Humanities & Social Sciences Reviews
Vol 2 (1), December 2014, pg 94-101

CYBER CRIMES: A THREAT TO HUMANITY

Dr. Shrish Kumar Tiwari
Assistant Professor, Allahabad Degree College,
A Constituent College of University of Allahabad, Allahabad.
Email: shrish.tiwari@gmail.com

Abstract

Good and bad has co-existence since the beginning of the world. Where first one comprises all things which are essential for wellbeing of all whereas other ones connotes negativity. Unfortunately technology cannot be mention as an exception of this rule. The internet and its technologies has opened up many opportunities for all countries to develop their economies. On one hand our scientist, technocrats are using this advanced stream of science for betterment of all and to make India self-dependent and secure from attack of our enemies while on the other hand a very well structured groups (Independent or Nation sponsored) are also using these technologies as a tool to make INDIA weak and helpless. Cyber criminals perform various acts like cyber stalking, on-line harassment, on-line defamation, hacking, and so forth collectively we call it cybercrime. When these activities are managed by organized group systematically and deliberately we term it as CYBER TERRORISM.

Cyber terrorism is a well-planned and organized use of technologies by cyber experts resides inside and outside the country for anti-national activities. Although our government is well capable to fight against such challenges it requires support, awareness and alertness from people.

This paper highlights some of the basics of cyber terrorism. This paper further discusses about the threats of cyber terrorism and the present status of various cybercrimes in India. This paper aims at creating awareness on cybercrime and suggests check on cybercrime.

Key Words: Cyber Terrorism, Hacking, Information Technology

INTRODUCTION

In present era of fierce competition every country is struggling to secure its future. Technology is a mighty tool which helps in cost efficiency and excellence, which are require to be enriched and profitable, with its web based approach. Almost whole world is adopting this new form of information science for the development of their people and launching various programme based on information and communication technology, termed, e-governance and this programme are witnessing that these projects are improving the efficiency of government by maintaining transparency, accessibility and quick responsiveness. Although it is the brighter or positive sides of Information and Communication Technology .There are some bad elements in the society who doesn't, want peace, harmony and constructive environment in country. Therefore they are using all possible tools, methods, for their malafied intentions and technology is no exception to it.

Various terrorist groups are adopting ICT as a tool to disrupt law and order of a country. Cyber terrorism is an organized criminal activity committed by one person or group of persons to disturb a genuine transaction.

This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terrorist threats made via electronic communication.

OBJECTIVES:

The paper contains following objectives:

1. To understand and analyze the status and types of cybercrime in India;

2. To find out the major reasons behind the increasing rate of cybercrime in India;

3. To provide suggestions to check the cybercrimes in India.

METHODOLOGY:

The paper is descriptive in nature. With the help of secondary data which are available as free source. Paper efforts to describe the form and status of cybercrime and analyses the complexity of cybercrime in modern age.

Forms of Cyber terrorism- Ghosts has so many faces

We can divide these activities as follows-

1. Crime against a Person;
2. Crime against a Nation.

Any criminal activity (committed through computer or network system or over computer or network system) in which Technology is used can be understood as cyber terrorism.

1. Offense against individual

"*Man is born free but that was his last moment to enjoy that one*".

Every person reside in a society is bound to certain laws, conventions, rules which protect any individual to disturb law and order of the society. At the same time these laws provide certain rights to that individual to protect him.

Constitution of India provides Right to privacy to any individual. Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. With the advent of information technology the traditional concept of right to privacy has taken new dimensions, which require a different legal viewpoint. With the passage of time cybercrimes has become much complicated and challenging.

Present status of computer-generated crime in India:

The Nation Crime Records Bureau (NCRB), Ministry of Home Affairs has released Cyber Crime Statistics for the 2013 year, which again shows rapid increase in cybercrime by 50% on year to year basis from 2012 to 2013. The statistics mainly show cases Registered under Cyber Crimes by Motives and Suspects (States & UTs): The maximum offenders came from the 18-30 age group. Among states, the highest incidents of cybercrime took place in Maharashtra (907) followed by Uttar Pradesh (682) and Andhra Pradesh (651).

