Major Initiatives for Prevention and Mitigation of Cyber Crime in India: An Over View

Gulshan Rai and B Vasanta

Abstract—**The emergent information society is predicated on a sound platform of information and communications technology and especially anchored on the critical role of the Internet both as a tool and as a platform for delivering various e-services such as e-commerce, e-banking and e-governance amongst many others. With an increasing usage of Internet, and Cyber space offering a plethora of opportunities for criminals, the ICT industry and the society at large are facing serious challenges related to security and forensic issues. This paper presents major initiatives taken by Department of Information Technology, Government of India for prevention and mitigation of Cyber Crime in India. It also covers briefly some of the infrastructure and training programs of other Government Departments as well as major IT Industry Associations, in the area of cyber crime and forensics.**

Index Terms— **Cyber Crime, Cyber Forensics, Cyber Laws, Information Technology Act 2000.**

I. INTRODUCTION

As the Cyber Landscape is changing with technological changes in computers, networks and applications, so is the crime scene changing rapidly both within and outside the nations and has made a significant impact on the criminal justice system prevalent throughout the world. Its effects are felt more as nations constantly endeavor to provide quicker and more efficient services to its citizens through the use of cyber space. Globally not only the cyber landscape and hence the crime scene is changing but unfortunately the crime rate is increasing alarmingly both in value terms as well as in numbers. Each nation having different geographic, socio-economic and political structure is evolving its own strategies to tackle this issue.

India enjoys a competitive edge over many other neighboring nations particularly in the global ICT and software business in spite of its wide geographic, cultural and linguistic spread. It is known for its large pool of technical/ skilled human resource (English speaking). The Indian software industry is focusing on a robust Information Security environment which is essential in the cyber arena to maintain its competitive market position. However crime cannot be avoided and the cyber crime is even increasing as the usage of internet applications in the society is increasing. Prevention and mitigation of cyber crime therefore becomes an important issue. Major initiatives (in the civilian sector) taken by Government of India as well as industry to prevent and mitigate cyber crime, different aspects of which are handled by different organizations, are presented in this paper.

Ministry of Home Affairs, under the Central Government is the nodal ministry for managing law and order and internal security besides other activities. The Police, Bureau of Police Research & Development (BPR&D), National Crime Records Bureau (NCRB), Directorate of Forensic Science (DFS), National Police Academy (NPA) etc. are all under this Ministry. However the law and order at state level, is a state issue and each state has its own set up i.e. State Police, State Forensic Laboratories, and State Police Academies etc.

The Central Bureau of Investigation (CBI), functioning under Ministry of Personnel, Pension and Public Grievances, Government of India, is the premier investigating police agency in India, playing a major role as a national investigative agency. It is also the nodal police agency in India, which coordinates investigation on behalf of Interpol Member countries.

While the basic crime investigation responsibility as well as training its personnel lies with the Law enforcement agencies, the Department of Information Technology (DIT) being the nodal agency for Information Technology facilitates and strengthens their capabilities in handling the Technology crimes like cyber crimes. With a broad vision "To make India an IT Super Power by the Year 2008", DIT assumes the role of a

- Pro-active facilitator
- Pro-active motivator
- Pro-active promoter
- Spread of IT to masses and
- Ensure speedy IT led development

Gulshan Rai is with the Department of Information Technology, Government of India, New Delhi-110003, India. He is presently the Head of Cyber Laws Division and Director, CERT-IN.

B Vasanta, is Scientist F in the Department of Information Technology, Government of India, New Delhi-110003, India.(phone: 91-11-24363648, email: vasanta@mit.gov.in)

II. LEGAL FRAMEWORK

A. *Information Technology Act 2000*

As a first step to handle cyber crime, DIT has established a legal framework in India through enactment of the Information Technology (IT) Act 2000 by the Parliament. The Act provides 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.

The Act defines various computer and crime related terms, offences as well as penalties and adjudication in such cases. The Act also provides for (i) appointing Adjudicating Officers to consider the cases of certain types of computer crimes in an expedite manner and (ii) establishing one or more appellate tribunals to be known as the Cyber Appellate Tribunal for considering the appeals arising out of the cases filed with Adjudicating Officers.

Government of India has notified the State Secretaries of IT departments as Adjudicating Officers.

As per the provision in the Information Technology Act 2000, the Cyber Appellate Tribunal consists of only one person, "The Presiding Officer of the Cyber Appellate Tribunal", who could be a judge of a High Court or a member of the Indian Legal Service and holding or has held the post of Grade I of that service for at least three years.

