Applications of Cyber Forensics: A Study of Cyber Security and IT Act 2000 to Prevent Cyber Crimes in Indian Society

Seema M. Shinde
Yeshwant college Nanded

Bhusare Sangita A.
Yeshwant College Nanded

Karhale Deepali

Abstract - The need for a common language for computer forensics is clear. Computer forensics lags behind other forensic disciplines in part due to insufficient dialogue between researchers and practitioners, and the result unreported due to a lack of awareness. The growth of cyber crime in India is on the rise and is that science| a fundamental component of forensics |is largely absent from computer forensics. An ability to communicate about the challenges of each side will ultimately help bring scientic method to computer forensics in the way that it exists in other forensic disciplines, such as DNA analysis where the statistics and science regarding the accuracy of the tests is well understood.

I. INTRODUCTION

1.1 Cyber crime

Cyber crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not limited and many activities can be characterized as falling in one or more category. Additionally, although the terms computer crime or cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and cheating, in which computers or networks are used to facilitate the criminal activity. [8]

Cyber crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access or illegal access, illegal interception non-public transmissions of computer data, from a computer system, data interference means unauthorized damaging, deletion, deterioration, alteration or suppression of computer data, systems interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, misuse of devices, ID theft, and electronic fraud. [12]

The modern thief can appropriate more with a computer. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb". Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes. Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system. Some knowledgeable observers consider this to be an unfortunate mistake, and point out that this difference is the cause of much of the insecurity of current computer systems -once an attacker has subverted one part of a system without fine grained security, user usually has access to most or all of the features of that system. Because computer systems can be very complex, and cannot be guaranteed to be free of defects, this security stance tends to produce insecure systems. [13]

1.2 Cyber law

Cyber law is important for cyber criminals punishing and it touches almost all aspects of communication and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may appear that Cyber law is a very technical field and that it does not have any attitude to most activities in Cyberspace. But the actual

truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and cyber legal perspectives. [11]

When Internet was developed, the founding fathers of Internet hardly had any tendency that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with people with intelligence, have been grossly misusing this aspect of the Internet to effect criminal activities in cyberspace. [46]

As the nature of Internet is changing is being seen as the critical medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails, to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyber law issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to make tighter your belts and take note of Cyber law for your own benefit. Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices such as hard disks, USB disks etc, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. [62]

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly cyberspace or the Internet. It is less a distinct field of law in the way that property or contract is as it is an intersection of many legal fields, including logical property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with heritage system of laws applicable to the physical world. [64]

1.3 Cyber Security

Cyber security is the organization of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In Cyber Security In this age of technology and communication convergence, you cannot help but be impacted by technologies and innovations that center on computers, cell phones and the Internet. But as we revolve our daily lives with these technologies, there are times that we set out to feel truly paranoid about our own safety. [1]

There are also attempts from the government, computer companies, digital experts, and additional companies to develop a more secure, stricter, and restructured cyber environment that's regulated by enforced laws and technical systems. With the existing setup, hackers and additional cyber criminals overcome free on the Internet, but additional cyber security and system developments in the cyber community will provide more fluent Internet usage and transactions with lesser risk for fraud and cyber attacks. [20]

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization. Cyber security is intended to protect personal and work-related data and information stored in our computer and personal websites. With the increase of persons, organizations, and members of the community falling prey to cyber crimes and security attacks, there is an addition in demands for more steps to be taken. [21]

The electronic computer was in the beginning produced as a harmless help to do complex formulas. Across the years, however, the harmless computer, which was appointed with just about unlimited potential, has become the foundation for cyber crimes. These cyber crimes, which impact persons, organizations, and even governments, demand tight cyber security to curtail the possibilities of imposing additional damage. But what comprises cyber security precisely. And protect the entire cyber community. [25]

There are also attempts from the government, computer companies, digital experts, and additional companies to develop a more secure, stricter, and restructured cyber environment regulated by enforced laws and technical systems. With the existing setup, hackers and additional cyber criminals prevail free on the Internet, but additional cyber security and system developments in the cyber community will provide more easy Inter Cyber security is not at all that hard. Once you've merged it into your system, then it is just like riding a bicycle or it can be as normal as walking. All you need is to find out how you'll be able to make it work well and establish a good habit to make cyber security uniform.Net usage and transactions with lesser risk for fraud and cyber attacks. [34].

