



## ICT Penetration and Cybercrime in India: A Review

Anand Kumar Shrivastav\*

Research Scholar, Department of Computer Science  
Mewar University, Chittorgarh, India

Dr. Ekata

Associate Professor, Deptt. of Applied Science  
Krishna Institute of Technology, Ghaziabad, India

**Abstract**— This paper investigates the ICT penetration and prevalence of cyber crimes in India. Using data from various sources, we have tried to explore the ICT penetration, cybercrime trend and prevention efforts towards curtailing Cybercrime in India. Findings from our research show that ICT penetration, Internet usage and cybercrime in India are on the rise. Most of the cybercrimes have been committed by young persons of the age group 18-30. Although awareness of cyber crimes is on the increase, the crimes mostly go either unreported or conviction is very poor. Our law enforcement agencies need to be adequately equipped to combat Cybercrime. This will not only prevent the cybercrime but will raise the chances of apprehension and conviction also.

**Keywords**— Cyber crime, ICT, IDI, Spam, Hacking, Stalking, Phishing.

### I. INTRODUCTION

Internet is world's largest information system and giant network. As telecom infrastructure developments continue to penetrate into smaller towns, Internet usage numbers showcase the effects with its ever increasing base of users. The Internet is now a part of the globalization process that is evidently sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a 'compact' world. The penetration of Information and Communication technologies (ICT) offers great opportunities and more and more users are getting connected. The cost of owning Internet enabled devices has also facilitated to this growth. The increase in penetration of ICT, has spurred a growth in ICT-based businesses and services. The ICT sector with its direct and indirect contribution to various socio-economic parameters has become one of the most significant growth catalysts for the Indian economy. Besides transforming India's image to that of a global player as provider of world class ITES enabled solution and services, this sector is also significantly influencing the lives of thousands of people on various parameters like employment, standard of living and diversity among others. It has embarked on various IT-enabled initiatives like Government to citizen services, public distribution systems, Healthcare, e-Learning, and mobile banking, etc.

We are now said to be in the midst of a 'new industrial revolution', one that will lead us into a new kind of society, an 'information age' [1]. Unfortunately, this growth of ICT has also raised the specter of new criminal activities and given birth to threats like attack on ICT infrastructure, online fraud, child pornography, hacking and cracking and intellectual property rights violation. The Internet has evolved from a benign research environment to a place of criminal activities. Increasingly, all variant of cyber criminals like spies, thieves, and vandals exploit computers and networks to disrupt services. They sabotage information system and steal valuable data. The computer crime is a matter of concern because it may circumvent traditional security and control technique. Modern technology provides cyber criminals with powerful tools that just make crime easier. Cybercrimes also poses a great threat to the national security of all countries, whether developing or developed. The cybercrime causes companies and other institutions to lose billions of dollars. By some estimates, revenues from cybercrime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time [2]. Despite improved cyber defense, the number and cost of attacks seems to be rising at an even faster rate. Nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime [3]. Norton's Cyber Crime Report 2011 reveals that India loses approximately INR 34,110 Crores annually due to cyber related crimes [4]. Cybercrime has also presented a challenge to information technology professionals who lack an awareness of an interest in the cybercrime phenomena. In many cases the law enforcement officers have lacked the tools needed to tackle the problem; old laws haven't quite fit the crimes being committed, new laws haven't quite caught up to the reality of what is happening, and there were few court precedents to look for guidance [5]. India's prominent role in the IT global market has become one of the compelling priorities for the country to provide secure computing environment, adequate trust and confidence in electronic transactions by creation of suitable cyber security policy in the country. Such cyber security policy ought to be updated regularly in line with technology and security issues keeping in mind the whole spectrum of ICT users and ICT providers including individuals, companies, and government/non-government entities.

The remaining part of the paper is organized in six sections including the introduction. In the second and third section, we review the basic concept, definition and type of Cybercrime. In fourth section we have discussed the ICT penetration. The fifth sections present the finding on Cybercrime in India. The sixth section is devoted to review of Cybercrime prevention efforts in India. The paper concludes with summary of findings and recommendations for practice directions.

