Cybercrime: A Global Threat to Cybercommunity

Dr.P.B.Pathak
Assistant Professor & Head, Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded, Maharashtra, India
pradeepbpathak@yahoo.com

***Abstract*—Cyberspace is a virtual space equal important as real space for business, politics and communities. Cyberspace is vulnerable to borderless cyberattacks. The global problem of Cybercrime is also social, legal and it's growing very fast. The present paper elaborates at length the concept of Cybercrime, various definitions and types. To successfully fight Cybercrime, people in the Information Technology (IT) community and those in the general population who are affected, directly or indirectly, by the criminal activity must work together.**

Keywords-Cybercrime; Cyberspace; Cybercommunity; Vulnerability; Threat; DoS

I. INTRODUCTION

The globalization has given rise to a globalization of criminal activity. Cybercrime has cross border dimensions and global implications. Networked technologies have created ample opportunities for criminal activity. There are various reasons for the rise in Cybercrimes: Global reach of the Internet, Lack of Information Security Management initiatives, Lack of awareness of Security Threats and Vulnerabilities, Misconception that only Firewalls and Antivirus Software's are adequate, Solid Information Security Policies and Procedures are either not enforceable / enforced or are not in place, Increasing Complexity of our Information Systems, Software written without security in mind, Lack of Information Security Integration into software projects, Widespread availability of attack scripts source code on the Internet, Ease of carrying out attacks, Poor chances of getting caught committing a Cybercrime due to kind of Anonymity provided by Computers and the Internet.

Threat can be defined as any potential occurrence, malicious or not, that can have an undesirable effect on the assets and resources associated with computer systems. There are Threats in large number as may be: *Confidentiality Threat* – Disclosure of unauthorized information, *Integrity Threat* – Incorrect modification of information, *Denial of Service (DoS) Threat* – Access to a system resource is blocked. Threats can be classified as: Physical or Logical Threat, Accidental or Deliberate Threat, Active or Passive Threat. Vulnerabilities are some characteristics of computer systems that make it possible for a threat to occur. Vulnerabilities are weakness discovered in operating systems, applications and devices by hackers, security professionals and organizations. Most of all attacks result from known vulnerabilities and Misconfigurations. Common Vulnerabilities include: Misconfigurations and Human Error, Vulnerable Operating Systems, Unsecured and Unnecessary Network Services, Unprotected files, Databases, Applications, Physical Access, Eavesdropping, Sniffing, Weak Passwords etc.

II. CYBERCRIME DEFINITIONS

Threat Defining Cybercrime is very important and challenging. Defining Cybercrime is not easy, the difficulty lies in what crimes should be considered as Cybercrimes. The terms Cybercrime, Computer Crime, Information Technology Crime, and High-tech Crime refer to crimes committed with, via, or by computer and other electronic media. Cybercrime is a new form of crimes which involves the use of a computer as the primary instrument to facilitate the crime and targets Computer Networks themselves. Various terms are used to define Cybercrime. There are number of different definitions of the term Cybercrime. [1-2]

Cybercrime as crime committed over the Internet. Cybercrime as any crime that is committed by means of special knowledge or expert use of computer technology. Cybercrime is the use of computers and networks used to harass victims or set them up for violent attacks, even to coordinate and carry out terrorist activities that threaten us all. Cybercrime is the criminal offenses committed using the Internet or another Computer Network as a component of the crime. Cybercrime is knowingly accessing a Computer, Computer Network, or Computer System without the effective consent of the owner. Altering, damaging, deleting, or otherwise using computer data to execute a scheme to defraud; deceiving, extorting, or wrongfully controlling or obtaining money, property, or data; using computer services without permission; disrupting computer services; assisting another in unlawfully accessing a computer; or introducing contaminants into a system or network, constitutes Cybercrime. Cybercrime is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. Cybercrime is unlawful acts wherein the computer is

either a tool or a target or both. Cybercrime is any unauthorized act deemed to be illegal involving computer equipment perpetrated through the medium of the Internet. Cybercrime is any illegal, unethical, or unauthorized behavior involving the transmission or automatic processing of data. [3-5]

III. CYBERCRIME TYPES

Threat There are several ways to categorize the various Cybercrimes. Cybercrimes can be classified as: Violent Cybercrimes and Non Violent Cybercrimes, Cybercrimes against Individual, Property, Organization and Society, Cybercrimes where Computer or Network as Target, as Tool, for Incidental Purposes, Cybercrimes against the Confidentiality, Integrity and Availability of Computer Data and Systems, Computer Related, Content Related and Copyright Related Cybercrimes, Privacy Related, Content Related, Intellectual Property Related and Economic Cybercrime.