The maximum cybercrime arrests of four hundred twenty six (426) under the IT Act took place in Maharashtra and Andhra Pradesh was a distant second with 296 arrests, followed by Uttar Pradesh with 283 arrests.

In percentage terms, the state that saw the most dramatic increase in cases registered under the IT Act was Uttarakhand at 475% (from 4 cases to 23); Assam a close second with 450% (from 28 cases to 154). Interestingly, the picture postcard union territory, Andaman and Nicobar islands, registered an eye-popping increase of 800% (two cases in 2012 to 18 in 2013) in the same category.

The Delhi city has registered 131 cases of cybercrime cases which is an increase of 72.4 percent as compared to last year 2012. Whereas Lakshadweep, Dadar and Nagar Haveli reported no cybercrime cases for the year 2013. Also Cyber Crime activities seem to rare in the northeastern states. In 2013, only one case each was registered in Nagaland and Mizoram.

The following data are well enough to describe cybercrime status in India:

TABLE-1.1

Incidence Of Cases Registered Under Cyber Crimes in States/UTs During 2012 & 2013 and Percentage Variation

Sl.No.	State/UT	IT ACT			IPC Section		
		2012	2013	% Variation	2012	2013	% Variation
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
STATES:							
1	ANDHRA PRADESH	429	635	48.0	25	16	-36.0
2	ARUNACHAL PRADESH	12	10	-16.7	0	0	@
3	ASSAM	28	154	450.0	0	0	@
4	BIHAR	23	23	0.0	7	116	1557.1
5	CHHATTISGARH	49	91	85.7	10	10	0.0
6	GOA	30	57	90.0	2	1	-50.0
7	GUJARAT	68	61	-10.3	10	16	60.0

8	HARYANA	66	112	69.7	116	211	81.9
9	HIMACHAL PRADESH	20	24	20.0	0	4	@
10	JAMMU & KASHMIR	35	46	31.4	0	0	@
11	JHARKHAND	10	13	30.0	25	13	-48.0
12	KARNATAKA	412	513	24.5	25	20	-20.0
13	KERALA	269	349	29.7	43	34	-20.9
14	MADHYA PRADESH	142	282	98.6	55	60	9.1
15	MAHARASHTRA	471	681	44.6	90	226	151.1
16	MANIPUR	0	1	@	0	0	@
17	MEGHALAYA	6	17	183.3	0	0	@
18	MIZORAM	0	0	@	0	0	@
19	NAGALAND	0	0	@	0	0	@
20	ODISHA	14	65	364.3	13	39	200.0
21	PUNJAB	72	146	102.8	6	10	66.7
22	RAJASTHAN	147	239	62.6	7	58	728.6
23	SIKKIM	0	0	@	0	0	@
24	TAMIL NADU	39	54	38.5	2	36	1700.0
25	TRIPURA	14	14	0.0	0	0	@
26	UTTAR PRADESH	205	372	81.5	44	310	604.5
27	UTTARAKHAND	4	23	475.0	0	4	@
28	WEST BENGAL	196	210	7.1	113	132	16.8
	TOTAL (STATES)	2761	4192	51.8	593	1316	121.9
UNION TERRITORIES :							
29	A & N ISLANDS	2	18	800.0	0	0	@
30	CHANDIGARH	33	9	-72.7	0	2	@
31	D & N HAVELI	0	0	@	0	0	@
32	DAMAN & DIU	0	1	@	0	0	@
33	DELHI	76	131	72.4	8	19	137.5
34	LAKSHADWEEP	0	0	@	0	0	@
35	PUDUCHERRY	4	5	25.0	0	0	@
	TOTAL (UTS)	115	164	42.6	8	21	162.5
	TOTAL (ALL INDIA)	2876	4356	51.5	601	1337	122.5

Note: @ indicates infinite percentage variation because of division by zeros

TABLE-1.1 (Concluded)

SL.No	State/UT	IT ACT			IPC Section		
		2012	2013	% Variation	2012	2013	% Variation
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
36	AGRA	22	30	36.4	4	3	-25.0
37	AHMEDABAD	25	24	-4.0	0	0	@
38	ALLAHABAD	4	17	325.0	6	26	333.3
39	AMRITSAR	15	13	-13.3	0	0	@
40	ASANSOL	16	25	56.3	0	52	@
41	AURANGABAD	31	47	51.6	0	0	@
42	BENGALURU	342	399	16.7	7	18	157.1