## II. BASIC CONCEPT AND DEFINITION

The concept of cybercrime is not so much different from that of conventional crime as both include conduct, which cause breach of rules of law. The definitions of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts [6]. Cyber crime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet. The Council of Europe's Cybercrime Treaty uses the term "Cybercrime" to refer to offences ranging from criminal activity against data to content and copyright infringement. Thomas and Loader define cyber crime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" [7]. Schinder define cybercrime as "a subcategory of computer crime and it refers to criminal offenses committed using the internet or another computer network as a component of the crime"[5]. Schell and Martin defined cybercrime as a crime related to technology, computers and the internet and it concerns governments, industries and citizens worldwide where cybercrime takes the form of either piracy, phreaking (obtaining free telephone calls), cyberstalking, cyberterrorism and cyberpornography. Schell and Martin define cyber crime broadly as "a crime related to technology, computers, and the Internet" [8]. Milhorn, on the other hand, simply defines cybercrime as any activity that uses the internet to commit a crime [9].

By these definitions, we can inference about the cyber crime or computer crime as, "It is a technique that employ ICT components like computer and communication equipments etc. to harm the individual, trade, government and ICT infrastructure".

## III. CYBER CRIME TYPE

A Cybercrime can be considered to be an electronic version of traditional crime. There are variety of Cybercrime and some common type of Cybercrimes are described below in brief -

- i. **Cyber Stalking/Online harassment:** When a victim is repeatedly and persistently followed and pursued online by e-mail or other electronic communication by offenders that may negatively impact a victim's livelihood, well-being, and mental or emotional state.
- ii. **Cyber Bullying:** Acts of harassment, embarrassment, taunting, insulting or threatening behaviour towards a victim by using internet, e-mail or other electronic communication device.
- iii. **Online Child Pornography:** Online child pornography is defined by pedophiles using computer resources to distribute illegal media of and to minors, as well as engaging in actions to sexually exploit children.
- iv. **Unwanted exposure to sexually explicit material etc.:** When a criminal sends pictures, videos, sound clips, cartoons or animations depicting sexual contents by e-mail or any other electronic means. This would include audio or video chat using web camera etc.
- v. **Hacking:** It is an electronic intrusion, or gaining access to resources like computer, e-mail or social networking accounts such as Face book, Orkut, Gmail, and Hotmail etc. via a computer or network resource without permission.
- vi. **Identity Theft:** When someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.
- vii. **Computer Fraud:** It is one of the most rapidly increasing forms of computer crime. It is also commonly referred to as Internet fraud. Essentially, computer or Internet fraud is "any type of fraud scheme that uses one or more components of the Internet-such as chat rooms, e-mail, message boards, or Web sites to present fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme"
- viii. **Credit/Debit Card Fraud:** It is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.
- ix. **Spoofing:** It is a technique whereby a fraudster pretends to be someone else's email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster's newly created fraudulent web site.
- x. **Phishing:** Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dope the victim into divulging sensitive information, such as passwords, credit card and bank account numbers. The victim, usually via email is provided with a hyperlink that directs hi/her to a fraudster's web site. This fraudulent web site's name closely resembles the true name of the legitimate business.
- xi. **Denial of Service:** A denial of service attack is a targeted effort to disrupt a legitimate user of a Service from having access to the service. Offenders can limit or prevent access to services by overloading the available resources, changing the configuration of the service's data, or physically destroying the available connections to the information

- xii. **Spam:** It is the distribution of bulk e-mail that offers recipients deals on products or services. The purpose of these unsolicited mails is to make customers think they are going to receive the real product or service at a reduced price. However, before the deal can occur, the sender of the spam asks for money, the recipients' credit card number or other personal information. The customer will send that information and never receive the product nor hear from the spammer.
- xiii. **Malicious Programs/Viruses:** Viruses and malicious programs can potentially impact a massive amount of individuals and resources. These programs are intended to cause electronic resources to function abnormally and may impact legitimate users access to computer resources.
- xiv. **Cyber terrorism:** It is the adaptation of terrorism to computer resources, whose purpose is to cause fear in its victims by attacking electronic resources.