Cyberterrorism: Terrorism committed, planned, or coordinated in cyberspace, via Computer Networks. It is politically motivated attacks against the state. Cyberterrorism is the convergence of cyberspace and terrorism. "Cyberterrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non combatant targets". [6] *Assault by Threat*: Threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for such as employees or communities through the use of a Computer Network such as email, videos, or phones. *Cyberstalking*: It is a form of electronic harassment, often involving express or implied physical threats that create fear in the victim and that could escalate to real life stalking and violent behavior. *Online Sex Offences:* Globalization and the widespread use of the technological advances particularly advancements in the Computer and Internet which have become the most important elements of modernization, given birth to the emergence of different and novel forms of crimes like Child Pornography, Human Trafficking, Child Trafficking, Cyberprostitution. *Child Pornography*: Child Pornography as Cybercrime is the use of Computers and Networks for, creating pornographic materials using minor children, distributing these materials and accessing them. Child pornography is the record of sexual abuse against a child. It can be a visual, descriptive or audio depiction of a child engaged in sexual activity with an adult, other children or sometimes an animal. [7,8] *Human Trafficking*: Human beings Trafficking constitutes a violation of human rights and is an offence to the dignity and the integrity of the human being. Human Trafficking is the modern form of the old worldwide slave trade involving use of IT's. It treats human beings as a commodity to be bought and sold. The victims are put to forced labor, usually in the sex industry. *Child Trafficking*: Child Trafficking is a form of human trafficking and is the recruitment, transportation, transfer, harboring, or receipt of children for the purpose of exploitation. Child Trafficking also refers to any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration. Global statistics indicate that most of the children involved in the Pornography are already victims of Child Trafficking within and outside states. *Cyberprostitution*: Use of computer for Advertising / soliciting prostitution services over the Internet. *Cybertrespass*: Is accessing a computer's or network's resources without authorization but not misusing or damaging the data there. *Cybertheft*: There are many different forms of Cybertheft, or ways of using a Computer and Network to steal information, money, or other valuables. Cybertheft offenses include: Embezzlement, Unlawful Appropriation, Cyber Espionage: Economic / Corporate / Industrial, Infringement of Intellectual Property Right (Patents, Trademarks, Designs, Copyright, Plagiarism, Piracy), Identity theft, Acquiring Personal Information, DNS Cache Poisoning.[9] *Embezzlement*: Involves misappropriating money or property for your own use that has been entrusted to you by someone else. *Unlawful Appropriation*: Differs from embezzlement in that the criminal was never entrusted with the valuables but gains access from outside the organization and transfers funds, modifies documents giving him title to property he doesn't own. *Cyber Espionage*: Economic / Corporate / Industrial: Persons inside or outside a company use the network to steal trade secrets, financial data, confidential client lists, marketing strategies, or other information that can be used to sabotage the business or gain a competitive advantage. *Infringement of Intellectual Property Right*: The standard legal definition of Intellectual Property as provided by the World Intellectual Property Organization (WIPO) is the "Intellectual Property protects products of the human mind, such as inventions, literary and artistic works, symbols, names, images, and designs used in commerce. Intellectual property comprises the areas of Patents, Trademarks, Industrial Designs, Geographic Indications of Source and Copyright, which includes literary and artistic works. Rights related to copyright include those of performing artists in their performance, producers of phonograms in their recordings, and those broadcasters in their radio and television programs". *Plagiarism*: The theft of someone else's original writing with the intent of passing it off as one's own. *Piracy*: The unauthorized copying of copyrighted software, music, movies, art, books, and so on, results in loss of revenue to the legitimate owner of the copyright. *Identity theft*: The Internet is used to obtain a victim's personal information, such as Social Security Number and driver's license numbers, in order to assume that person's identity to commit criminal acts or to obtain money or property or use credit cards or bank accounts belonging to the victim.[10] *Acquiring Personal Information*: Using sophisticated means, Identity (ID) thieves can acquire victims' personal information for their own purpose from online news providers. ID thieves make use of Directory Harvest Attacks (DHAs) and launch

