Lecture in 12th working Session on 28th February,2010 in International Conference of Jurists on Sea: Global Warming & Rule of Law organized by International Council of Jurists at Lido Auditorium of Super Star Virgo Cruise, Singapore

By

Justice Rajesh Tandon,
Chairperson,
Cyber Appellate Tribunal
Ministry of Communications & Information Technology Department of Information Technology,
Jeevan Bharti (LIC) Building, Connaught Place,
New Delhi.

Subject

CYBER TERRORISM AND LAW

The Information Technology Act,2000 came into force on 17th October, 2000. This Act was amended vide notification dated 27th October,2009. The Definitions in the Amended Act are as under:

(a) "Act" means Information Technology Act,2000 (21 of 2000)

(b) "Communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication"

(c) "Communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource.

The Information Technology Act,2000 was introduced on 9th June,2000. Mitigation that has led to the introduction of the Information Technology Act,2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No.51 of 162 dated 30th January,1997 which has recommended that all the States should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication. The preamble of Act 21 of 2000 provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act,1872, the Banker's Books Evidence Act,1891 and the Reserve Bank of India Act,1934 and for matters connected therewith or incidental thereto;

Whereas the General Assembly of the United Nations by resolution A/RES/51/162 dated 30th January,1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade law;

And whereas the said resolution recommends, inter alia, that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information."

Gradually the Act was amended on 5th February,2009 being the Amendment No.10 of 2009 which has introduced the world digital signature instead of electronic signature as provided under Chapter II of Section 3 of the Act. In Section 2, Clause (ha) was introduced after the word (h) which provides the Communication device. It reads as under:

"Communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;"

The Information Technology Act,2000 came into force on 17th October, 2000. It has 94 sections divided into 13 chapters. This Act was amended vide notification dated 27th October,2009.

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd edition 2005 has defined the same in the word of `Cyberspace". It has used a term as a `floating' in an electronic environment, which is accessible internationally. Then the Author has also defined the `Cyber theft' known as the act of using an online computer service.

In this dictionary `Cyber law' is defined as under:-

> "The field of law dealing with computers and the Internet including such issues as intellectual property rights, freedom of expression, and free access to information."

The definition of the Information Technology Act provides as under:

"Computer" means any electronic, magnetic, optical or other high speed date 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;

Section 1(2) of the Information Technology Act,2000 reads as under:-

> "1(2) "It shall extend to the whole of India and, save as otherwise provide din this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

PROVISIONS RELATING TO JURISDICTION IN CYBER SPACE UNDER THE INFORMATION TECHNOLOGY ACT,2000

The most powerful invention of the 20th Century is the **information and communication technology** for the society and its application for the society development such as administration of **Information and Communication technology** in judicial system will play an integral role for the society to trust on its judicial process, due to its inherent advantage of fast processing, Trivial retrieval, less human intervention, relatively low cost of development and in some criminal cases where physical presence is an issue this solution is the best one .

The offences under the Information Technology Act are as under:

(1)Tampering computer source documents. **Section 65**

(2)Hacking with Computer System
Data alteration **Section 66**.

(3) Punishment for sending offensive messages through communication service etc. Section 66A

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

(5) Punishment for identity theft. Section 66C

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

(7) Punishment for violation of privacy. Section 66E.
(8) Publishing obscene information . **Section 67**
(9) Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Section 67A

(10)Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. Section 67B
(11) Preservation and retention of information by Intermediaries. Section 67C

(12) Un-authorized access to protected system. **Section.70**

(13) Penalty for misrepresentation. Section 71

(14) Breach of Confidentiality and Privacy **Section 72**

(15) Punishment for disclosure of information in breach of lawful contract. Section 72A

(16) Publishing false Digital Signature Certificates. **Section 73**

Section 78 of I.T. Act empowers Inspector of Police to investigate cases under the Act.

JURISDICTION UNDER THE INDIAN PENAL CODE IN RELATION TO CYBER OFFENCES

(i)	Sending threatening messages by email	Section 503 IPC
(ii)	Sending defamatory messages by email	Section 499 IPC
(iii)	Forgery of electronic records	Section 463 IPC
(iv)	Bogus websites, cyber frauds	Section 420 IPC
(v)	Email spoofing	Section 463 IPC
(vi)	Web-jacking	Section 383 IPC
(vii)	E-Mail Abuse	Section 500 IPC
(viii)	Online sale of Drugs	NDPS Act
(ix)	Online sale of Arms	Arms Act

Cyberterrorism

Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyberterrorism. Cyberterrorism can also be defined much more generally, for example, as "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives." This broad definition was created by Kevin G. Coleman of the Technolytics Institute.[1] The term was coined by Jared Westrup.[2]

In the wake of the recent computer attacks, many have been quick to jump to conclusions that a new breed of terrorism is on the rise and our country must defend itself with all possible means. As a society we have a vast operational and legal experience and proved techniques to combat terrorism, but are we ready to fight terrorism in the new arena – cyber space?

A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism.

As a society that prides itself on impartiality of justice, we must provide clear and definitive legislative guidelines for dealing with new breed of terrorism. As things stand now, justice cannot be served as we have yet to provide a clear definition of the term. In this light, I propose to re-examine our understanding of cyber-terrorism.

There is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar "cyber" and less familiar "terrorism". While "cyber" is anything related to our tool of trade, terrorism by nature is difficult to define. Even the U.S. government cannot agree on one single definition. The old maxim, "One man's terrorist is another man's freedom fighter" is still alive and well.

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd Edition 2005 has defined **`Cyber theft'** known as the act of using an online computer service.

In this dictionary **`Cyber law'** is defined as under**: -**

> "The field of law dealing with computers and the Internet, including such issues as intellectual property rights, freedom of expression, and free access to information."