Recent developments nationally, and internationally particularly with respect to provisions related to data protection and privacy in the context of BPO operations, liabilities of network service providers, regulation of cyber cafes, new crimes etc. has brought the IT Act 2000 into focus again. With an objective to review the IT Act 2000, in the light of such developments and to consider the feedback received for removal of certain deficiencies in the Act, an Expert Committee was set-up. The Expert Committee has completed its deliberations and submitted its report giving due consideration for two main issues namely, (i) using the IT as a tool for socio-economic development and employment generation, and (ii) further consolidation of India's position as a major global player in IT sector. The Bill for amendment of IT Act 2000 is under process.

B. *Controller of Certifying Authorities*

The IT Act provides for setting up of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities (CAs) who in turn issue digital signature certificates to users for electronic authentication.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates as the Root Certifying Authority of India (RCAI). The CCA also maintains the National Repository of Digital Certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

The following are the licensed CAs in India:

1. SAFESCRIPT
2. National Informatics Center (NIC)
3. Institute for Development and Research in Banking Technology (IDRBT)
4. Tata Consultancy Services (TCS)
5. Mahanagar Telephone Nigam Limited (MTNL)
6. Customs & Central Excise
7. (n)Code Solutions

To generate awareness of the IT Act and its implementation, cyber crime & forensics etc, CCA also conducts seminars periodically.

C. *CERT-In*

The Indian Computer Emergency Response Team, CERT-In has been set up recently by DIT, to become the nation's most trusted referral agency for responding to computer security incidents as and when they occur; the CERT-In also assists members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

Besides providing a platform for incidence reporting, issuing virus alerts, advisories, vulnerability and incidence notes etc, CERT-In also publishes a monthly security bulletin and organizes workshops on related subjects.

CERT-In also empanels 'IT Security Auditors', for auditing, including vulnerability assessment and penetration testing of computer systems & networks of various Government organizations, the critical infrastructure organizations and those in other sectors of Indian economy.

III. CYBER CRIMES IN INDIA

NCRB publishes an annual report, "Crime in India" which is a compendium of crime statistics provided by the State Governments and Union Territories (UT) administrations and Heads of other Law Enforcement Agencies relating to Indian Penal Code (IPC) and other special and local laws portraying the overall crime scenario of the country in its various aspects. After the enactment of IT Act 2000 which has specified certain Computer, Network and Data related acts as punishable, Cyber Crime has found an entry into this Report. NCRB published data is used in this section.

During the year 2005, 179 cyber crime cases have been registered under IT Act 2000 as compared to 68 cases during

the previous year, as can be seen from Table 1 below, thereby reporting a significant increase of 163.2 percent in 2005 over 2004.

TABLE 1

CYBER CRIMES/CASES REGISTERED UNDER IT ACT 2000 DURING 2004-2005

S.No.	Crime Heads	Cases Registered 2004	2005
1.	Tampering (*Sec.65*)	2	10
2.	Hacking{*Sec.66(1), Sec.66(2)*}	26	74
3.	Obscene publication/transmission (*Sec.67*)	34	88
4.	Failure(*Sec.68, Sec.69*)	0	1
5.	Un-authorized access/attempt (*Sec.70*)	0	0
6.	Obtaining License or Digital Signature by misrepresentation/suppression of fact (*Sec.71*)	0	0
7.	Publishing false digital Signature certificate (*Sec.73*)	0	0
8.	Fraud – Digital Signature (*Sec.74*)	0	1
9.	Breach of confidentiality/privacy (*Sec.72*)	6	5
	Total:	**68**	**179**

Of the total 179 cases registered under IT Act 2000, about 50 percent (88 cases) were related to Obscene Publications / Transmission in electronic form, normally known as cyber pornography.

A. Crime, head-wise and age-group wise

TABLE 2

PERSONS ARRESTED UNDER CYBER CRIME, BY AGE GROUP, DURING 2005 (Offences Under IT Act)

S.No.	Crime Head	Below 18 yrs	Between 18-30 yrs	Between 30-45 yrs	Between 45-60 yrs	Above 60 yrs	Total
1.	Tampering	1	9	0	0	0	10
2.	Hacking						
	i)Loss/damage to computer resource	0	19	6	2	0	27
	ii)Hacking	0	12	2	0	0	14
3.	Obscence publication/transmission in electronic form	0	85	36	3	1	125
4.	Fraud Digital/ Signature	0	0	3	0	0	3
5.	Breach of confidentiality/ privacy	0	6	6	1	0	13
	Total:	**1**	**131**	**53**	**6**	**1**	**192**

Profile of the offenders arrested under IT Act 2000 is shown in Table 2 above. The age-wise profile of persons arrested in Cyber Crime cases under IT Act, 2000 shows that 68.2 percent of the offenders were in the age group 18 – 30 years (131 out of 192) and 27.6 percent of the offenders were in the age group 30- 45 years (53 out of 192). Nearly 65.1 percent (125 out of 192) of the offenders were arrested under head 'Obscene publication/transmission in electronic form' of which 68.0 percent (85 out of 125) were in the age-group 18 –30 years. Of the total persons arrested for 'Hacking Computer Systems', more than 75 percent (31 out of 41) were in the age group of 18-30 years.