#### IV. Ict Penetration

Information and Communication Technologies for Development is a term used to refer the application of Information and Communication Technologies (ICTs) within the field of socioeconomic development. The ICT Development Index (IDI) is a composite index combining 11 indicators into one benchmark value (presented on a scale from 0 to 10). The objectives of the IDI are to monitor progress in ICT developments in both developed and developing countries and to measure the evolution of the global digital divide [10]. Out of 155 countries, India ranks at 119 while Republic of Korea stands at rank one. In 2011, at least 2.3 billion people – equivalent to more than one third of the world's total population had access to the internet. Developed countries enjoy higher levels of internet access (70 per cent) than developing countries (24 per cent). However, the absolute number of internet users in developing countries already far outnumbers that in developed countries. Some 62 per cent of all internet users were in developing countries in 2011 [6]. In 2013, over 2.7 billion people are using the Internet, which corresponds to 39% of the world's population. In 2013, 41% of the world's households are connected to the Internet. Half of them are in the developing world, where household Internet penetration has reached 28%. In developing countries, the number of mobile-broadband subscriptions more than doubled from 2011 to 2013 (from 472 million to 1.16 billion) and surpassed those in developed countries in 2013 [11]. Internet usage in India is still driven by the youth. India figures in the list of top 20 Internet users country (Table-1), [12].

The smaller towns have witnessed 41% growth of active internet users. According to 2011 Census, 339 million individuals live in the urban India. Of these, about 39% people know how to operate a computer. This number has grown from 32% in 2009 and 38% in 2011. 63 % of the computer literate individuals claim to have used the internet at least once in the past. Of these, about 80% of individuals have claimed to have been actively accessing the Internet, at least once in the past month. As of June 2012, there are 137 million claimed Internet Users in India: 99 million from Urban India and 38 million from the rural parts of the country. Out of these 137 million claimed Internet Users, there are 111 million Active Internet Users (80 million in urban and 31 million in rural areas) [13].

**Table-1**

| S.N.              | Country or Region | Population, 2012 Est | Internet Users Year 2000 | Internet Users Latest Data | Penetration (% population) | Users % World |
|-------------------|-------------------|----------------------|--------------------------|----------------------------|----------------------------|---------------|
| 1                 | China             | 1,343,239,923        | 22,500,000               | 538,000,000                | 40.1 %                     | 22.4 %        |
| 2                 | United States     | 313,847,465          | 95,354,000               | 245,203,319                | 78.1 %                     | 10.2 %        |
| 3                 | India             | 1,205,073,612        | 5,000,000                | 137,000,000                | 11.4 %                     | 5.7 %         |
| 4                 | Japan             | 127,368,088          | 47,080,000               | 101,228,736                | 79.5 %                     | 4.2 %         |
| 5                 | Brazil            | 193,946,886          | 5,000,000                | 88,494,756                 | 45.6 %                     | 3.7 %         |
| 6                 | Russia            | 142,517,670          | 3,100,000                | 67,982,547                 | 47.7 %                     | 2.8 %         |
| 7                 | Germany           | 81,305,856           | 24,000,000               | 67,483,860                 | 83.0 %                     | 2.8 %         |
| 8                 | Indonesia         | 248,645,008          | 2,000,000                | 55,000,000                 | 22.1 %                     | 2.3 %         |
| 9                 | United Kingdom    | 63,047,162           | 15,400,000               | 52,731,209                 | 83.6 %                     | 2.2 %         |
| 10                | France            | 65,630,692           | 8,500,000                | 52,228,905                 | 79.6 %                     | 2.2 %         |
| 11                | Nigeria           | 170,123,740          | 200,000                  | 48,366,179                 | 28.4 %                     | 2.0 %         |
| 12                | Mexico            | 114,975,406          | 2,712,400                | 42,000,000                 | 36.5 %                     | 1.7 %         |
| 13                | Iran              | 78,868,711           | 250,000                  | 42,000,000                 | 53.3 %                     | 1.7 %         |
| 14                | Korea             | 48,860,500           | 19,040,000               | 40,329,660                 | 82.5 %                     | 1.7 %         |
| 15                | Turkey            | 79,749,461           | 2,000,000                | 36,455,000                 | 45.7 %                     | 1.5 %         |
| 16                | Italy             | 61,261,254           | 13,200,000               | 35,800,000                 | 58.4 %                     | 1.5 %         |
| 17                | Philippines       | 103,775,002          | 2,000,000                | 33,600,000                 | 32.4 %                     | 1.4 %         |
| 18                | Spain             | 47,042,984           | 5,387,800                | 31,606,233                 | 67.2 %                     | 1.3 %         |
| 19                | Vietnam           | 91,519,289           | 200,000                  | 31,034,900                 | 33.9 %                     | 1.3 %         |
| 20                | Egypt             | 83,688,164           | 450,000                  | 29,809,724                 | 35.6 %                     | 1.2 %         |
| TOP 20 Countries  |                   | 4,664,486,873        | 273,374,200              | 1,776,355,028              | 38.1 %                     | 73.8 %        |
| Rest of the World |                   | 2,353,360,049        | 87,611,292               | 629,163,348                | 26.7 %                     | 26.2 %        |
| Total World Users |                   | 7,017,846,922        | 360,985,492              | 2,405,518,376              | 34.3 %                     | 100.0 %       |