The ambiguity in the definition brings indistinctness in action, as D. Denning pointed in her work Activism, Hactivism and Cyber terrorism, "an e-mail bomb may be considered hacktivism by some and cyber-terrorism by others"

It follows that there is a degree of "understanding" of the meanings of cyber-terrorism, either from the popular media, other secondary sources, or personal experience; however, the specialists' use different definitions of the meaning. Cyber-terrorism as well as other contemporary "terrorisms" (bioterrorism, chemical terrorism, etc.) appeared as a mixture of words terrorism and a meaning of an area of application. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term "Cyber terrorism", defined cyber-terrorism as the convergence of cybernetics and terrorism. In the same year Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."

Since that time the word cyber-terrorism has entered into the lexicon of IT security specialists and terrorist experts and the word list of mass media "professionals". One of the experts, a police chief, offers his version of definition: "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."

The media often use cyber-terrorism term quite deliberately: "Canadian boy admits cyberterrorism of his family: "Emeryville, Ontario (Reuter) - A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday"

A renowned expert Dorothy Denning defined cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". R. Stark from the SMS University defines cyber-terrorism as " any attack against an information function, regardless of the means"

Under the above-mentioned definitions of cyber-terrorism one can only point to the fact that any telecommunications infrastructure attack, including site defacing and other computer pranks, constitute terrorism. It means that cyber-terrorism has already occurred and we "live " in the epoch of cyber terror.

However, another expert, James Christy the law enforcement and counterintelligence coordinator for the DIAP (Defense-wide Information Assurance Program), which is steered by the office of the assistant secretary of defense for command, control, communications and intelligence, states that cyber-terrorism has never been waged against the United States. "Rather, recent hacking events – including a 1998 web page set up by a supporter of the Mexican Zapatistas rebel group, which led to attacks on the U.S. military from 1,500 locations in 50 different countries – constitute computer crime. William Church, a former U.S. Army Intelligence officer, who founded the Center for Infrastructural Warfare Studies (CIWARS) agrees that the United States has not seen a cyber terrorist threat from terrorists using information warfare techniques. "None of the groups that are conventionally defined as terrorist groups have used

information weapons against the infrastructure" Richard Clarke, national co-coordinator for security, infrastructure protection and counterterrorism at the National Security Council offered to stop using "cyberterrorism" and use "information warfare " instead

The above-mentioned observations drive a clear line between cyber-terrorism and cyber crime and allow us to define cyber-terrorism as: **Use of information technology and means by terrorist groups and agents.**

In defining the cyber terrorist activity it is necessary to segment of action and motivation. There is no doubt that acts of hacking can have the same consequences as acts of terrorism but in the legal sense the intentional abuse of the information cyberspace must be a part of the terrorist campaign or an action.

Examples of cyber terrorist activity may include use of information technology to organize and carry out attacks, support groups activities and perception-management campaigns. Experts agree that many terrorist groups such as Osama bin Ladenn organization and the Islamic militant group Hamas have adopted new information technology as a means to conduct operations without being detected by counter terrorist officials.

Thus, use of information technology and means by terrorist groups and agents constitute cyber-terrorism. Other activities, so richly glamorized by the media, should be defined as cyber crime.

Cyber terrorism

The most deadly and destructive consequence of this helplessness is the emergence of the concept of “cyber terrorism”. The traditional concepts and methods of terrorism have taken new

dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism. The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace " is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straightjacket formula or pigeons hole. In fact, the first effort of the Courts should be to interpret the definition as liberally as possible so that the menace of cyber terrorism can be tackled stringently and with a punitive hand. The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world. The laws have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognises no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which a country may not have any reciprocal arrangements, including an "extradition treaty". The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security

technology and a law dealing with cyber terrorism is the need of the hour.

The Internet is a global medium of communication, business and information. The nature of the medium is such that many financial and economic frauds, data breaches, hate-speech on blogs, occur on a large scale. For instance, many credit card numbers and passwords are frequently stolen or breached. The scales of many of these crimes are due to the nature of the medium which is global. Many of these large scale economic offences, run the risk of being labeled as acts of "cyber terrorism" under the law, entailing punishment upto life imprisonment. While expanding the ambit of "terrorism" to economic offences on one hand through section 66F and repealing anti-terror laws such as PTA and TADA that dealt with violent acts of terror on grounds of gross misuse, is a major contradiction.

With the increasing use of computers and Internet, the cyber crime is also on the rise. Some such offences are new like 'denial of service' attacks, 'phishing', credit card fraud etc. The others are different ways to commit conventional crimes such as Nigerian Fraud (cheating using online medium), blackmailing, defamation through e-mails. In recent days general citizens, govt. Departments, Private organizations and Bank including foreign banks operating in India, are approaching the Cyber Crime PS with different nature of complaints relating to tampering of computer source documents, Phishing of user names & passwords of net banking accounts, Nigerian Frauds, receiving of abusive and defamatory e-mails, hacking of e-mail IDs, fraudulent withdrawals of amounts through debit and credit cards etc.

The following table shows the number of cases reported at Cyber Crime PS with head wise break up during 2008 & 2009. There is no exclusive designated Court for the Cyber Crime Police Station, CID.

	Source Code Tampering (Sec. 65 IT Act)	Hacking (Sec. 66 IT Act)	Obscene Content (Sec. 67 IT Act)	Nigerian Fraud	Phishing	Credit and Debit Card misuse	Others	Total
2008	-	7	2	2	10	-	1	22
2009	1	4	5	6	7	3	2	28

Since inception the officers and staff of Cyber Crime Police station, CID kept up the expectations and successfully investigated the reported cases. The IPC cases the investigation of which require computer skills are also investigated at Cyber Crime PS on being specially entrusted by the chief of CID. The case in Crime No. 17/2008 U/s 419,420,468 & 471 IPC requires special mention where in an amount of Rs. 48 Lakhs was siphoned off by two young educated offenders from the ICICI Bank, Khairathabad SB Account. In this case the offenders have exploited the loopholes that prevailed in the Banks and others financial institutions and committed the fraud. One of the accused persons worked in the call centre of ICICI Bank on temporary basis, by which he could gain the critical information of the account having found huge balance. Then he along with co-accused opened false India Bulls trading account and also false AXIS bank account. They have first transferred the amount from the victim's ICICI Bank SB Account to India Bulls account and from that to fake Axis Bank account, Tarnaka Branch, Hyderabad from where they could withdraw the whole amount. After the detection of the case, a letter was addressed to the Reserve Bank of India mentioning the instances of

loopholes in the banking system exploited by the culprits for executing the said fraud and with advice to take necessary corrective steps on the loopholes in the banking system. There are already indications that RBI has moved swiftly and alerted all the banks on this count and directing them to adhere more stringently to the guidelines. Similarly CBI, DOT are also addressed about such system loopholes that have come across while the investigation of cyber offences. In specific addressed letters to DOT with reference shared IP Addresses and to CBI with reference to Bank Frauds, e-mail high jacking, Nigerian frauds.