the attacks against online news providers with two possible attack methodologies. One Email Address as Login ID/Username and Password Login and two Forwarded HTML Newsletters. [11, 12] *DNS Cache Poisoning*: A form of unauthorized interception in which intruders manipulate the contents of a computer's Domain Name System (DNS) cache to redirect network transmissions to their own servers. *Cyberfraud*: Generally, Cyberfraud involves promoting falsehoods in order to obtain something of value or benefit. *Phishing*: Phishing is a well known problem. Phishing attacks today are frequent and numerous. The term Phishing originated in 1996 to refer to a practice of tricking users into giving up their America On-Line (AOL) accounts to be used to distribute pirated software and other misuse. Originally the attacker would use instant messaging and purport to be an administrator from AOL. They would then ask users to provide their credentials. Later emails were used in a similar fashion. [13] *Pharming*: In Pharming fraudster steals sensitive information. Pharming directs users to fake sites, via a bogus email or more commonly a virus or piece of spyware, when they are trying to access legitimate websites. A customer logs on to the website, often using the web address they have stored in their internet explorer favorites folder, and is unknowingly redirected to a fraudulent site. It is possible for viruses to swap all of the websites in your favorites list to scam sites.[14] *Cross Site Scripting (XSS):* Cross Site Scripting represents the combination of Phishing and Pharming, which applies a more technical dimension to a traditional crime of deception using the Internet. The cyber criminal is able to exploit vulnerabilities in website design code to allow them to steal passwords and login codes. The crucial difference between traditional Phishing - Pharming and Cross Site Scripting is that the site used to steal information is legitimate and not a spoof or copy.[15]

Destructive Cybercrimes: Destructive Cybercrimes include those in which network services are disrupted or data is damaged or destroyed, rather than stolen or misused. These crimes include: Hacking / Cracking, Social Engineering, Malware or Malicious Code, Denial of Service attack, Distributed Denial of Service Attack.

Hacking/Cracking: The term hacking and cracking are used interchangeably. Hacking is breaking into computers and computer networks, either for profit or motivation by the challenge. Cracking is breaking into other people's computer systems to cause harm. Hacking into a network and deleting data or program files and hacking into a Web server and vandalizing Web pages.[16] *Social Engineering*: Social engineering exploits human weaknesses like carelessness, the desire to be cooperative to gain access to legitimate network credentials. The talents that are most useful to the intruder are a charming or persuasive personality or a commanding, authoritative presence. Social engineering is defined as obtaining confidential information by means of human interaction. *Malware or Malicious Code*: Malware, or Malicious Code, is software designed to infiltrate or damage a computer system, without the owner's consent. The term is perhaps a combination of "mal" from "malicious" and "ware" from "software", and describes the intent of the creator, rather than any particular features. Malware is commonly taken to include: Viruses, Worms, Trojan Horses, Spyware, Adware, Keyloggers, Botnets, and Rootkits. [17] *Viruses*: Virus can be defined as "A program that infects other computer programs and systems by attaching itself to a host program in the target system, executes when the host program is executed, and spreads by cloning itself, or part of itself, and attaching copies to other host programs on the system or network". Much like human viruses, computer viruses can range in severity; some viruses cause only mildly annoying effects while others can damage your hardware, software, or files. *Worms*: A worm is similar to a virus by its design, and is considered to be a sub class of a virus. Worms spread from computer to computer, but unlike a virus, have the ability to travel without any help from a person. A worm takes advantage of file or the information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its ability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge and devastating effect. *Trojan Horses*: A Trojan (or Trojan Horse) is an apparently harmless or legitimate program inside which malicious code is hidden; it is a way to get a virus or worm into the network or computer. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. When a Trojan is activated on your computer, the results can vary. *Spyware*: "Spyware is malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user". Spyware is a type of program that watches what users do with their computer and then sends this information to a hacker over the Internet. *Adware*: Adware is software integrated into or bundled with a program. Adware is primarily advertising supported. Adware often takes is a form of Spyware, in which information about the user's activity is tracked, reported, and often resold, typically without the knowledge or consent of the user. *Keyloggers*: Keystroke logging or keylogging is a diagnostic used in software development that captures the user's keystrokes. Keylogging is providing a means to obtain passwords or encryption keys and thus bypassing other security measures. Keyloggers can be distributed as a Trojan horse or as part of a virus or worm. Keyloggers are widely available on the Internet and can be used by anyone for these illegal purposes. *Botnet*: Botnet is jargon for a collection of software robots, or bots, which run autonomously. Botnet is any group of bots that refer to a collection of compromised machines running programs (malware) under a common command and control infrastructure. A botnet's originator can control the group remotely. Most botnets are developed for organized crime where doing targeted attack to gain money. A bot typically runs hidden. Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. [18]

Rootkits: A Rootkit is a set of software tools frequently used by an intruder after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge. Rootkits are known to exist for a variety of operating systems. A computer with a Rootkit on it is called, a rooted computer.