1.4 Cyber forensic

Cyber forensic is the art and science of applying computer science to aid the legal process. Although plenty of science is attributable to computer forensics, most successful investigators possess a nose for investigations and a skill for solving puzzles, which is where the art comes in. [25]

It is more than the technological, systematic inspection of the computer system and its contents for evidence or supportive evidence of a universal wrong or a criminal act. Computer forensics requires specialized expertise and tools that goes beyond the normal data collection and preservation techniques available to end users or system support personnel. One definition is similar to "Electronic Evidentiary Recovery, known also as e-discovery, requires the proper tools and knowledge to meet the Court's criteria, whereas Computer Forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Another is a process to answer questions about digital states and events. This process often involves the investigation and examination computer system, including, but not limited to the data gaining that resides on the media within the computer. The forensic examiner opinion, based upon the examination of the material that has been recovered. After representation an opinion and report, to determine whether they are or have been used for criminal, civil or unauthorized activities. Computer forensics experts investigate data storage devices these include but are not limited to hard drives, portable like. Data devices USB Drives, External drives, Micro Drives and many more. [29]

In Cyber Forensic Investigations Most organizations have an incident handling and incident response team typically they do not perform the role to investigate computer crimes. Forensics is typically associated with law enforcement and criminal investigations, forensics techniques and technologies have wide spread applications ranging from complex incident response to ediscovery. The knowledge of understanding the processes is vital. An organization may own the best policy and process but do not have the skills and expertise to handle the computer related crime may potentially damage the process. [34]

II. CONCLUSION AND RECOMMENDATION

Cyber crimes in India are rapidly evolving from a simple e mail crime to more serious crimes like hacking and source code theft. It is a known fact that given the unrestricted number of free Web sites, the Internet is unquestionably open to misuse. Further, cases of spam, hacking, cyber stalking and email fraud are wild and, although cyber crimes cells have been set up in major cities, the problem is that most cases remain to control its scope and difficulty is the pertinent need today. It can be combated, diminished, cornered. Cyber space offers an excess of opportunities for cyber criminals either to cause harm to innocent people, or to make a fast jump at the cost of unsuspecting citizens. Although laws and cyber cells help people to capture culprits, also people need to be aware of cybercrimes happening and the cyber laws to curb criminals. Many of us do not report the crime to cops, but it is the responsibility of victim to report it to cops so the criminals get punished. This will certainly require a wider public awareness of the situation, and will take time, effort and challenge. There are some ethical challenges which include the complex technical and juridical issues arising in the struggle against cybercrime sometimes seem impossible. So much so that authorities and governments may legally feel helpless, and as a reaction, may be tempted to consider radical directives, in the Process endangering human rights in general and individual liberties in particular. This is a real danger, and must by no means be underestimated especially in a high tech domain, the workings of which are difficult to the loads. It is worth noting that none of the challenges described cannot be overcome. To be addressed efficiently, a strong political will is certainly almost always needed. A strong political will often stems from a strong public opinion. Is there such a thing as a public opinion on cybercrime? Most people actually do not know that viruses, Trojans and other malware in general are solely aimed at making money, and view them as more or less mean geek jokes, which in the best case would open one's CD-ROM player and in the worst case burn one's hard drive. As a matter of fact, most infected people ignore the fact that they are infected, and thereby part of a botnet, the infamous zombie computer networks at the core of cybercriminal activity.

The problem is that most cases remain unreported due to a lack of awareness. This poor awareness is further blurred by laws against illegal downloading, which designate average, tremendously common users as cybercriminals.

From the study of this dissertation I have come to conclusion that,

- Cybercrimes in India are rapidly evolving from a simple e mail crime to more serious crimes, causing huge loss to economy and large section of our society is unaware about how to combat these crimes.
- Although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness. Many users are unaware about how to report the cybercrime and about the IT act.
- IT Act is not sufficient as there are some ethical challenges which include the complex technical and juridical issues arising in the struggle against cybercrime.
- Also people, who are aware about cybercrimes & laws, do not report it due to hectic and the lengthy court battle by our judiciary system to get justice.

- Cyber forensics lags behind other forensic disciplines in part due to insufficient dialogue between researchers and practitioners, and the result is that science, a fundamental component of forensics is largely absent from cyber forensics.
- In India lots of time is wasted in making laws and sometimes a strong political will is not shown. A strong political will often stems from a strong public opinion. These factors have made IT act weak law. More stringent amendments need to be made in the IT act.
- In India, fully equipped, with trained staff cyber forensics laboratories are rarely observed.

I have studied Cyber Laws, Cyber Forensics and Cyber Crimes, IT Act 2000 in detail. As per my opinion, I feel that, the cyber laws are not sufficient to stop the cyber crimes. Cyber crimes are happening in a large scale. More efforts should be taken, more laws should be introduced, and they should be implemented strictly. If persons are follows some principles to stop growth of cyber crimes. Cyber principles are specially design for different organization like firms, governments, and civil society. The IT Act 2000 also castigate various cyber crimes and provides strict punishments, it's also not sufficient, we need implement new act, its implementation

REFERENCE AND BIBLIOGRAPHY

[1] CYBER TOP COPS ARTICLES: THE LATEST IN CYBER SECURITY.

