CYBER TERRORISM – PREVENTION AND TRENDS: IN PERSPECTIVE OF INDIA

Paramjeet Singh[*]

Abstract:

Cyber Terrorism can be described as politically motivated attacks in cyber space. These attacks are intended to cause grave harm such as loss of life or severe economic damage. Any criminal activity that uses a computer either as an instrumentality, target or means for perpetuating further crimes comes within the ambit of cyber crime. IT Act 2000 is not very effective in dealing with several emerging cyber crimes. The paper will examine the nature of and problem created by cyber crime, along with some of the legal and policy challenges arising in relation to the development of national and international law enforcement and regulating response to cyber crime. This paper is based on various reports from news media, government official websites and also text books.

Keywords: ICT, WMO, J&K, IT Act, Syntactic, Semantics.

[*] District Informatics Associate, National Informatics Centre, MCIT, Government of India Associate Member of CSI, (Doing Certified System Security Analyst course from NIELIT, Gorakhpur)

Introduction:

Cyber crime refers to computer mediated activities which are either criminal or regarded as illicit and which can be conducted through global electronics networks. The computer age has provided organized crime with more sophisticated and potentially secure techniques for supporting and developing networks for a range of criminal activities, including drug trafficking, money laundering, illegal arms trafficking, and smuggling. Cyber Crime poses new challenges for criminal justice, criminal law and law enforcement. Much of the information we have on cyber crime losses in derived from government sites & offices. Cyber Terrorism is a now rising national security issue facing India. The war on terrorism is sure to result in cyber attacks against us assets launched by terrorist groups, nations states that provide support for terrorists, and hackers who sympathize with terrorists.

Cyber terrorism can also be define much more generally as “The premeditated use of descriptive activities”, or the treats thereof , against computer and/or networks, with the intention to cause harms or further social , ideological , religious, political or similar objective. Through these attacks occurs in cyberspace, they still exhibit to four elements common to all acts of terrorism.

- Conducted by ad hoc agents as opposed to national armies.
- Political and designed to impact political structures.
- Premeditated and not simply acts born of rage.
- Targeted at civilians and civilians installations.

Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff.
By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social.

Effects of Cyber Terrorism: Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

1. Cyber terrorism can have serious large-scale influences on significant numbers of people. It can weaken countries economy greatly, thereby stripping it of its resources and making it more vulnerable to military attacks.
2. Cyber terror can also affect internet-based business, E-governance and E-commerce.
3. Cyber terrorism can also bring about religious differences and disharmony between different communal groups.
4. MNC (Multi-national corporations) can face threats from terrorist and others, to their security and safety.

Taxonomy of Cyber Attacks:

Gally (1996) discusses three types of attacks against computer systems-

1. Physical

2. Syntactic
3. Semantics

Physical attacks use conventional weapons, such as bombs or fire. A syntactic attacks uses virus types software to disrupt or damage a computer system or networks. A semantic attack is a more subtle approach. Its goal is to attack user's confidence by causing a computer system to produce errors and unpredictable results.

Analysts warn that terrorist acts will now include more sophisticated forms of destructions and extortion such as disabling or penetrating vital commercial computers systems. Terrorists are likely to make increasing use of non weapon technologies for destructive ends. Technological advances in ICT help them to give another meaning to the acronyms WMD – Weapons of Mass Disruption, not necessarily of mass destructions.

Computer based attacks in world:

➢ India & Pakistan dispute on Kashmir moved into cyberspace when pro-Pakistan hackers began repeatedly attacking computers in India. The number of attacks has grown yearly (vatis 2002). Some Indian hackers also attacks on Pakistani sites.

➢ The Israel-Palestine conflict saw its first cyber attacks in October 2000 when some Israeli teenagers launched DOS attacks against computer maintained by the Palestinian Organizations Hezbollah and Hamas (Kratt, 2000).

➢ When planes from the North-Atlantic Treaty Organization (NATO) bombed targets in Kosovo, the NATO computers suffered sustained attacks (Nuttall, 1999).

➢ The mid-air collision of an American surveillance plane and a chines fighter aircraft in 2001 engendered a political and diplomatic dispute between two countries. The political conflict was accompanied by an online campaign of cyber attacks carried out by both sides, with hackers around the globe joining in (Mc Wethy & Starr, 2001; vatis, 2002).