43	BHOPAL	1	19	1800.0	0	1	@
44	CHANDIGARH CITY	33	9	-72.7	0	2	@
45	CHENNAI	15	5	-66.7	0	8	@
46	COIMBATORE	3	3	0.0	1	3	200.0
47	DELHI (CITY)	73	131	79.5	7	19	171.4
48	DHANBAD	0	2	@	0	0	@
49	DURG- BHILAINAGAR	6	10	66.7	0	0	@
50	FARIDABAD	15	12	-20.0	0	0	@
51	GHAZIABAD	9	17	88.9	0	0	@
52	GWALIOR	7	6	-14.3	1	0	-100.0
53	HYDERABAD	42	159	278.6	0	1	@
54	INDORE	5	28	460.0	8	0	-100.0
55	JABALPUR	5	1	-80.0	3	1	-66.7
56	JAIPUR	69	110	59.4	5	21	320.0
57	JAMSHEDPUR	0	4	@	0	4	@
58	JODHPUR	25	78	212.0	0	0	@
59	KANNUR	7	8	14.3	2	0	-100.0
60	KANPUR	6	4	-33.3	1	4	300.0
61	KOCHI	45	26	-42.2	20	11	-45.0
62	KOLKATA	68	84	23.5	0	12	@
63	KOLLAM	20	10	-50.0	0	9	@
64	KOTA	1	5	400.0	0	0	@
65	KOZHIKODE	8	13	62.5	1	1	0.0
66	LUCKNOW	23	37	60.9	3	72	2300.0
67	LUDHIANA	7	32	357.1	1	0	-100.0
68	MADURAI	14	10	-28.6	0	3	@
69	MALAPPURAM	5	6	20.0	0	0	@
70	MEERUT	6	19	216.7	0	2	@
71	MUMBAI	33	40	21.2	72	92	27.8
72	NAGPUR	24	23	-4.2	0	0	@
73	NASIK	11	18	63.6	2	2	0.0
74	PATNA	21	10	-52.4	7	10	42.9
75	PUNE	76	97	27.6	32	3	-90.6
76	RAIPUR	16	58	262.5	0	0	@
77	RAJKOT	3	1	-66.7	0	1	@
78	RANCHI	0	3	@	0	8	@
79	SRINAGAR	24	20	-16.7	0	0	@
80	SURAT	8	3	-62.5	0	1	@
81	THIRISSUR	10	28	180.0	0	0	@
82	THIRUVANANTHAPURAM	15	25	66.7	1	1	0.0
83	TIRUCHIRAPPALLI	6	3	-50.0	0	0	@
84	VADODARA	14	13	-7.1	0	0	@
85	VARANASI	0	4	@	0	3	@
86	VASAI VIRAR CITY	2	10	400.0	1	0	-100.0
87	VIJAYAWADA	7	16	128.6	0	0	@
88	VISHAKHAPATNAM	153	173	13.1	1	2	100.0
	Total (Cities)	**1396**	**1948**	**39.5**	**186**	**396**	**112.9**

Note : @ denotes infinite percentage variation because of division by zeros.

TABLE – 2.1

Incidence Of Cases Registered And Number Of Persons Arrested Under Cyber Crimes

(IT Act + IPC Sections) During 2013All-India)

Sl. No	Crime Head	Cases Registered	Persons Arrested
(1)	(2)	(3)	(4)
	A. Offences under IT Act		
1	Tampering computer source documents	137	59
2	Hacking with Computer Systems		
	i) Loss/damage to computer resource/utility	1966	818
	ii) Hacking	550	193
3	Obscene publication/transmission in electronic form	1203	737
4	Failure		
	i) Of compliance/orders of certifying Authority	13	3
	ii) To assist in decrypting the information intercepted by Govt. Agency	6	7
5	Un-authorised access/attempt to access of protected Computer system	27	17
6	Obtaining License or Digital Signature Certificate by misrepresentation/suppression of fact	12	14
7	Publishing false digital Signature Certificate	4	8
8	Fraud Digital Signature Certificate	71	51
9	Breach of confidentiality/privacy	93	30
10	Other	274	161
12	**Total (A)**	**4356**	**2098**
	B. Offences under IPC		
1	Offences by/Against Public Servant	1	2
2	False electronic evidence	6	7
3	Destruction of electronic evidence	6	4
4	Forgery	747	626
5	Criminal Breach of Trust/Fraud	518	471
6	Counterfeiting		
	i) Property/mark	10	34

	ii) Tampering		8	10
	iii)Currency/Stamps		41	49
7	**Total(B)**		**1337**	**1203**
	Grand Total (A+B)		**5693**	**3301**

