws or amended their existing laws yet when one country’s laws criminalize high-tech and computer-related crime and another country’s laws do not, cooperation
to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible. Inadequate regimes for international legal assistance and extradition can therefore, in effect, shield criminals from law enforcement; criminals can go unpunished in one country, while they thwart the efforts of other countries to protect their citizens. We have seen that efforts to control cyber terrorism very few nations have taken steps to have legal provisions in their statutes and the effectiveness of even those who have taken the lead is also uncertain. In the face of the emergence of cybercrime at national level and the global implications of the crime, moreover, different legal systems of different nations, it becomes more difficult if not impossible to have any effective legal control mechanism.