FUTURISTIC POLICE COMMUNICATION – ASSAM POLICE CONVERGENCE NETWORK (APCN)

Convergence technology integrating voice, video and data in a single network is a major development in computer and communications technology and found appropriate for adoption in Police communication. This can be augmented by the 4G like system which adds multimedia facilities to wireless by allowing audio, video and graphics application. The Assam Police Convergence Network (APCN) proposed under Vision 2020 incorporates convergence along with the adoption of 4G technology in order to achieve the common integrated networking of Police Communications. APCN can provide integration of the isolated Police nets to achieve an integrated networking with higher Bandwidth and introduction of a PDA (Personal Digital Assistant) kind of hand-set for the police officials catering to all three requirements of voice, video and data transmissions. Convergence technology integrating voice, video and data in a single network is a major development in computer and communications technology and found appropriate for adoption in

Police Communication. 3G is an ITU specification for the third generation of mobile communications technology. The 3G technology adds multimedia facilities to mobile phones by allowing audio, video and graphics application. 3G promises increased bandwidth, up to 2 Mbps in fixed applications, 384 Kbps when a device is stationary or moving at pedestrian speed and 128 Kbps in a car. 4G is the fourth generation wireless superceding 3G in respect of band-width, end-to-end IP, high quality video etc.

Third generation (3G) and fourth generation (4G) system promise faster communications services, including fixed, mobile, voice, data, fax, internet and multimedia services, anytime and anywhere with seamless global roaming. One of its key visions is to provide seamless global roaming, enabling users to move across borders while using the same number and handset. This technology can be appropriately adopted to cater to the requirements of Police Communication all over India.

WHY AND WHEN A CRIMINAL NEEDS A BANK

The criminals are in the business of generating money whether from bank robberies or from financial frauds or from selling narcotics; and once they have the money, it is no good to them unless they can use it. This is where the banks come into play. The banks are the prime place the criminal wants to have his money so that he can use it for his benefit, whether that is to buy toys like cars, boats or aeroplanes or to collect high valued works of art or any other of a myriad of activities. If the criminal can place his money into banks that have a level of secrecy from the law enforcement that is investigating him, that is what he will do .

When a bank receives dirty money it can do one of the two things: Provide a safe haven for the criminal or provide law enforcement a unique and valuable source of information. If it provides the information, the high level criminal (even the head of an organized criminal organization) can be identified and tied to the ill-gotten gains and therefore to the crime. Once this is done, law enforcement is a step closer to prosecuting him and putting him in jail. On the other hand, if the banks provide an atmosphere of protection where the criminal can safely hide his money away from the prying eyes of law enforcement then the criminal will go scot-free.

POLICE AS AN INSTRUMENT OF SOCIAL CHANGE

It is important to know what type of social change we are talking about. If the social change is for an egalitarian, secular, castless, classless modern society or if it is for otherwise, as the utter paradox is that Police now follow orders and try to prove themselves more subservient to the wishes of power wielders, regardless of ideal implications and imperatives.

If society gets divided on the basis of class, cast subcast, religion and other parochial and other jingoist issues then a docile and divided Police force will also be equally shattered to pieces.

In that context it is very relevant to first get Police house in order and – insulate it. So that, it, at least can withstand negative personal onslaughts contrary to the law and ideals as enshrined in the constitution and federal laws, state laws as well as in the Directive Principles of state police.

If we see the real picture then it is a sight in sadness to see a weak, implementation of law of land on the grounds if losing vote bank and for appeasing politicians as well as for the alibi of alienating a particular class.

Social change is a quantum process, it happens in jumps, with strong minds and leadership and requires a strong well disciplined and oiled machinery to implement it. Following broad points need consideration.

TERRORISM – A CHALLENGE BEFORE THE NATION

The year 2008 will go down as a period when India was held hostage by terror. It began on 1st January 2008 itself with an attack by Lashkar on CRPF camp in Uttar Pradesh and virtually every month in 2008, news of terrorist attacks were pouring in. By the time 2008 drew to a close with Mumbai's 60-hou horror India had lost 434 precious lives in nine major terror attacks. Terrorist attacks took place in almost all corners of our country and in all our major cities. IN addition to this the continuing insurgencies in Kashmir and the North-East claimed 1,157 lives this year. Be it the rich or the poor terrorism affected all of us equally. It was found that a large number of incidents to terrorism was perpetrated by those having complex interstate and international linkages and connection with anti-national activities such as smuggling of arms, drugs, infiltration, pushing in and circulation of fake currency.

POLITICALLY MOTIVATED ACTION

Terrorism is a politically motivated action combining psychological (fear inducing) and physical (violent action)

components carried out by individuals or small groups with the aim of forcing or compelling the state or the authorities to meet their demands. That is, political terrorism can be thought of as the use of violence by a group acting either on behalf of, or in opposition to, an established authority. The key element is the prosecution of activities with a view to wear out the established authority by causing panic, destruction, distrust and demoralization among the people at large. Thus, the range of such activities covers cases of hijacking or buses and planes, taking of any person or persons as hostage, abduction of the leaders or their family members, assassination of heads of states or government or of important political personalities, explosion of bombs to destroy public buildings and kill innocent people living or assembled therein and the like. Thus, the terrorists believe in the 'cult of the pistol and the bomb'. In short terrorism "is a political goal-oriented action, involving the use or threat of extra ordinary violence performed for psychological rather than material effect." The victims, mostly innocent, are symbolic sacrificial goats for the sinister design of the terrorist. With some rogue states supporting the terrorist elements and even providing men, material training and brazen support international terrorism of late acquired dangerous propositions.