Types of Cyber Crime: There are a good number of cyber crime variants. A few varieties are discussed for the purpose of completion. This paper is not intended to expose all the variants.

➢ Cyber terrorism
➢ Hacking
➢ Theft of telecommunications
➢ Industrial Espionage
➢ Telecommunication Piracy
➢ Dissemination of offensive Materials
➢ Unauthorized Access to systems
➢ Virus/ Worms/ Trojans Attacks
➢ E mail Spoofing / spamming / bombing
➢ Electronic vandalism
➢ Credit Card/ EFT Frauds
➢ IPR Violations

Controlling Digital Crime: Legislation, Law Enforcement, Investigation & Information security.

General Cyber Act in India

○ Indian Telegraphy Act, 1933

- Indian wireless Act 1933
- Semiconductor Integrated Circuits is layout Design Act 2000
- Information Technology Act 2000
- Telecom Regulating Authority of India Act, 2000

Cyber Law

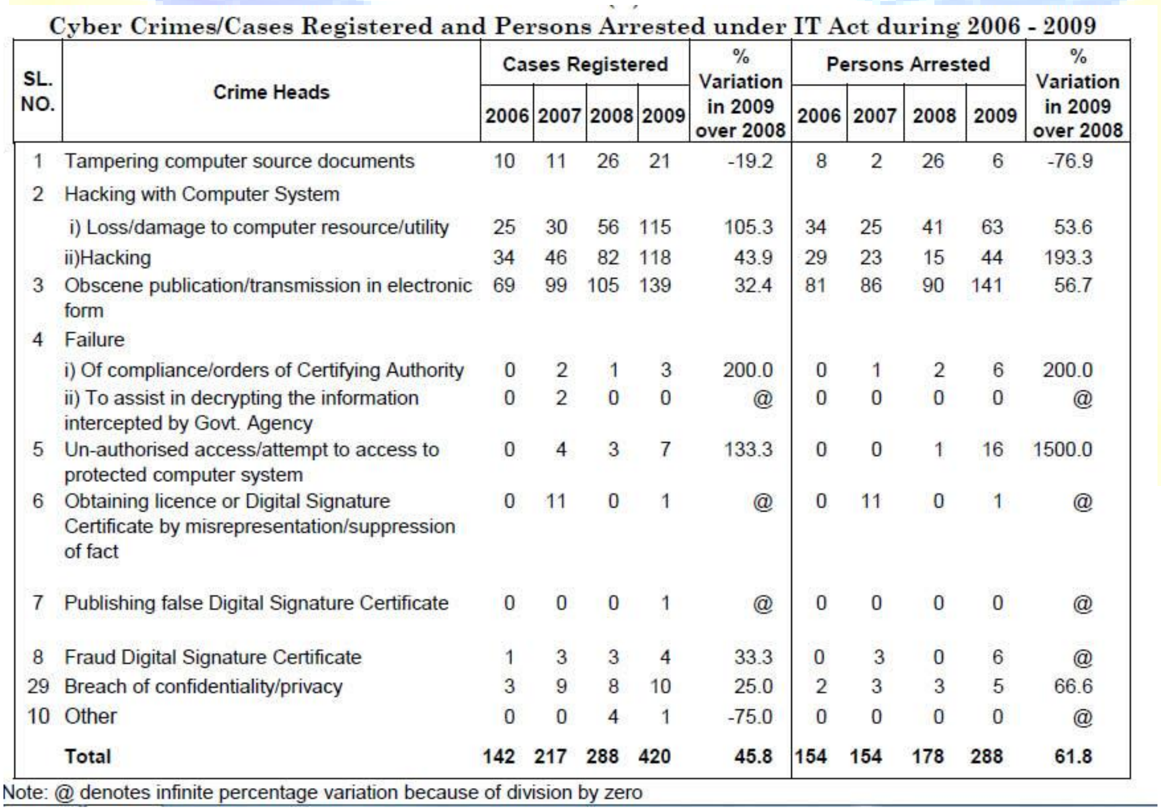
Cyber law is a generic term which refers to all the legal and regulating aspects of internet and the World Wide Web. Anything concerned with or related to any legal aspects or issues concerning any activity of netizens and others, in cyberspace come within the circle of cyber law.