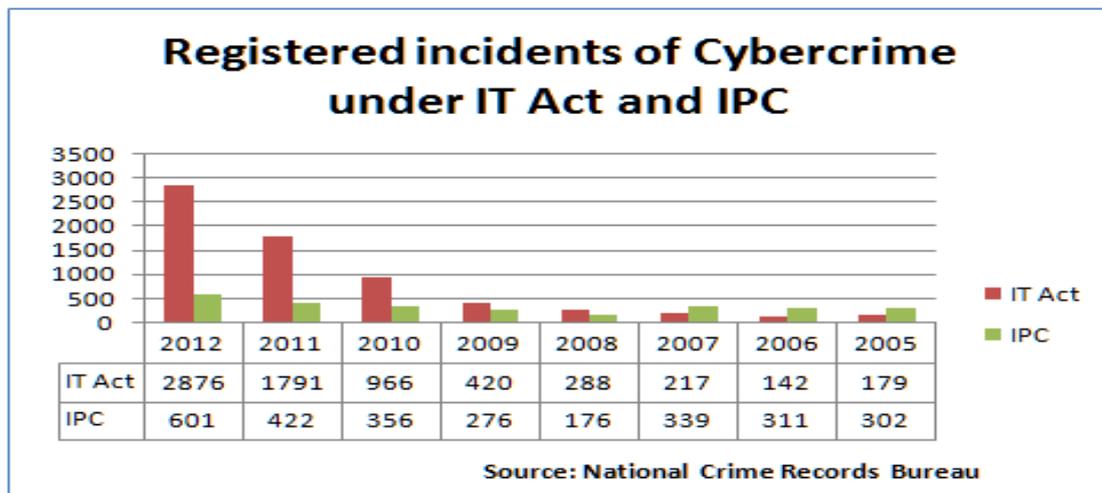
**Top 20 Countries with highest number of Internet users – June 30, 2012.**

(Source: [www.internetworldstats.com](http://www.internetworldstats.com))