[2] "*CYBERLAW - THE INDIAN PERSPECTIVE*- 2009 EDITION WITH IT ACT AMENDMENTS 2008 " - A book by Asia's Foremost authority & Expert on Cyberlaw, Pavan Duggal

[3] Source: Star Of Mysore Online By: MAYA BABU, MYSORE GRAHAKARA PARISHAT

[4] Chris L.T. Brown, Computer Evidence Collection and Preservation

[5] Computer Forensics: *Computer Crime Scene Investigation* – John R. Vacca, Charles River Media
[6] Computer and Intrusion Forensics – George Mohay, Alison Anderson, Byron Collie, Olivier De Vel, Rod McKemmish, Artech House
[7] Windows Forensics & Incident Recovery - Harlan Carvey, Addison Wesley
[8] *Digital Evidence and Computer Crime*, 2nd Edition - Eoghan Casey
[9] *Incident Response: Computer Forensics* - Chris Prosise, Kevin Mandia
[10] Access Denied: The Complete Guide to Protecting Your Business on the Internet, by Cathy Cronkite; Jack McCullough
[11] Advent of Netwar, by John Arquilla; David Ronfeldt
[12] Net Crime and Net Sex, the Truth Behind the Hype, by Charles Platt
[13] At Large: A True-Crime Tale of the Internet Age, by Charles C. Mann; David H. Freedman
[14] The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, by Clifford Stoll
[15] The Complete Hacker's Handbook: Everything You Need to Know about Hacking in the Age of the Web, by Dr K
[16] Computer Crime: A Crime-Fighters Handbook, by David Icove; William Vonstorch; Karl Seger
[17] Computer Crime: Phreaks, Spies, and Salami Slicers, by Karen Judson, ISBN: 0766012433, Jan 1999.
[18] Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, by Peter N. Grabosky; Russell G. Smith, ISBN: 0765804581, June 1998
[19] Cyber Crime: How to Protect Yourself from Computer Criminals, by Laura E. Quarantiello
[20] Cybercrime: Security and Surveillance in the Information Age, by Douglas Thomas; Brian Loader.
[21] Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption, by Winn Schwartau
[22] Cyberwar 3.0: Human Factors in Information Operations and Future Conflict, by Alan D. Campen; Douglas H. Dearth.
[23] Cyberwars: Espionage on the Internet, by Jean Guisnel; Gui Masai; Winn Schwartau
[24] Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (with CDROM), by Eoghan Casey
[25] Electronic Warfare in the Information Age (with Disk), by D. Curtis Schleher
[26] Fighting Computer Crime: A New Framework for Protecting Information, by Donn Parker
[27] The Fugitive Game: Online with Kevin Mitnick, by Jonathan LittmanHacker Crackdown: Law and Disorder on the Electronic Frontier, by Bruce Sterling
[28] Hackers: Crime in the Digital Sublime, by Paul A. Taylor
[29] Hacking Exposed: Network Security Secrets & Solutions, by Joel Scambray; George Kurtz; Stuart McClure.
[30] Handbook of Computer Crime Investigation: Forensic Tools and Technology, by Eoghan Casey.
[31] High-Technology-Crime Investigator's Handbook: Working in the Global Information Environment, by William C. Boni; Gerald L. Kovacich,.
[32] Identity Theft: The Cybercrime of the Millennium, by John Q. Newman
[33] Incident Response: Investigating Computer Crime, by Chris Prosise, ISBN: 0072131829, May 2001
[34] The Information Revolution and National Security: Dimensions and Directions, by Stuart J. D. Schwartzstein, ISBN: 0892062886, Jan 1997.
[35] Information Warfare and Security, by Dorothy E. Robling Denning.
[36] Information Warfare: Corporate Attack and Defense in a Digital World, by William Hutchinson; Matthew Warren.
[37] Information Warfare: Cyber terrorism--Protecting Your Personal Security in the Electronic Age, by Winn Schwartau, ISBN: 1560251328, Oct 1996.
[38] Information Warfare: How to Survive Cyber Attacks, by Michael Erbschloe, ISBN: 0072132604, May 2001.
[39] Information Warfare Principles and Operations, by Edward Waltz, ISBN: 089006511X, Sept 1998.
[40] Investigating Computer-Related Crime: Handbook for Corporate Investigators, by Peter Stephenson.
[41] The Next World War: Computers Are the Weapons and the Front Line is Everywhere, by James Adams.
[42] Organizing for Computer Crime Investigation and Prosecution, by Diane Pub Co.

[43] Secret Software: Making the Most of Computer Resources for Data Protection, Information Recovery, Forensic Examination, Crime Investigation and More, by Norbert Zaenglein.
[44] Strategic Information Warfare: A New Face of War, by Roger Molander; Peter A. Wilson; Andrew S. Riddile.
[45] Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace, by Richard Power; Rik Farrow.
[46] Transnational Criminal Organizations, Cybercrime and Money Laundering A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators, by James R. Richards.
[47] The Transnational Dimension of Cybercrime and Terrorism, by Abraham D. Sofaer; Seymour F. Goodman.
[48] Michael G. Noblett; Mark M. Pollitt, Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence".
[49] A Yasinsac; RF Erbacher, DG Marks, MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy.
[50] Warren G. Kruse; Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. pp. 392..