Why Cyber law in India?

The major cyber crimes reported, in India, are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

Here we are showing statistics on Cyber Crimes are collected under the following heads:
i) Offences registered under the Information Technology Act 2000. (Table 1 & Image 1)
ii) Offences under the IPC (with use of Computers) (Table 2 and Image 2)

(Data collected by National Crime Records Bureau, India)



Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2006 - 2009

SL. NO.	Crime Heads	Cases Registered				% Variation in 2009 over 2008	Persons Arrested				% Variation in 2009 over 2008
		2006	2007	2008	2009		2006	2007	2008	2009	
1	Tampering computer source documents	10	11	26	21	-19.2	8	2	26	6	-76.9
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	25	30	56	115	105.3	34	25	41	63	53.6
	ii)Hacking	34	46	82	118	43.9	29	23	15	44	193.3
3	Obscene publication/transmission in electronic form	69	99	105	139	32.4	81	86	90	141	56.7
4	Failure										
	i) Of compliance/orders of Certifying Authority	0	2	1	3	200.0	0	1	2	6	200.0
	ii) To assist in decrypting the information intercepted by Govt. Agency	0	2	0	0	@	0	0	0	0	@
5	Un-authorised access/attempt to access to protected computer system	0	4	3	7	133.3	0	0	1	16	1500.0
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	0	11	0	1	@	0	11	0	1	@
7	Publishing false Digital Signature Certificate	0	0	0	1	@	0	0	0	0	@
8	Fraud Digital Signature Certificate	1	3	3	4	33.3	0	3	0	6	@
29	Breach of confidentiality/privacy	3	9	8	10	25.0	2	3	3	5	66.6
10	Other	0	0	4	1	-75.0	0	0	0	0	@
	Total	**142**	**217**	**288**	**420**	**45.8**	**154**	**154**	**178**	**288**	**61.8**

