Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2016 = 6.17, www.srjis.com
UGC Approved Sr. No.49366, MAR–APR, 2018, VOL- 5/44

CYBER CRIME AND ITS IMPACT

Rupali Sharma, Ph. D.

Asst. Professor, College of Law, IPS Academy, Indore (M.P.)

E-Mail -: drrupalisharma@rediffmail.com

Abstract

The subject of this research paper is Cyber Crime and its Impact that deals with the aspects of our life and economic growth of the country as well. The aim of this paper is to provide the thrust areas and impact of cyber crime with changing scenario of latest technologies .This paper tries to address the basic and infrastructural problems and glitches as well with suggesting appropriate options to be implemented

Computer crime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Netcrime** refers to criminal exploitation of the Internet Cybercrimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

Topology

Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers directly; (2) crimes facilitated by

computer networks or devices, the primary target of which is independent of the computer network or device. Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Crimes that use computer networks or devices to advance other ends include:

- Cyberstalking
- Fraud and identity theft
- Information warfare
- Phishing scams

Spam: Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful in some jurisdictions. While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time. **Fraud:** Main article: Computer fraud Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss] In this context, the fraud will result in obtaining a benefit by:

- Altering computer input in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions: this is difficult to detect;
- Altering or deleting stored data;
- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.

A variety of Internet scams target consumers direct.

Obscene or offensive content: The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.

Over 25 jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

Harassment: Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyber bullying, cyber stalking, harassment by computer, hate crime, Online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

There are instances where committing a crime, which involves the use of a computer, can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, Kramer was served an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3)[8] for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct."

Connecticut was the first state to pass a statute making it a criminal offense to harass someone by computer. Michigan, Arizona, and Virginia have also passed laws banning harassment by electronic means. Harassment by computer statutes are typically distinct from cyberbullying laws, in that the former usually relates to a person's "use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act," while the latter need not involve anything of a sexual nature.

Threats: Although freedom of speech is protected by law in most democratic societies (in US this is done by First Amendment) that does not include all types of speech. In fact spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate", that also applies for online or any type of network related threats in written text or speech. The US Supreme Court definition of "true threat" is "statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group".**Drug trafficking:** Drug traffickers are increasingly taking

advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

Cyber terrorism: Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyberextortion is a form of cyberterrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

Cyber warfare: Sailors analyze, detect and defensively respond to unauthorized activity within U.S. Navy information systems and computer networks

The U.S. Department of Defense (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

Documented cases: One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.

A hacking group called MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bell suffered losses of $370,000 alone. In 1983, a nineteen year old UCLA student used his PC to break into a Defense Department international communications system.. Between 1995 and 1998 the Newscorp satellite pay to view encrypted SKY-TV service was hacked several times during an on-going technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek re-runs in Germany; which was something which Newscorp did not have the copyright to allow. On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and copy of the virus via e-mail to other people.

In February 2000 a individual going by the alias of Mafia Boy began a series denial-of-service attacks against high profile websites, including Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged Mafia Boy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.

The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad". It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with an individual activities earning up to $150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet.

On 2 March 2010, Spanish investigators arrested 3[] in infection of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.

In August 2010 the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members, and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide. On March 1, 2011 at Lassiter High School, two students were accused of impersonation of a staff member via cybercrime, but both claimed they were uninvolved. The offense was made a felony in the Cobb County School District two months after the impersonation had happened. Shortly afterwards, the head of the LHS School Board said "The teacher just wouldn't do this at all". The case ended on May 9, and no evidence was found.

References

^ *Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.*

^ *Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.*

^ *David Mann And Mike Sutton (2011-11-06). ">>Netcrime". Bjc.oxfordjournals.org. Retrieved 2011-11-10.*

^ * *Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9*

^ *Internet Security Systems. March-2005.*

^ *"Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow'S Battlefield". Law.duke.edu. Retrieved 2011-11-10.*

^ *See, e.g., Telephone Consumer Protection Act of 1991, Do-Not-Call Implementation Act of 2003, CAN-SPAM Act of 2003.*

^ *"2011 U.S. Sentencing Guidelines Manual § 2G1.3(b)(3)".*

^ *[1][dead link]*

^ *"Section 18.2-152.7:1". Code of Virginia. Legislative Information System of Virginia. Retrieved 2008-11-27.*

^ *[a] [b] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010, pp. 91*

^*http://www.eresecurity.ca/PDF/Cyberextortion%20by%20DoS,%20Risk%20Magazine%20June%202006.pdf*

^*http://www.carlisle.army.mil/DIME/documents/War%20is%20War%20Issue%20Paper%20Final2.pdf*

^ *[a] [b] [c] Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.*

^*David Mann And Mike Sutton (2011-11-06). ">>Netcrime". Bjc.oxfordjournals.org. Retrieved 2011-11-10.*

^ *"A walk on the dark side". The Economist. 2007-09-30.*

^ *"DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children". Dhs.gov. Retrieved 2011-11-10.*