Above data are for the year 2013 by which we can understand the seriousness of cybercrime. To meet this challenge recourse of Information Technology Act, 2000 can be taken the various provisions of the Act suitably protect the online privacy rights of the netizens. Certain acts have been categorized as offences and contraventions, which have tendency to intrude with the privacy rights of the netizens. These rights are available against private individuals as well as against cyber terrorists. Section 1 (2) read with Section 75 of the Act provides for an extra-territorial application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of computer, computer system or computer network located in India, he would be liable under the provisions of the Act. This makes it clear that the long arm jurisdiction is equally available against a cyber-terrorist, whose act has resulted in the damage of the property, whether tangible or intangible.

2. **Information protection and records stealing-**

The information technology can be misused to get government secrets and data of private individuals and the Government and its agencies which are sensitive and important in nature. Government owned network usually contains valuable information concerning defense, nuclear and other departments which the Government will not wish to share otherwise. The same can be targeted by the terrorists to facilitate their activities, including destruction of property. It must be noted that the definition of property is not restricted to moveable or immovable alone.

Thus, if any 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 data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c. Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programme residing in such computer, computer system or computer network;

She/he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. The expression "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network The expression "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means. These provisions make it clear that secret information appropriation and data theft by the cyber terrorists will be dealt with punitive sting and monetary impositions.

2. Crime against Nation

Any individual is a basic element of nation .Thus any crime against any individuals is serious concern for any government as for maintaining law and order is concern but there are various other vurnibilities which can be named by crime against Nation which are as follows:

A- **Challenges before administration**

E-governance is replacing traditional governance in almost each country .India is also adopting e-governance in form of e-administration.

The aim of e-governance is to make the interaction of the citizens with the government offices (G to P) easy to share information with transparency and reliability . In a democracy, people govern themselves and they cannot govern themselves properly unless they are aware of social, political, economic and other issues confronting them. It is noticeable that the immediate goal of all cyber terrorist activities is to collapse a sound communication system, which includes an e-governance base. Thus, by a combination of virus attacks and hacking techniques, the e-

governance base of the government can be caused to be collapsed. This would be more deleterious and disastrous as compared to other tangible damages, which were caused by the traditional terrorist activities. Similarly, the terrorists to the common detriment of the nation at large can illegally obtain information legitimately protected from public scrutiny by the government in the interest of security of the nation. Thus, a strong e-governance base with the latest security methods and systems is the need of the hour.

B. **Denial of services attack:**

Availability of system when require is the core of any sound and robust network system. This has much importance in case of network related to government's organizations' because it contains matter data related to interest of Nation and any breach of any information's resides in these system might be harm full for whole country. So there must be robust & secure information security measures in network availed by government for communication and networking. In India, reason online security experts, the apathy towards strengthening online security stems from the fact that the maximum attacks we have seen are defacing a site or largely sending denial of services.

C. **Network Damage and Disruptions**:

The main aim of cyber terrorist activities is to cause networks damage and their disruptions. This activity may divert the attention of the security agencies for the time being thus giving the terrorists extra time and makes their task comparatively easier. This process may involve a combination of computer tampering, virus attacks, hacking .According to Indian Computer Emergency Response Team around 6000 Indian websites were defaced in 2009.

FINDINGS:

1. Lack of co-ordination among various concerning agencies.
2. Lack of proper and adequate training among police and administration department personals.
3. Lack of farsighted approach among policy formulators.
4. out dated and non-technical approach to deal with cybercrime.
5. Lack of special enforcement force.
6. Lack of e-court and cyber police stations at different parts of country.
7. Lack of awareness among people regarding cybercrime and cyber ethics.
8. Unprofessional and lethargic approach of concerning departments.