Note: @ denotes infinite percentage variation because of division by zero

Table 1

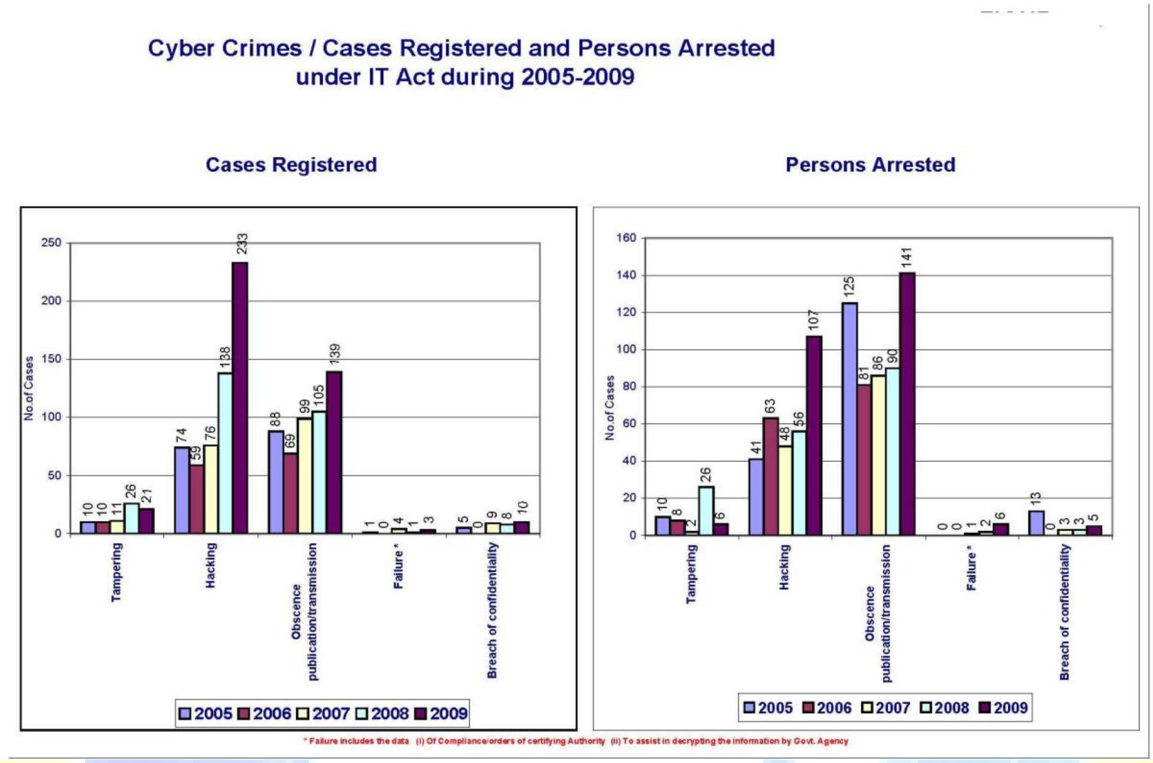
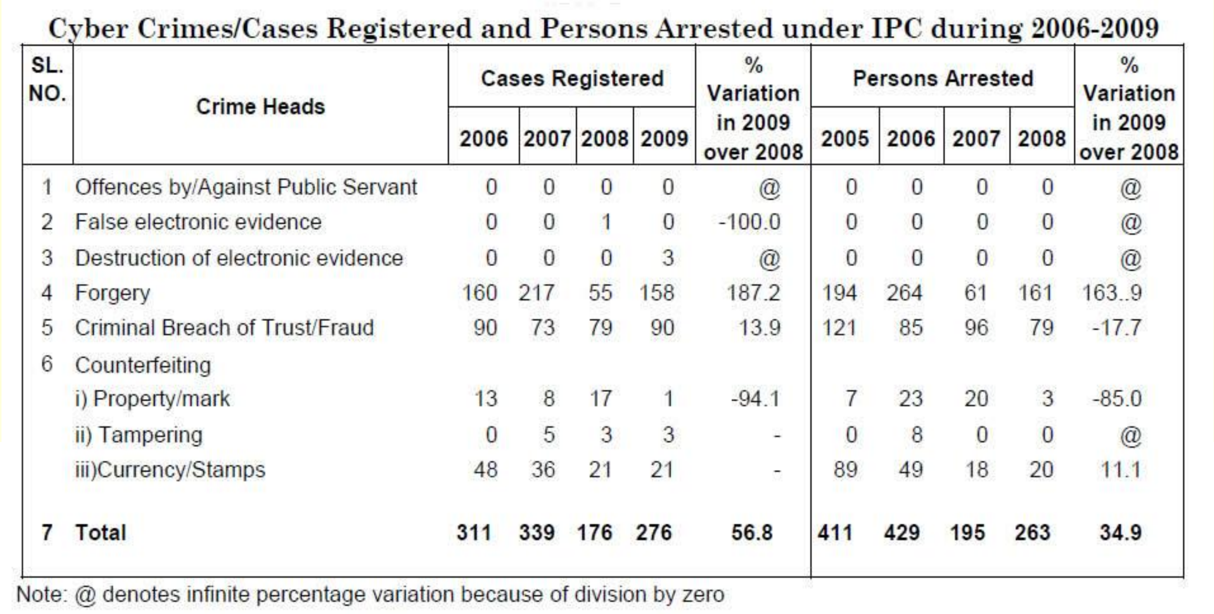


Image 1



Cyber Crimes/Cases Registered and Persons Arrested under IPC during 2006-2009

SL. NO.	Crime Heads	Cases Registered				% Variation in 2009 over 2008	Persons Arrested				% Variation in 2009 over 2008
		2006	2007	2008	2009		2005	2006	2007	2008	
1	Offences by/Against Public Servant	0	0	0	0	@	0	0	0	0	@
2	False electronic evidence	0	0	1	0	-100.0	0	0	0	0	@
3	Destruction of electronic evidence	0	0	0	3	@	0	0	0	0	@
4	Forgery	160	217	55	158	187.2	194	264	61	161	163..9
5	Criminal Breach of Trust/Fraud	90	73	79	90	13.9	121	85	96	79	-17.7
6	Counterfeiting										
	i) Property/mark	13	8	17	1	-94.1	7	23	20	3	-85.0
	ii) Tampering	0	5	3	3	-	0	8	0	0	@
	iii)Currency/Stamps	48	36	21	21	-	89	49	18	20	11.1
7	**Total**	**311**	**339**	**176**	**276**	**56.8**	**411**	**429**	**195**	**263**	**34.9**