The data clearly indicates that persons in the age group 18-30 years commit cyber crimes more, and obscene publication/transmission in electronic form is the most common cyber crime committed during the year 2005.

B. Incidence of Cyber Crimes in Cities

From the cyber crime data as reported in the NCRB report, it has also been found that 25 cities out of 35 mega cities in India (with population of more than 1 million) did not report any case of Cyber Crime during the year 2005. The cyber crimes are registered either under the IT Act 2000 or under IPC. The cases reported under IPC are shown in Table3 below.

TABLE 3

INCIDENCE OF CYBER CRIME CASES REGISTERED IN MEGA CITIES DURING 2005 (OFFENCES UNDER IPC)

S.No	City	Forgery	Breach of Trust Fraud	Currency Stamp Paper Fraud	Total
1.	Ahmedabad	2	5	-	7
2.	Delhi	8	-	-	8
3.	Meerut	-	1	-	1
4.	Surat	2	113	31	146
5.	Vijayawada	1	-	-	1
	TOTAL	**13**	**119**	**31**	**163**

Non reporting of cases under the IT Act 2000, from some of the mega cities could be partly due to fear of losing reputation/brand name on the part of the victims and partly due to insufficient understanding and interpretation of different Sections of IT Act 2000 on the part of Law Enforcement Personnel or other reasons which may need further analysis. The high incidence of crime, for example in Surat could be a random incidence in 2005 but needs further studies as well as more statistically dependable data to draw any conclusion.

Only 5 mega cities have reported 163 cyber crime cases

under IPC. There has been a significant increase of 527 percent (from 26 cases in 2004 to 163 cases in 2005) in cases as compared to previous year (2004). While increasing population is observed to be one of the important factors influencing incidence of crime, increased criminal activities in mega cities could also be on account of unchecked migration, socio-cultural disparities, uneven distribution of incomes etc. More data and detailed analysis are required to correlate these statements.

IV. INFRASTRUCTURE FACILITIES

The Directorate of Forensic Science under the Ministry of Home Affairs, with its three Computer Forensic Labs (CFLs) and three offices of Government Examiner of Questioned Documents (GEQDs) provides the necessary forensic analysis expertise to the Law enforcement agencies. Most of the States also have Forensic Science Laboratories, and some of the cyber crime cells at the state police stations also have limited facilities and expertise to handle common cyber crimes related to emails, pornography, hacking etc. However, the Central and State Forensic Laboratories are more conversant with conventional areas of forensics like Ballistics, Toxicology/Serology, Physical & Chemical sciences etc. and Computer/Cyber forensics has not yet been identified as an independent discipline in forensics. Cyber forensics is one amongst many other crime investigation facilities operated by these organizations and being a new area, have scanty infrastructure & trained personnel. Very few of them have facilities and expertise to meet the changing needs in cyber crime investigations.

Two technical resource centers, one focusing on computer disk forensics and the other on steganograhy, set up at Center for Development of Advanced Computing (CDAC) Thiruvananthapuram and Kolkata respectively, have been sponsored by DIT. These centers besides research also facilitate law enforcement agencies in cyber crime investigations.

V. TRAINING

For successful prosecution of cyber crimes it is essential to have adequate and cogent digital evidence against the suspect and then link this information to the suspect in a legally acceptable manner. Information stored in digital form is transient in nature and therefore law enforcement personnel require specialized skills to seize, collect, analyze and report digital evidence in a Court of Law.

Many organizations like NCRB-Delhi, CBI Academy-Ghaziabad, National Police Academy -Hyderabad etc conduct training programs, generally on computers software packages and fundamentals of cyber forensics. Some collaborative training programs with FBI are also conducted. CERT-IN, CCA, CFSL etc conduct some subject specific courses on Cyber Security, Cyber Laws, Cyber Crimes & related issues. In general, the courses on cyber forensic tools, their suitability for specific applications, comparisons, technology & crime trends, international best practices etc are rare or very few. Police personnel are also frequently transferred to hold different assignments & hence there is a continuous need for training in the enforcement department. Also, as most of the crimes involve use of computers & electronic gadgets at some stage of committing the crime or the other, basic knowledge & training in digital evidence is always desirable and advantageous for the law enforcement personnel. There is an urgent need for conducting more training programs and there is scope for public private partnership as well as international cooperation in this area.