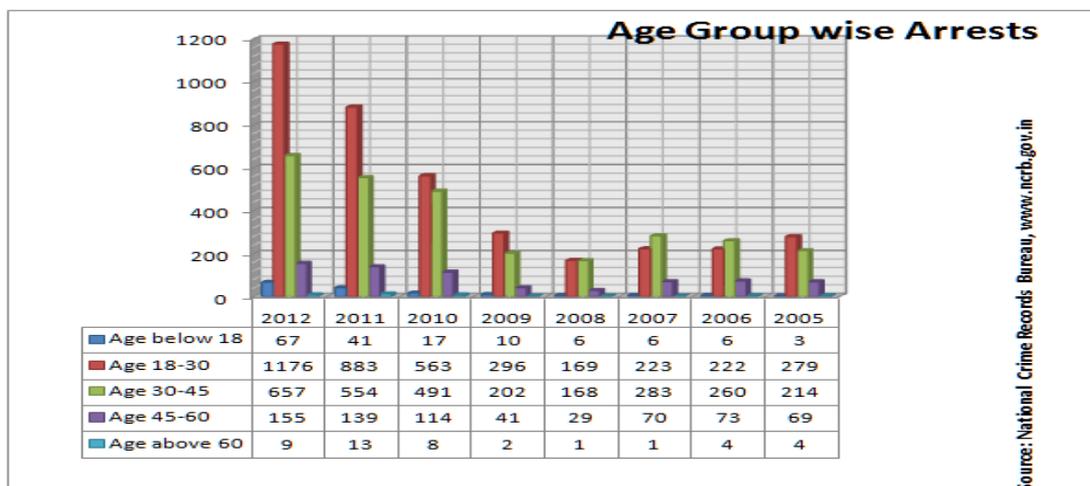
### V. Cyber Crime In India

Every year, cyber crime in India is going up by 50 per cent and during the last five years, around 9,000 Indian websites including those of various government departments were hacked. Many government websites, some of them carrying sensitive information have become victims of cross-border hacking, mainly from Pakistan, Bangladesh, Nepal and China [14]. As per IC3's annual report 2012, India, ranked among the top five nations for the maximum complaint of cyber crime and it ranked 6th in terms of complainant loss to the tune of \$3,740,736.53 [15]. Information and Cyber insecurity has been ranked at third position in India Risk Survey 2013 to which companies are most vulnerable [16]. According to Norton cyber crime report 2012 [17], a global financial loss of up to \$110 billion occurred due to cyber crime. The report also reveals that 66 per cent of Indian online adults have been victims of cyber crime in their lifetime. In the past 12 months, 56 per cent of online adults in India have experienced it (a little over 115,000 daily victims or 80 per minute). In India, one in three online adults (32 per cent) has been a victim of either social or mobile cyber crime in last 12 months, and 51 per cent of social network users have been victims of social cyber crime. The report says most internet users take basic steps to protect themselves and their personal information. These include deleting suspicious emails and being careful with their personal details online. However, other core precautions are being ignored. For instance, 25 per cent don't use complex passwords or change their passwords frequently. And, 38 per cent do not check for the padlock symbol in the browser before entering sensitive personal information, such as banking details, online. Well over half (64 per cent) of online adults in India report having been notified to change their password for a compromised email account. Close to 42 million people in India were hit by cyber crime attacks in the past 12 months, causing an approximate loss of \$8 billion (INR 44,500 Crore). The average direct financial cost per victim is \$192, up 18 per cent over 2011 (\$163).

In India, Cybercrime cases are registered under Indian Penal Code (IPC) and under Information Technology Act (IT-Act). The IT Act was enacted in year 2000 and later amended in 2008. During year 2005, 302 persons were booked under IPC and 179 under IT Act, while in year 2012, 2876 persons were charged under IT Act and 601 persons were charged under IPC. It shows awareness of IT Act among police personnel. It is also observed that in year 2012, a total of 2064 persons were arrested in Cybercrime cases and out of these, 1176 arrested persons were between age group of 18-30 year. In year 2011, a total of 1630 persons were arrested, out of these, 883 persons were of age group 18-30 year of age. [18]. A graphical representation of the statistics is shown in Figure-1 and Figure-2.