Note: @ denotes infinite percentage variation because of division by zero

Table 2

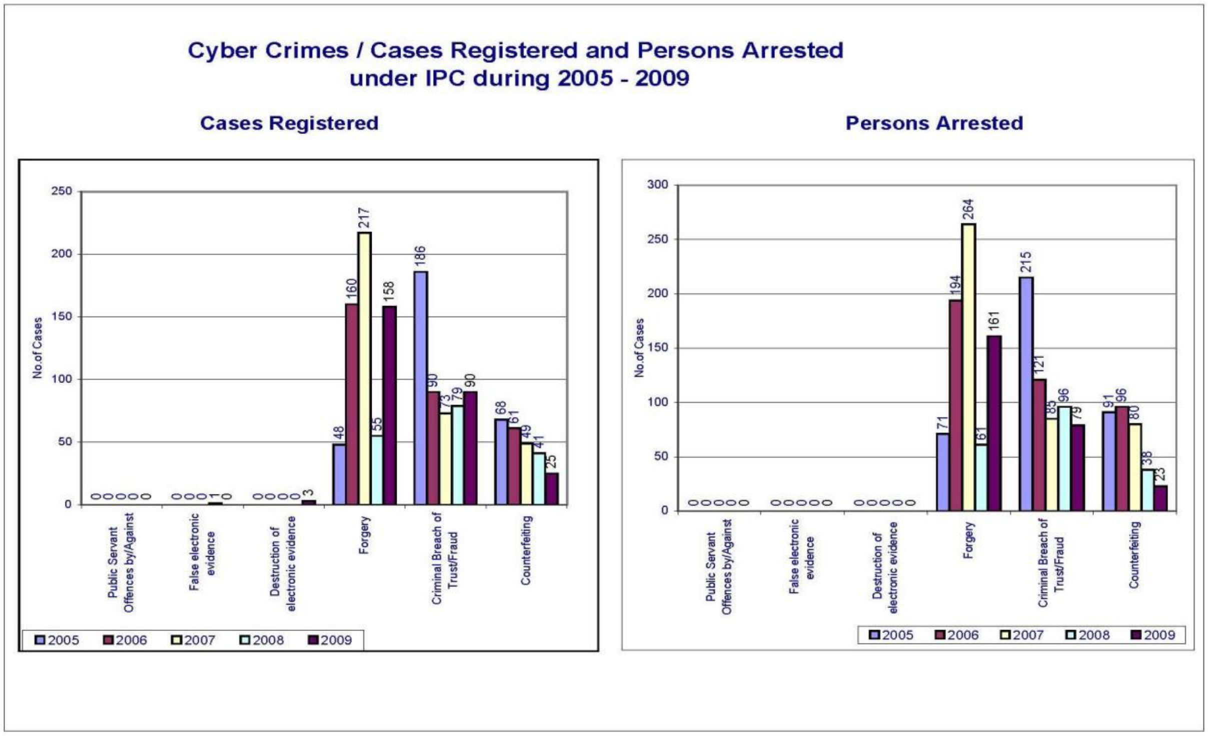


Image 2

So there should be Cyber Law in India.

1. Existing laws in India were enacted keeping in view the relevant political, social, economic and cultural scenarios of that time.
2. The coming of internet led to the emergence of numerous ticklish legal issues and problems, which necessitated the enactment of cyber laws.
3. The existing Laws of India could not be interpreted in the light of the emerging cyber space to include all activities of cyber space.
4. None of the existing laws gave any legal validity or sanction to the activities in cyber space.
5. Internet requires an enabling and supported Legal infrastructure in tune with the times.

IT Act 2008

It act 2000 now known as amended it act 2008 by information technology amendment bill 2006 passed by Loksabha & Rajaysabha in 2008 presidential assent given on 5 February 2009 and notified with effect October 27, 2009.