SECOND ARC ON FIA

The second administration reforms commission (ARC) headed by Veerappa Moily recommended in its $7^{th}/8^{th}$ report submitted to the government in September 2008 the creation of a Federal Intelligence Agency (FIA) which could be set up by ordinance or through a constitutional amendment to the National Security Act of 1980. Earlier a similar proposal was made by the

Subrahmanyam Committee on security reforms set up by the NDA government. Neither proposal was acted upon, in part, according to Moily, because the states are apprehensive that this might infringe upon their rights in the federation. While this is an important concern, it is possible to accommodate it in another way, for example through some consultative machinery in an advisory capacity so that national security, which is a responsibility of the centre, is not jeopardized as it has so often been.

According to the recommendations of the Moily and Subrahmanyam Committees the FIA should be responsible for coordinating tasks that are divided among different intelligence agencies such as RAW, IB, CBI, etc. Additionally, it has been suggested that the authority should also coordinate between State Police Forces through the appointment of special police commissioners. Though the coordination of intelligence inputs is under the purview of national security under the Home Ministry, having a dedicated authority will at least make a sole agency responsible. To that extent it may succeed in plugging some of the existing gaps, especially in information transfer to prevent or minimize terrorist attacks.

The 11/9/2001 terrorist attack was an eye opener to the world as all countries awoke to the necessity of making stringent law to punish the merchants of death and destruction. Australia, USA, Italy, Canada and later France came out with harsh deterrent laws to punish the enemies of civilization. In India also, the then Vajpayee government enacted the Prevention of Terrorist Activities Act (POTA) which was later criticized by the opposition parties and labeled it as a draconian measure. Consequently when the United Progressive Alliance (UPA) government came to power

in 2004 it repealed the POTA and again the country is left without any law against terrorism. This might have emboldened the terrorist organizations to indulge in more inhuman and barbaric acts of terrorism as witnessed during 2008. there was wide criticism that while the entire world is making stringent laws to punish the terrorist, India was trying to survive without a proper and effective law against this scourge. On December 12, 2008 about 40 intellectuals including former Justices and Chief Justices petitioned to the leaders of political parties to usher in reforms in police administration and the government took the same seriously and ultimately came out the two bills – the national Investigation Agency Bill and the Unlawful Activities (Prevention) Amendment (UAPA) Bill of 2008.

Therefore, in December 2008 the Government of India enacted the National Investigation Agency (NIA) Act to constitute an apex body on the lines of the Federal Bureau of Investigation (FBI) of the United States of America. The establishment of NIA will give the Centre the power to suo moto direct the NIA to investigate certain offences. FBI in the US, for instance investigates not only terrorist and espionage cases but also white collar crimes and corruption cases. For India a federal agency on the lines of NIA is long over due. After the constitution of NIA the Central government is empowered to decide what constitutes terror and investigate such attacks in any part of the country covering offences, including challenge to the country's sovereignty and integrity, bomb blasts, hijacking of aircraft and ships and attacks on nuclear facilities. The NIA should have sufficient infrastructure, so that it can function on par with the best investigating agencies of the world. The selection of the NIA officials should be transparent and fair so that its functioning is not affected.

Today terrorism is a grave threat to world peace with notorious organizations like AI Qaida, Jaish-e-Muhammad, Lashkar-e-Taiba, etc., spearheading this barbaric form of protest. There is growing fear of unspeakable consequences if weapons of mass destruction fall into the hands of these agents of destruction. The nations partronizing international terrorists must be identified and terrorists must be identified and isolated. All material and financial assistance to such countries must be stopped and international travel and communication be suspended. "In order to contain international terrorism effectively, nations especially those who have been the frequent targets of international terrorists, should increase cooperation among themselves by coordinating their anti-terrorist activities."

DEFINING CRIME

Generally, crime is the deviant behavior or an individual against the accepted norms of the society. In general, human actions can be classified into two broad categories: (i) those conforming to the norms of the society, and (ii) those not conforming to these norms. Thus, conformity to norms means behavior according to generally accepted norms of the society while non-confirming means violation of these accepted norms. But there is persistent vagueness in the definition of crime and deviant behavior. Crime, as defined in criminology, is violation of legal norms. In the social sense, deviant behavior is the commission of an act prohibited by the society. The idea of deviant behavior is not an invention of a sociologist but is a fact of social life. People in society, term certain acts as violation of norms and certain individuals as norm-breakers. Nevertheless, they would fail to precisely define deviance and conformity because sometimes

people themselves are not sure as to what deviance and conformity are. Thus, the concept of crime is relative in the context of law as well as society. In the unfolding history of criminal laws in different parts of the world, the concept of crime as to what it entails has also undergone a vast change. For instance, the practice of Sati, child marriage and discrimination on the basis of caste were socially acceptable and practiced in India once upon a time. Today, they are all punishable under the law of the land."

MEETING THE MAOIST CHALLENGE – POLICE RESPONSE

What is Maoism? Is it a typical communist ideology, is it a call to arms, is it a manual for rural guerilla warfare? It appears to be all this and much more.

The rise of Mao Tse Tung and his People's Liberation Army in China was the culmination of a series of factors in China.

One was the humiliations faced by the Chinese from the mid 19th century when foreign powers such as UK, USA, and other European countries forced the Qing dynasty to grant them trading concessions.

Second was the grabbing of huge chunks of Chinese territory by Russia and Japan in the 19th century.

Third was the all pervading corruption of the Chinese administration where the peasantry bore the brunt of a corrupt and feudal system.

From 1926 the Guomindang party and the Communists had allied to drive out the foreigners and warlords from China. Gradually the Communists under the leadership of Mao Tse Tune and Zhou Enlai, Ju Deh and others built up their guerrilla bases and guerrilla areas and by 1949 had thrown both the Japanese

occupation army and Chiank Kai Chek out of the Chinese mainland.