(Figure-1)



(Figure-2)

Despite the increasing cases of cybercrime incidents, and arrests of culprits, the conviction rate is very poor in India. There have only been few cybercrime convictions in the whole country, which can be counted on fingers [19]. The Computer crime can be convicted only on digital evidence and lack of the same leads to low conviction. One of the reasons may be that, in India, most of the police stations are not technically equipped for cyber crime investigation and collection of digital evidences. Secondly, the purpose of setting up of specialized cyber crime cell is defeated when police personnel from law and order are transferred into cyber crime police stations; they hardly are of any help as they lack the expertise. Most of the time electronic evidence is not captured, retained and preserved in the manner required by the Indian Evidence Act. The digital evidence required to be collected as early as possible and by not acting on time contributes to the cause of low convictions. Because of its inability to come up with credible and legally valid electronic evidence, the police find it extremely difficult to defend their case in court of law. Lack of legal awareness related to cyber laws, dearth of cyber law experts, insufficient number of cyber cells across country, interdependence of cyber world and most importantly, rise of a net savvy generation are chiefly responsible for making this risk very critical.[20].

#### **VI. Prevention Efforts**

In order to deal with cybercrimes, India has established Computer Emergency Response Teams (CERT) with an objective to coordinate and respond during major security threats. The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development. Sectoral CERTs have been functioning in the areas of defence and Finance for catering critical domains. [21]. Bangalore has been credited with introducing one of the first cyber cells in India. As of now, there are 18 cyber cells in major cities of India, but with increasing dependence on the internet, even smaller cities are registering a significant rise in the number of such cases [20].

The Department of Information Technology (DIT) has set up Resource Centre for Cyber Forensics at the Centre for Development of Advanced Computing (C-DAC, Thiruvananthapuram, which has developed indigenous cyber forensic tools. These tools are now being used by agencies to investigate cyber crime cases. The C-DAC, Thiruvananthapuram also conducts training programmes for law enforcement agencies on these tools. The Indian Computer Emergency Response Team (CERT-In) provides reactive and proactive support to the cyber incidents in the country. It also liaisons with similar agencies worldwide and users of cyber space in the country including Government, public or private and issues alerts, advisories and vulnerability notes. These advisories are also published on the website of CERT-In (<http://www.cert-in.org.in>). The CERT-In also interacts with cyber users in the country to mitigate such incidents. Besides these, a framework of the IT roadmap has been published and government has granted permission for closer government/industry cooperation to leverage the output of India's world-class IT software industry. In addition, a new National Defense University and Defense Intelligence Agency (DIA) have been established.

#### **VII. Conclusion**

Internet and Communication Technology has influenced every wake of our life in one or other way. In comparison to other developing country, the higher ICT penetration in India is appreciable. However, this increase has also lead towards an abundant growth in criminal activity conducting exclusively through virtual means. The present study reveals that most of the Internet users and perpetrator of Cybercrime in India are young. This is in harmony to the world figure. These young perpetrators have some degree of technical competence to commit computer-related crimes. This review brought to the fore the fact that cyber crime is fast gaining grounds in India and the agencies responsible for investigation, controlling and apprehending online criminals lack the technical knowledge needed to tackle the problem. With increasing penetration of ICT, its impact appears to be worse in developing countries where the technology and law enforcement expertise is inadequate. Analysis of literature and data shows that that most culprits go un-punished due to lack of evidence. Defence lawyers often win over when the prosecution presents poor evidence. It gives an impression that the Indian police are insufficiently organized to combat cyber crime. The Information security requires sufficient number of skilled professionals to deal with variety of domain specific actions. The police and law enforcement agencies should be empowered with power of Information Technology by providing the needed training, and infrastructure so that they may discharge their duties effectively. There is a need for continuous change in the police organization. Since cybercrime is a global problem, the need also arise for law enforcement agencies including State police to collaborate in the area of information sharing, infrastructure and personnel with other agencies such as the Central Bureau of Investigation (CBI), National Technical Research Organization (NTRO), Cert-In and INTERPOL to crack-down on cyber criminals. In order to train security professionals with special skill sets, it is imperative to create master trainers and training organizations to cater to these special skill sets and to train all types of users including law enforcement agencies, judicial officers, owners/operators of e-Government services etc. Towards this effect, it is an imperative need to set up adequate training infrastructure to cater to the needs of all types of users. Due to lack of information security awareness on the part of computer users, developers and administrators, many cyber vulnerabilities exist. The promotion of information security awareness is an ongoing process, required to achieve the broadest penetration to enhance awareness against any security threats. The children and small computer users are most vulnerable to criminal exploitation on the Internet. A specially designed cyber security awareness programme is imminent for this sect of society. Besides these, there is a need of concerted effort on the part of individual and companies, to report cyber crime cases.