VI. INTERNATIONAL COOPERATION

Cyber Crime cases are covered under Mutual Legal Assistance Treaties (MLATs), which India has with various countries. Moreover, India is a member of Cyber Crime Technology Information Network System (CTINS), which is a Japanese Govt. initiative for mutual exchange of information regarding cyber crimes among the member countries, which is advisory in nature. This system is presently installed in the Cyber Crime Investigation Cell of Central Bureau of investigations (CBI), which is also 24x7 point of contact for Sub Group of Hi-tech Crimes of G-8 Countries.

VII. INDUSTRY INITIATIVES

The two industry associations in India which are participating in major promotional activities in the IT sector are, National Association of Software and Service Companies, NASSCOM, and Manufacturer Association of Information Technology, MAIT.

MAIT, initially set up for purposes of scientific, educational and IT industry promotion, has emerged as an effective and dynamic organization with majority of the Members coming from the Hardware Sector, by turnover, and the remaining from Training, Design, R&D and the associated services sectors of the Indian IT Industry. MAIT's charter is to develop a globally competitive Indian IT Industry, promote the usage of IT in India, strengthen the role of IT in national economic development and promote business through international alliances. The organization's special focus is on domestic market development and attracting foreign investment in the Indian IT Industry.

NASSCOM, the premier trade body and the chamber of commerce of the IT software and services industry in India was set up to facilitate business and trade in software and services and to encourage advancement of research in software technology. It is a not-for-profit organization. With over 1050 members, of which over 150 are global companies from the US, UK, EU, JAPAN AND CHINA, NASSCOM is a true

global trade body, with member companies in the business of software development, software services, software products and it-enabled/bpo services.

Information Security remains one of the key priorities for the Indian IT Enabled Services –Business Process Outsourcing (ITES-BPO) industry, a challenge that has to be overcome in order to firmly establish the sector's credentials as a trusted sourcing destination. Recognizing the fact that security breaches in leading BPO firms can put a spanner in India's successful outsourcing run, the industry has come forward to devise roadmaps and outline strategies that will help create an impregnable Information Security environment. The country, in fact has been working very closely with representatives of the US market, the largest outsourcer of processes to India. Two years ago, this collaborative effort bore fruit as the Indian IT-ITES industry, represented by NASSCOM and the US market, represented by the Information Technology Association of America (ITAA), came together to launch the prestigious "India-US Information Security Summit."

Cyber laws, cyber security, cyber crime etc are important issues discussed in several seminars and workshops conducted periodically by the industry associations.

A joint initiative of NASSCOM and Mumbai Police, the Mumbai Cyber Lab is a unique initiative of Police-Public collaboration to facilitate investigations of cyber crime; some of its the broad objectives are to:

- Promote collaboration among Mumbai Police, Information Technology industry, academia and concerned citizens to address cyber crime and its related issues.
- Develop pro-active strategies for anticipating trends in cyber crime and formulating technical and legal responses on various fronts.
- Facilitate cyber crime investigation training among police officers.
- Develop cyber crime technology tools for criminal investigation. Improve awareness of cyber crime among the people and enhance Information Security in Mumbai city in general.
- Act as Resource Center for other police organizations in the country.

VIII. CONCLUSION

To combat cyber crime, India, besides ensuring a robust Information Security environment, has put up a legal framework in place, initiated awareness and training programs and set up cyber forensic facilities. However the cyber crime data for year 2005 indicates an increase in the crime rate, particularly in mega cities and more offenders are in the age group, 18-30 years which draws special attention and needs further studies to understand the motives, implications etc. More focused awareness and training programs in cyber crime related topics and social engineering in general and for this age group in particular involving private partnership could probably go a long way in improving the scenario.

Acknowledgment

The authors wish to acknowledge making extensive use of information available in public domain from the reference sites given below for preparing this paper.

NOTE: The views expressed in this paper are those of the authors and do not reflect those of Government of India.

REFERENCE SITES/PAGES

http://www.mit.gov.in/it-bill.asp

http://www.cca.gov.in/index.jsp

http://www.cert-in.org.in/roles.htm

http://mha.nic.in/police_main.htm

http://ncrb.nic.in/crime2005/home.htm

http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=11154

http://www.mumbaicyberlab.org/about/vision.htm

http://www.mait.com/aboutus.htm