One point overlooked by many is the help received by the Chinese Red Army from the Russians. The Russians had played an important role in defeating the million strong Japanese army in Manchuuria in 1945. The Russians handed over to the Chinese Communists huge amounts of captured Japanese military supplies – 3700 artillery pieces, 600 tanks, 861 planes apart from many naval vessel ('Guerrilla warfare & Marxism' – International Publishers – p27)

The following quotations from Mao Tse Tung clearly illustrate the principles of revolutionary war propounded by him.

Every communist must grasp the truth, "Political power grows out of the barrel of a gun".

(Mao Tse Tung, in "Problems of War & Strategy", Nov 6, 1938, Selected Works, Vol. II p. 224)

"War is the continuation of politics and war itself is a political action; since ancient times there has never been a war that did not have a political character……

But war has its own peculiar characteristics and in this sense it cannot be equated with politics in general. War is the continuation of politics by other means"…….. It can therefore be said that politics is war without bloodshed while war is politics with bloodshed.

The seizure of power by armed force, the settlement of the issue by war, is thew central task and the highest form of revolution. The Marxist Leninist principle of revolution holds good universally, for China and for all other countries….. Mao Tse Tung

According to Marxist theory of the state, the army is the chief component of state power. Whoever wants to seize and retain state power must have a strong army. Some people ridicule us as advocates of the "omnipotence of war." Yes, we are advocates of the omnipotence of revolutionary war; that is good, not bad, it is Marxist. The guns of the Russian Communist Party created socialism. We shall create a democratic republic. Experience in the class struggle in the era of imperialism teachers us that it is only by the power of the gun that the working class and the laboring masses can defeat the armed bourgeoisie and landlords; in this sense we may say that only with guns can the whole world be transformed

The revolutionary war is a war of the masses; it can be waged only by mobilizing the masses and relying on them.

MALAYSIA

Before analyzing the cyber crime related laws in Malaysia, it is important to have a basic understanding about the foundation of the Malaysian legal system.

The Constitution of Malaysia provides for a dual justice system – the secular laws (criminal and civil) and sharia laws (applicable for Muslims in personal law matters e.g. marriage, inheritance etc).

Federal laws enacted by the Parliament of Malaysia apply throughout the country while state laws enacted by the State Legislative Assemblies apply to the particular state.

The application of English law or common law is specified in the statutes. Section 5 of the Criminal Procedure Code states that English law shall be applied in cases where no specific legislation has been enacted. Similarly, in the context of civil law, Sections 3 and 5 of the Civil Law Act allows for the application of English common law, equity rules, and statutes in Malaysian civil cases where no specific laws have been made.

The investigation of crimes comes under enforcement agencies like the Royal Malaysian Police, Anti Corruption Agency, Royal Customs and Excise, Securities Commission etc. The prosecution is under the Attorney General.

UNAUTHORISED ACCESS

According to section 2(2) of the Computer Crimes Act, a person **secures access** to any program or data held in a computer if, by causing a computer to perform any function, he:

1. alters or erases the program or data; or
2. copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; or
3. uses it; or
4. causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

Section 3 of the Computer Crimes Act prohibits acts or unauthorized computer access. A person is guilty of an offence under this section if:

1. he knowingly causes a computer to perform any function with intent to secure access to any program or data held in any computer;
2. the access he intends to secure is unauthorized; and

Section 4 of the Computer Crimes Act prohibits unauthorized access with intent to commit or facilitate commission of further offence. A person is guilty of an offence under this section if he commits an offence referred to in section 3 with the intention:

1. to commit an offence involving fraud or dishonesty or which causes injury, or
2. to facilitate the commission of such an offence whether by himself or another person.

Violation of this section is punishable with imprisonment upto **10 years** and / or fine upto **1,50,000 ringgit**.

SINGAPORE

Before analyzing the cyber crime related laws in Singapore, it is important to have a basic understanding about the foundation of the Singapore legal system. According to the Singapore Ministry of Law website:

Singapore is a republic with a parliamentary system of Government.

The roots of Singapore's legal system can be traced back to the English legal system and it has evolved over the years. The

sources of law are derived from our Constitution, legislation, subsidiary legislation (e.g. Rules and Regulations etc) and judge-made law.

The Constitution is the supreme law of the land and lays down the basic framework for the three organs of state, namely, the Executive, the Legislature and the Judiciary.

The Executive includes the Elected President, the Cabinet and the Attorney-General. The President is elected by the people and is empowered to veto government budgets and appointments to public office. The Cabinet comprises of the Prime Minister and Ministers appointed from among the Members of Parliament and is responsible for the general direction and control of the Government and is accountable to Parliament. The Attorney-General is the principal legal advisor to the government and has the power and discretion to prosecute offenders.

The Legislature comprises the President and parliament and is the legislative authority responsible for enacting legislation. Parliament is made up of elected, non-constituency and nominated Members of Parliament. The President's assent is required for all bills passed by Parliament and he may in his discretion withhold assent to certain bills.

The Judiciary consists of the Supreme Court and the Subordinate Courts and the head of the Judiciary is the Chief Justice. Judicial power in Singapore is vested in the Supreme Court and in such subordinate courts as may be provided for by any written law for the time being in force.

According to the Supreme Court website:

Although Singapore became independent on 9 August 1965, the ties between the judicial systems of Singapore and Malaysia were not severed until 1969. The Supreme Court of Judicature Act 1969, re-established the supreme Court of Singapore, comprising the High Court, the Court of Appeal and the Court of Criminal Appeal.

Jury trials were abolished in 1969. The next important milestone for Singapore's judicial system was the introduction of judicial Commissioners to the Supreme Court Bench, with the first Judicial Commissioner being appointed on 1 July, 1986. A Judicial Commissioner is appointed for specific periods of time and may exercise the powers and perform the functions of a Judge. In this capacity, he enjoys the same immunities as a Judge.

UNAUTHORIZED ACCESS

According to section 2(2) of the Computer Misuse Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he –

1. alters or erases the program or data;
2. copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
3. uses it; or
4. causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner).