Applicability of law to the whole of India included J&K

Section 75 of the act states that the provision of the act shall apply to any offences or contravention committed anywhere in the world irrespective of is nationality if the act or conduct constitute the offence or contravention involves a computer, computer system, computer network located in India

Positive aspects of Act

1- Email is now a valid and legal form of communication in our country
2- cyber law provides legal infrastructure to regulate to commercial transaction
3- digital signatures have been given legal validity
4- E governance in now possible with a legal framework
5- corporate can keep and retain valuable and corporate in formation
6- Enhance security
7- punishment for breaking in to computers
8- Cyber crime are punishable hence it controls the activities of perpetrator of cyber crime

Weaknesses in Act

1- The act does not deal with privacy and data protection issue on the internet
2- The Act fails to cover cyber laundering of money spamming, phishing cyber staking cyber squatting and other innovative cyber crimes.
3- The Act does not clarify the situation regarding the liability of network service providers.
4- The Act does not address the issue of protection of intellectual property on the internet
5- The Act fails to address the issue of cross border taxation that may arise in international contracts
6- The jurisdiction of a particular country over online transactions which involves more than are jurisdiction has been left open. This can lead to a conflict of jurisdictions.

Investigations

Investigations are required to maintenance data of the computer to check out what exactly happened to the computer and who is responsible for it. We have to enforce computer forensic in India to control cyber crime. **Computer forensic** is a branch of forensic science relating to legal evidence found in computers and digital storage mediums. It deals with broader concepts which is relating to crimes happening in computers. The primary goal of computer forensic is to explain the current state of digital artifact which includes computers systems, a storage medium, an electronic document or a sequence of packets moving on a network.

Information security

Information security means protecting information and information infrastructure assets against the risks of loss, misuse from unauthorized access, disclosure, disruption, modification, perusal, inspection, theft, recording or destruction.

Information security is not something you buy, it is something you do.

Benefits Information security

✓ Protects information from arrange of threats ,
✓ minimize financial loss
✓ Optimizes return investments
✓ Increases business opportunities
✓ Ensure business controls

Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information and information assets and deciding what measures should be taken in reducing risk to an acceptable level to strengthen information security we have to follow ISO/ IEC 27001- ISMS(Information Security Management System) recommendation. The ISMS in designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Initiatives in India

India has established many cyber crime cells in many cities to control crime rate.

- ✓ Cyber Crime Investigation Cell of Mumbai Police
- ✓ Cyber Crime cell Chennai
- ✓ Cyber Crime Police Station, Banglore
- ✓ Crime Investigation Department, Hydrabad
- ✓ Cyber Crime and Technical Investigation Cell, Gurgaon
- ✓ Cyber Crime Police Station, SAS Nagar, Patiala.

Conclusion

This research argues that cyber terrorism in a critical issue for the computer industry and society in general. Cyber terrorism covering the threat of viruses' hackers and miscellaneous security breaches, regardless of whether or not they actually originated from terrorists. There for it is very important that IT faculty develop ways to teach their students in collages and all employees should be trained on the need for physical an IT security in NGO, commercial organization and in also government sector. It is a well-known fact that terrorists have been using the Internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have the capability to paralyze large parts of communication networks, cause financial meltdown and unrest. The degree of our preparedness in the face of all these potential threats, does leaves much to be desired. The Government should also take note of this slow but worrying development and put in place a proper mechanism to curb the misuse. Foster a culture of safety & security this makes information security an indispensable part of all operation a cross different domains all around world.

"Failure is not when you fall down, but when you fail to get up."

References:

National Crime Records Bureau, India

Siegel, D., van de Bunt, H. and D. Zaitch (2003). *Global Organized Crime: Trends and Developments*, London: Kluwer Academic Publishers.

Laqueur, W. (1999). *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, New York: Oxford University Press.

Abrams, N. (2005). *Anti-Terrorism and Criminal Enforcement, Second Edition*, St. Paul, MN: Thomson/West Publishing.

"The Next War Zone: Confronting the Global Threat of Cyberterrorism" by James F. Dunnigan, Osborne/McGraw-Hill; 2002, ISBN: 0806524138.

"Black Ice: The Invisible Threat of Cyber-Terrorism" by Dan Verton, McGraw-Hill Osborne Media; 1st edition 2003, ISBN: 0072227877.

Chandigarh Tribune

The Hindu