Denial of Service Attack: Brings down the server or prevents legitimate users from accessing Network resources. A type of Network attack, where a maliciously generated traffic aims at consuming the resources of a server, thus preventing valid traffic from reaching the machine, which regular users experience as denying the service that the server should provide.

Distributed Denial of Service Attack : Distributed Denial of Service Attack is a form of DoS attack, but performed using multiple computers, which then focus the malicious traffic on a victim server, consuming its bandwidth. In most cases, these computers are controlled remotely by hackers and are connected in so called Botnets. Such computers are also called Zombies.

Other Cybercrimes: There are many more nonviolent varieties of Cybercrime. Again, many of these only incidentally use the Internet to accomplish criminal acts that have been around forever. Some examples include: Internet Gambling, Internet Drug Sales, Cyberlaundering, and Cybercontraband.

Internet Gambling: Gambling over the Internet. The gambling service providers use illegally credit cards, debit cards, electronic fund transfers electronic for payment of gambling. *Internet Drug Sales*: Illegally selling drug through the internet. *Cyberlaundering*: Using electronic transfers of funds to launder illegally obtained money. *Cybercontraband*: Transferring illegal items, such as encryption technology that is banned in some jurisdictions, over the Internet.

IV. CONCLUSION

Preventing Cybercrime need application of techniques and tactics, legal and regulatory system, peer pressure, existing and emerging technologies. Immediate detection and complete information of incident to minimize the harm done and maximize the chances of identifying and successfully prosecuting the Cybercriminals requires some response mechanism. The only effective way to curb Cybercrime is collaboration, sharing knowledge and expertise in different areas of Cybercrime.

REFERENCES

[1] Brenner S. (2007) “Cybercrime: re-thinking crime control strategies” in Jewkes, Y (ed) Crime Online, London: Willan Publishing
[2] Debra Littlejohn Shinder (2002) “Scene Of Cybercrime: Computer Forensics Handbook”
[3] Sinrod E. J., Reilly W. P. (2004), "Cyber crimes: a practical approach to the application of federal computer crime laws", Santa Clara Computer & High Tech Law.
[4] Watson Business Systems Ltd “A guide to computer crime”, http://legal.practitioner.com
[5] Mcafee (2007) "Cyber Crime: A 24/7 Global Battle", http://www.mcafee.com
[6] Foltz C. B. (2004) “Cyberterrorism, computer crime, and reality.” Information Management & Computer Security
[7] McLaughlin J. (2004). “Cyber Child Sex Offender Typology.” http://www.ci.keen.nh.us
[8] Salter A. (2003) “Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Ourselves and Our Children.” New York, NY: Basic Books.
[9] Ben-Itzhak Y. (2009) "Organised cybercrime and payment cards", Card Tech Today
[10] Diller-Haas A. (2004) “Identity theft: It can happen to you.” The CPA Journal,
[11] Clyman J. (2004). “Understanding Directory Harvest Attacks; ever wonder how spammers got your carefully guarded e-mail address?” PC Magazine.
[12] Shaffter G. “Good and Bad Passwords How-To: Password Cracking Goals, Techniques and Relative Merits and Cracking Times of Different Techniques.”, http://geodsoft.com
[13] Grigg I. (2005) “GP4.3 - Growth and Fraud - Case #3 – Phishing.” http://www.financialcryptography.com
[14] Dhamija R., Tygar J.D. (2005) “The Battle Against Phishing: Dynamic Security Skins”
[15] Anti-Phishing Working Group. (2004) “Phishing Attack Trends Report.” http://www.antiphishing.org
[16] Harvey B. (2004). “Computer hacking and ethics.” University of California, Berkeley. http://www.cs.berkeley.edu
[17] Aaron G., Bostik K. (2008) "Protecting the web: Phishing, malware, and other security threats", Proceeding of the 17th International Conference on WWWeb 2008
[18] Ken Dunham and Jim Melnick.(2009) “Malicious Bots, an inside look into the cyber-criminal undergroun of the Internet.” Taylor & Francis Group, LLC.