Section 3 of the computer Misuse Act punishes "unauthorized access to computer material". The essential elements or unauthorized access under this section are:

1. The act must be done with knowledge.
2. The act must cause a computer to perform any function.
3. The purpose must be to secure access to any program or data held in any company.
4. The act must be without authority.

In order to curb the terrorism, the legislation has enacted the Act known as **`Prevention of Terrorism Act,2002'**

Section 2(c) provides the proceeds of terrorism, which reads as under:

"(c) "proceeds of terrorism" shall mean all kinds of properties which have been derived or obtained from commission of any terrorist act or have been acquired through funds traceable to a terrorist, act, and shall include cash, irrespective of person in whose name such proceeds are standing or in whose possession they are founds;"

Section 2(d) defines the property which reads as under:

"(d) "property" means property and assets of every description, whether corporeal or incorporeal, moveable or immovable, tangible or intangible and deeds and instruments evidencing title to, or interest in, such property or assets and includes Bank account."

Section 2(g) defines the terrorism, which reads as under: "(g)"terrorist act" has the meaning assigned to it in sub-section (1) of Section 3, and the expression "terrorist" shall be construed accordingly."

In **Hintendra Vishnu Thakur** (1994) 4 SCC 602, the terrorist activity has been defined, which provides that the terrorist activity does not merely arise by causing disturbance of law and order or of public order. The same reads as under:

"A `terrorist' activity does not merely arise by causing disturbance of law and order or of public order. The fall out of the intended activity must be such that it travels beyond the capacity of the ordinary law enforcement agencies to tackle it under the ordinary penal law. Experience has shown us that `terrorist' is generally an attempt to acquire or maintain power or control by intimidation and causing fear and helplessness in the minds of the people at large or any section thereof and is a totally abnormal phenomenon. What distinguishes `terrorism' from other forms of violence, therefore, appears to be the deliberate and systematic use of coercive intimidation. More often than not, a hardened criminal today takes advantage of the situation and by wearing the cloak of `terrorism', aims to achieve for himself acceptability and respectability in the society because unfortunately in the States affected by militancy, a `terrorist' is projected as a hero by his group and often even by the misguided youth…"

Section 18 thereafter defines terrorist organization as under:

"18. Declaration of an organization as a terrorist organization.- (1) For the purposes of this act an organization is a terrorist organization if,

(a) it is listed in the Schedule, or

(b) it operates under the same name as an organization listed in that Schedule.

(2) The Central Government may by order, in the official Gazette,

(a) Add an organization to the Schedule;

(b) Remove an organization from that Schedule;

(c) Amend that Schedule in some other way.

(3) The Central Government may exercise its power under clause (a) of sub-section (2) in respect of an organization only if it believes that it is involved in terrorism.

(4) For the purposes of sub-section (3) an organization shall be deemed to be involved in terrorism if it

(a) Commits or participates in acts of terrorism,

(b) Prepares for terrorism,

(c) Promotes on encourages terrorism, or

(d) Is otherwise involved in terrorism."

For curbing out the terrorism, Special Courts have been formulated under the Act, which is called as a Special Courts. Sub clause (1) and (2) of Section 23 provides the formation of Special Courts. In other words, the provision for constituting the Special courts for curbing out the terrorism, role and responsibilities of intellectuals comes into play.

If we look to the history of the United Nations, the same was formed with a view to maintain the balance of power arising out of the second world war, which started in the year 1939. The term United Nations was resolved in the declaration by United Nations on January 1,1942 at the Sanfrancisco Conference. The United Nations was the formation of the steps, which has led as a result of the London Declaration Atlantic Charter, United Nations

Declaration, Mosco Declaration, Tehran Declaration, Sanfranscisco Conference and therefore, the object reads as under:

"We the people of the United Nations determined to save succeeding generations from the scourge of war, which twice in our life-time has brought untold sorrow to mankind, and to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations, large and small, and to establish conditions under which justice and respect for the obligations arising from treaties and other sources of International Law can be maintained, and to promote social progress and better standards of life in larger freedom, and for these ends to practice tolerance and live together in peace with one another as good neighbors, and to unite our strengths to maintain international peace and security, and to ensure…That armed force shall not be used, save in the common interest, and to employ international machinery for the promotion of the economic and social advancement of all peoples, have resolved to combine our efforts to accomplish these aims.

"Accordingly, our respective Governments….have agreed to the present Charter of the United Nations and do hereby establish an international organization to be known as the United Nations."

The objects are further elaborated in Article I of the Charter which says that the purposes of the United Nations are to maintain international peace and security, to develop friendly relations among nations based on the principle of equal rights and self-determination of people, to achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and to be a center for harmonizing the actions of nations in the attainment of these common ends."

The role of intellectuals in curbing terrorism also has been given a shape from other Acts also like Information Technology Act where Section 16 has been incorporated for the security measures in order to avoid terrorism. Said section is quoted below:-

16. Security procedure.- The Central Government shall, for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-

(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.

In order to curb the terrorism, apart from the intellectuals, judiciary also plays an important role, being guardian of the creation of our Constitution.

So far as Information Technology Act is concerned, Section 1(2) and Section 75 provides as under:-

1. **Short title, extent, commencement and application**.-
(1)……..

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

75. Act to apply for offence or contravention 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.

If we come to the universal declaration of human rights, 1948, it contains 29 Articles. It contains the frame of equal dignity and the rights. The form of human rights also contains in the judgment of the Apex Court in Kapila Hingdorani Vs. State of Bihar 2003 (7) AIC 18 (SC) 194, which provides that the right to food is an essential part of the human rights. It reads as under:-

Paragraph- 50: The term 'life' used in Article 21 of the Constitution of India has a wide and far-reaching concept. It includes livelihood and so many other facets thereof. `Life' as observed by Field, J.in Munn V.Illinois 11877(94)US 11311 means something more than mere animal existence and the inhibition against the deprivation of life extends to all those limits and facilities by which life is enjoyed. (See Board of Trustees of the Port of Bombay Vs. Dilipkumar Raghvendranath Nadkarni and others 1983 (1) SCC 124 and Olga Tellis and others Vs. Bombay Municipal Corporation and others 1985(3) SCC 545.