SUGGESTIONS:

Although it's very big challenge before government to fight with hidden war in form of cyber terrorism because some time these activities may be organized and planned by enemy country/s rather than an individual or any small group but by using following precautions we can minimize the possibilities to commit these crime-

- Necessary steps must be taken to enable concerning bodies.
- Computer security and awareness training
- Continuing awareness and education regarding terrorist trends and methodologies
- Future readiness to defend against attacks
- Establishment of special court, e-court, in which complain can register on-line and on the date of hearing video conferencing should be used to avoid physical presence.
- Sensitive information should not be stored in the computer systems which are connected to the internet.
- Background of outsourcing agencies should be check prior to outsource any assignment, task to maintain information security inform of authenticity, confidentiality and authenticity of data.
- Special training programme for judicial officers to deal with cases related to cybercrimes.
- Effective use of intelligence gathered from all sources
- Ministries and departments have been advised to update IT systems and carry out regular audits to ensure an error-free system.
- There must be a specific police force to deal with cybercrimes in the country.
- Separate laws for each of the classification of cybercrime instead of amending the Information Technology Act.
- Creation of special enforcement agencies to deal exclusively with cyber laws.
- Government should impose a ban on websites that exclusively display pornography and hate speeches
- Continued enhancement of resources which are essential to make Network mush secure and robust
- Public/Private interaction to get mixes approach of advanced technology and expert implementation mechanism

- Organizations possessing critical information must implement information security management practices based on ISO 27001.
- Cyber ethics should be including as a subject in various curriculum at school and college level.
- Establishment of e-cops in those city which contains economic importance
- Promotion of Research and Development in the field of information security
- A techno-legal panel for provide training to various concerning departments.
- Last but not the least creation of awareness among each and every part of administration and society.

CONCLUSION:

Cyber terrorism is not a movement or just attack but a war. Well planned, well designed and organized war which is more harmful than traditional attack. Hackers attack with bots, viruses and Trojans instead of planes or armored vehicles and missiles and systematically create on-line "trapdoors" to invade servers and computers and steel passwords of high importance .So there must be long-term strategy to fight with this new and advance form of terrorism .Integrated approach is require for this in which cooperation of our Political bodies, Judiciaries, Administration, and above of all common people is inevitable.

REFERENCES:

1. http://www.cyberlawtimes.com/cyber-crime-statistics-india-2013-2014
2. http://www.crime-research.org/library/Cyber-terrorism.htm
3. http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx (Dec 5,2013)
4. http://www.digitalattackmap.com/understanding-ddos/
5. http://cybercrime.org.za/data-theft/
6. http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf
7. http://ibnlive.in.com/news/cyber-crimes-up-by-51-per-cent-in-india-maharashtra-ap-karnataka-top-list/482969-3.html
8. Chip Magazine. 'Special Edition'. Mumbai
9. http://www.acronymfinder.com/Association-of-Public-Internet-Access-Provider-%28India%29-%28APIAP%29.html
10. Official Website of NASSCOM
11. Cyber Crime Cell, Mumbai PHISHING.mht
12. file:///C:/Documents%20and%20Settings/sai/Local%20Settings/Temp/Temporary%20Directory%201%20for%20cyberterrorism.zip/CYBER%20TERRORISM%20AND%20ITS%20SOLUTIONS%20AN%20INDIAN%20PERSPECTIVE.htm
13. *https://secure.infragard-ct.org/.../harold_hendershot_02092003*
14. www.cert.org
15. **Kumar Abhay**, Information Security Policy & Regulation Issues
16. **Sharma K.K.**, Responsive Administration of the criminal justice system in India, special number on Towards Good Governance: initiatives in India, Prentice- hall of India, New Delhi
18. **Sharma Vakul**, E-governanace & Information Technology Act ,2000(book name is Information Technology Law and Practice cyber law & e-commerce) Universal law publishing Co. Pvt. Ltd.
21. *www.allvoices.com/...india...check-cyber-terrorism/stories - United States*
22. "INDIA NOT READY FOR CYBERWAR" Business Standard (Lucknow edition) February 4th, 2010, pg.11.
23. " Moiley for special law to tackle cybercrimes" business standard (lucknow edition) February 1st,2010,pg.6