**REFERENCES**

- [1]. Webster, F. "Theories of the Information Society", 2nd edn. London: Routledge, (2003).
- [2]. O'Connell, "Cyber-Crime hits \$ 100 Billion in 2007", ITU News related to ITU Corporate Strategy, 17.10.2007, [http://www.ibls.com/internet\\_law\\_news\\_portal\\_view\\_prn.aspx?s=latestnews&id=1882](http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882) [Accessed: 11-05-2013 ]
- [3]. IBM survey, 14.05.2006, <http://www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html>, [Accessed: 11-05-2013]
- [4]. Symantec Corporation, "Norton Cyber Crime Report 2011"; [www.symantec.com](http://www.symantec.com)
- [5]. Debra Littlejohn Shinder, "Scene Of The Cybercrime: Computer Forensics Handbook", (2002).
- [6]. United Nations Office on Drugs and Crime, Vienna, "Comprehensive Study on Cybercrime", February 2013
- [7]. Thomas, D and Loader, B, "Cybercrime: Law Enforcement, Security and Surveillance in the Information Age", London: Routledge, (2000)
- [8]. Schell, B. & Martin, C, "Cybercrime: A Reference Handbook". Santa Barbara: ABC-CLIO, (2004).
- [9]. H. Thomas Milhorn, 'Cybercrime: How to Avoid Becoming a Victim', Universal Publishers, (2007).
- [10]. Measuring the Information Society", International Telecommunication Union, (2012).
- [11]. "World in 2013, ICT Facts and Figures", International Telecommunication Union, 2013)
- [12]. Internetworld stats ([www.internetworldstats.com](http://www.internetworldstats.com))
- [13]. "Internet in India 2012", Internet and Mobile Association of India (IAMAI) , [www.imrbint.com](http://www.imrbint.com).
- [14]. "Cyber crime increasing in India at fast clip: P Chidambaram"; PTI Feb 14, 2012, 11.18PM IST)
- [15]. IC3 Report, [http://www.ic3.gov/media/annualreport/2012\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf) [Accessed: 15-05-2013]
- [16]. "India Risk Survey 2013", Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI) <http://www.ficci.com/Sedocument/20228/India-Risk-Survey-2013.pdf>; accessed 18-06-2013)
- [17]. Symantec Corporation, "Norton Cyber Crime Report 2012", [www.symantec.com](http://www.symantec.com). [Accessed: 09-04-2013]
- [18]. National Crime Records Bureau, "Crime in India-2012", [www.ncrb.gov.in](http://www.ncrb.gov.in), [Accessed: 12-06-2013].
- [19]. Talwant Singh, "Cyber Law and Information Technology", <http://delhidistrictcourts.nic.in/CYBER%20LAW.pdf>, [accessed 18-06-13].
- [20]. "India Risk Survey 2012", Pinkerton and FICCI, <http://ficci.com/SEDdocument/20186/IndiaRiskSurvey2012.pdf>, [Accessed:18-06-2013].
- [21]. Press Information Bureau India, <http://pib.nic.in/newsite/erelease.aspx?relid=61597>, [Accessed 10/06/2013].
- [22]. Computer Emergency Response Team, India; <http://www.cert-in.org.in>