The Constitution envisages the establishment of a welfare State at the federal level as well as at the State level. In a welfare State the primary duty of the Government is to secure the welfare of the people Providing adequate medical facilities for the people is an essential part of the obligations undertaken by the Government in a welfare State.

In Kharak Singh Vs. State of U.P.AIR 1963 SC 1295, the Supreme Court acknowledged that the term "life" means something more than mere animal existence. The inhabitation against its deprivation extended to all those limbs and faculties by which the life is enjoyed. It equally prohibited the mutilation of the body by the amputation of an arm or leg, or putting out of an eye, or the destruction of any other organ by the body through which the soul

communicates with the outer world. It postulates to be free from restrictions on the enjoyment of a decent, respectable and healthy life. Right of life under Article 21 of the Constitution is a right of a person to be free from restrictions or encroachment. Where imposed directly or directly brought about by calculated measures.

National Human Rights Courts.- For the purpose of providing speedy trial offences arising out of violation of human rights, the State Government may, with the concurrence of the Chief Justice of the High Court, by notification, specify for each district a Court of Session to be a Human Rights Court to try the said offences;

Provided that nothing in this section shall apply if

(a) A court of Session is already specified as a Special Court; or
(b) A Special Court is already constituted, for such offences under any other law for the time being in force.

These are the courts, which are being shared by the Intellectuals.

Although the Human Rights courts have been established but in various States, the courts are lacking. There are no courts of Human Rights. If the courts of Human Rights are established at every place, we can pursue the wrong doers for a remedy from the Human Rights courts.

In view of the aforesaid, the nut shell is that the responsibilities of Intellectuals in order to curb the terrorism has been conferred not only on the statutory protection given by the Prevention of Terrorism Act,2002 but also by the International Law through the process of International Court of Justice and United Nations organization, National Human Rights Commission and now by the Information Technology Act which contains a special enactment for the security in order to get rid of the Terrorist Act. After the

enforcement of Information Technology Act, 2000, the entire terrorism has now shifted to the process of Internet device and for that purpose Forensic Labs have been established in Kolkata, Allahabad, Hyderabad and New Delhi. Time has come when the Government is to take steps to establish the Forensic Labs in every State in order to curb the terrorism. The time has also come where in the shape of International Court of Justice namely Human Rights Commission and International Treaty concerning Cyber law are also required to be established covering the cyber space which dealt with the cyber crimes with no geographical back ground.

Counter strike through aggressive defence

The concept of counterstrike through aggressive defence presupposes the adoption and use of information technology to produce legitimate and legalized disabling and reasonably destructive effects. Some adopted measures completely destroys the functioning of the offending computer while others simply disable the computer for the time being by either shutting it down or making it temporarily non-functional. Thus, the adopted measure to gain public support and legitimacy must be "proportionate" to the harm that could have caused had that measure not been adopted. For instance, the shutting down of the computer of the person using the malware is permissible whereas the destruction or procurement of data and information stored in such computer, having no connection and association with that malware, may not be commensurate with the protection requirements. Such destruction or procurement of data may be unlawful and perhaps exceed the limits of self-defence. Thus, technology adopted must not only be safe and effective, but it

must also be " legal and law-abiding". A countermeasure, which is not very accurate, and law abiding would be a remedy worst than the malady and hence it should be avoided. For instance, if a virus has been launched by using a public server, then by disabling that server the genuine and legitimate users will be unnecessarily harassed and they would be denied the services which they are otherwise entitled to. Thus, the countermeasure measure adopted must be job specific and not disproportionate to the injury sought to be remedied.

Indian perspective

In India there is no law, which is specifically dealing with prevention of malware through aggressive defense. Thus, the analogous provisions have to be applied in a purposive manner. The protection against malware attacks can be claimed under the following categories:

(1) Protection available under the Constitution of India, and
(2) Protection available under other statutes.

(1) Protection under the Constitution of India: The protection available under the Constitution of any country is the strongest and the safest one since it is the supreme document and all other laws derive their power and validity from it. If a law satisfies the rigorous tests of the Constitutional validity, then its applicability and validity cannot be challenge and it becomes absolutely binding. The Constitutions of India, like other Constitutions of

the world, is organic and living in nature and is capable of molding itself as per the time and requirements of the society. It is presumed that the Parliament intends the court to apply to an ongoing Act a construction that continuously updates its wordings to allow for changes since the Act was initially framed. While it remains law, it has to be treated as always speaking. This means that in its application on any day, the language of the Act though necessarily embedded in its own time, is nevertheless to be construed in accordance with the need to treat it as a current law . We cannot allow the dead hand of the past to stifle the growth of the living present. Law cannot stand still; it must change with the changing social concepts and values. If the bark that protects the tree fails to grow and expand along with the tree, it will either choke the tree or if it is a living tree it will shed that bark and grow a living bark for itself. Similarly, if the law fails to respond to the needs of changing society, then either it will stifle the growth of the society and choke its progress or if the society is vigorous enough, it will cast away the law, which stands in the way of its growth. Law must therefore constantly be on the move adapting itself to the fast-changing society and not lag behind . Thus, horizons of constitutional law are expanding and they can easily tackle the problems of cyber terrorism and the menace of malware. It must be noted that as a general rule the protection of fundamental rights is available against the might of the " State and its Instrumentalities". This, however, does not mean that the protection cannot be extended against "Private individuals" having no element and colour of Statehood. There are instances where the Supreme Court has extended the protection of fundamental rights against private individuals. For instance, a writ of Habeas Corpus can be issued, when a person complains

of illegal custody or detention of an individual by a private person . Similarly, the Supreme Court has the power to regulate private rights in public interest by legitimately exercising its powers .

In US, I have come to know that a Team has been formed known as The Communications Assistance for Law Enforcement Act (CALEA) and its purpose is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to monitor all telephone, broadband internet, and VoIP traffic in real-time.

The original reason for adopting CALEA was the FBIU's worry that increasing use of digital telephone exchange switches would make taping phones at the phone company's central office harder and slower to execute, or in some cases impossible. Since the original requirement to add CALEA-compliant interfaces required phone companies to modify or replace hardware and software in their systems, U.S.Congress included funding for a limited time period to cover such network upgrades. CALEA was passed into law on October 25,1994 and came into force on January 1,1995.

The U.S Congress passed the CALEA to aid law enforcement in its effort to conduct criminal investigations requiring wiretapping of digital telephone networks. The Act

obliges telecommunications companies to make it possible for law enforcement agencies to tap any phone conversations carried out over its networks, as well as making call details records available.

Common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service-all three types of entities are defined to be "telecommunications carriers" and must meet the requirements of CALEA.

The CALEA Implementation Unit at the FBI has clarified that intercepted information is supposed to be sent to Law Enforcement concurrently with its capture.

Technical Implementation

To be CALEA-compliant, telecommunications providers must install new hardware and software, as well as modify old equipment so it does not interfere with any law enforcement agency's ability to perform real-time surveillance of any telephone or Internet traffic. Most of this equipment and software is purchased from "Trusted Third-Parties," such as narus (e.g. NarusInsight), Pen-Link (e.g. Pen-Link 8 Software, and their LINCOLN systems & software), and other surveillance equipment/software providers.

For adjudicating of the dispute under the Information Technology Act, Section 46 was enacted which has given the power for adjudication of the crimes. The power has been given to the Secretary, Information Technology and he has power to

adjudge the quantum of compensation under Sections 46 and 47 of the Act.

Sections 46 and 47 are quoted below:

46. Power to adjudicate.-

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made hereunder the Central Government shall, subject to the provisions of Sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer or holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in Sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3)No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4)Where more than one adjudicating officer are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5)Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Sub-Section (2) of Section 58, and-

(a)All proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860)

(b)Shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974)

47. Factors to be taken into account by the adjudicating officer. -

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely-

(a)The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.

(b)The amount of loss caused to any person as a result of the default;

(c) The repetitive nature of the default.

Sections 43 and 44 of the Information Technology Act,2000 provides penalties and their Adjudication. It reads as under:

Penalties and Adjudication

43. Penalty for damage to computer to com0puter, computer system etc.- If the person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer date-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 authorized 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 hereunder;

(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.

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

66A. Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

66B. 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.

66C. 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.

66D. 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.

66E. 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.

For publishing of information which is obscene in electronic form is Section 67. Same are quoted below:-

"67. Publishing of information which is obscene in electronic form- Whoever publishes or transmits or cause to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees."

By Amended Act, Section 67A and Section 67B are added. Section 67A is quoted below:

"67A. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to tine lakhs ruppes.

For adjudicating the aforesaid crimes, the power has been given to the Adjudicating Officer.

For adjudicating of the dispute under the Information Technology Act, Section 46 was enacted which has given the power for adjudication of the crimes. The power has been given to the Secretary, Information Technology and he has power to

adjudge the quantum of compensation under Sections 46 and 47 of the Act.

ctions 43 and 44 of the Information Technology Act,2000 provides penalties and their Adjudication. It reads as under:

Penalties and Adjudication

44. Penalty for damage to computer to com0puter, computer system etc.- If the person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer date-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 authorized 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 hereunder;

(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.

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.-For the purposes of this section-

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

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

(ii) "computer data-base" means a representation of information knowledge, facts, concepts or instructions in text, image, audio, \ video that are being prepared or have been prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or 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.

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information, return, etc.- If any person who is required under this Act or any rules or regulations made thereunder to-

(i) furnish any document, return or report to the Controller of the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(j) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(k) maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.- Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty five thousand rupees to the

person affected by such contravention or a penalty not exceeding twenty five thousand rupees.

The crimes which are being adjudicated by the Adjudicating Officer have also been defined under the Information Technology Act.

For the tampering with computer source documents is Section 65.

For punishment for cyber terrorism, there is Section 66F of the IT Act,2000 which provides as under:

> 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
> (iii) introducing or causing to introduce any computer contaminant;

After the decision of the Adjudicating Officer, the appeal lies to the Appellate Tribunal under Section 48 of the Information Technology Act,2000. It reads as under:

"48.Establishment of Cyber appellate Tribunal.- (1) The Central Government shall, by notification, establishes one or more appellate tribunals to be known as the Cyber Regulation Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in Sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction."

He exercises the powers contained under Section 58 of the Information Technology Act, which reads as under:-

58. Procedure and powers of the Cyber Appellate Tribunal.-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2)The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely-

(a)Summoning and enforcing the attendance of any person and examining him on oath;

(b)Requiring the discovery and production of documents or other electronic records;

(c)Receiving evidence on affidavits;

(d) Issuing commissions for the examination of witnesses or documents;

(e) Reviewing its decisions

(f) dismissing an application for default or deciding its ex parte;

(g) any other matter which may be prescribed.

(3)Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228, and for the purposes of Section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to

be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure.

According to its preamble, the IT Act basically seeks to:

Provide legal recognition for electronic commerce.

Section 1(2) of the Information Technology Act, 2000 reads as under:-

> 1(2) "It shall extent to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

The aforesaid definition covers the offences or contravention even committed outside India by any person.

In Section 70 of the principal Act, the following sub-section are substituted, namely,

> (1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
>
> After sub-section (3), the following sub-section is inserted, namely,

(3) The Central Government shall prescribe the information security practices and procedures for such protected system.

After Section 70 of the principal Act, the following sections are inserted, namely:-

70A (1) The Central Government may, by notification published in the Official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2)The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3)The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70B. (1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2)The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.

(3)The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security;-

(4) Collection, analysis and dissemination of information on cyber incidents;
(5) Forecast and alerts of cyber security incidents;
(6) emergency measures for handling cyber security incidents;
(7) coordination of cyber incidents response activities;
(8) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
(9) such other functions relating to cyber security as may be prescribed.

For Section 77 of the principal Act, the following sections are substituted, namely.

"77. No compensation awarded, penalty imposed or confiscation made under this Act shall be prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77A. A court of competent jurisdiction may compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind;

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions

of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure,1973 shall apply.

77B. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.