SJIF 2014 = 3.189
ISSN: 2348-3083
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL FOR HUMANITY SCIENCE & ENGLISH LANGUAGE

CYBER CRIME AND CYBER TERRORISM ARE CONCERNS FOR EVERY SECTOR

Dr. Veena Devi Trivedi

Abstract

Cyber Crime *is the use of Internet attacks in criminal activities, including acts of deliberate, large-scale disruption of computer networks, especially computers of personal use attached to the Internet, by the means of tools such as computer viruses. Cyber terrorism is a dual meaning term. Some authors choose a very narrow definition, relating to terrorist activities, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyber terrorism.Cyber terrorism can also be understood as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this can be seen as a form of terrorism. There is much concern from government, public and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies. Several minor incidents of cyber terrorism have been documented.*

Key Words: Issues, Cyber, Crime, Terrorism

1:Introduction:

1.1: What is a Cyber Crime?

Computer crime or **cyber crime**, is any crime that involves a computer and a network.

"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)".

- Dr. Debarati Halder and Dr. K. Jaishankar (2011)

Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.(Wikipaedia)

The computer is used in conducting crime, or it may be the target.

Net crime is use of internet in conducting any crime or criminal activities.

2: Classification of Cyber Crime:

Computer crime covers a broad range of activities;

2.1: Cyber Fraud and Financial Crimes:

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 in an unauthorized way;
- 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;
- Facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.
- A variety of internet scams may be based on what is called Phishing as well as Social Engineering target direct to consumers, however,
- Businesses are also susceptible to these scams.

2.2: Cyber Extortion: Cyber extortion is 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, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. An example of cyber extortion was the attack on Sony Pictures of 2014. 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.

2.3: Cyber Warfare

Sailors analyze, detect and defensively respond to unauthorized activity within naval information systems and computer networks. 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 war fighting military commanders in the future.

2.4: Computer as a Target: These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have - which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. Crimes that primarily target computer networks or devices include:

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

2.5: Computer as a Tool: When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace or apprehend.

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

- Fraud and identity theft
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

2.6: Cyber 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 legal. 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.

2.7: Cyber Harassment: Cyber harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation.

A. cyber bullying,
B. cyber stalking,
C. on line predator and
D. stalking

Harassment as defined is typically distinct from cyber bullying, 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.(Wikipaedia).

2.8: Cyber Threats: Although freedom of speech is protected by law in most democratic societies .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".

2.9: Cyber Drug Trafficking: 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.

3.1: Who is a Terrorist?

Someone who uses violence, mayhem, and destruction — or the threat of those things — to coerce people or countries into taking a certain action is a terrorist.

A *terrorist* may be motivated by religious fervor, politics, or just plain old-fashioned greed.

Terrorist has at its root the word "terror," which comes from the Latin word *terrorem*, meaning great fear. Great fear is exactly what terrorists hope to create so they can manipulate the situation to their benefit. The label *terrorist* is a subjective one.

3.2:Who is a Cyber Terrorist?

A cyber-terrorist is a criminal who uses computer technology and the Internet, especially to cause fear and disruption. Some cyber-terrorists spread computer viruses, and others threaten people electronically. When a crime involves computers, particularly a crime that terrorizes, or threatens real harm or significant disruption, its perpetrator is a cyber-terrorist. Cyber-terrorists might have ideological or religious reasons for wanting to terrorize, and others do it for personal gain. While this kind of crime is new and rare, governments fear that cyber-terrorists could disrupt a country's economy in the near future. The prefix *cyber* is used here because the terrorist attacks or uses technology.

3.3: Cyber Terrorism: Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. 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 cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or 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).

3.4: Issues in Cyber Terrorism: Cyber terrorism is also the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this can be seen as a form of terrorism. There is much concern from government, public and print or electronic media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies. Several minor incidents of cyber terrorism have been documented. As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyber terrorism. As well there are also hacking activities directed towards people within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining people's lives, robberies, blackmailing etc. Cyber terrorism is the use of internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks. Cyber terrorism is a controversial concept. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption

attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any events of cyber terrorism.

3.5: Prevention of Cyber Terrorism & Cyber Crime for a Harmonious Society: Cyber terrorism can be prevented up to certain extent by,

1. Establishing Business Continuity and Disaster Recovery Plans
2. Encouraging Research and Development
3. Pursuing and Prosecuting the Perpetrators
4. Cooperating with Various Firms and Working Groups
5. Developing Best Security Practices
6. Increasing Security Awareness
7. Framing Strict Cyber Laws
8. Becoming Proactive in this regard
9. Deploying Vital Security Applications

References:

http://en.wikipedia.org/wiki/Computer_crime.Retrieved on 9th April 2015.

David Mann And Mike Sutton (2011-11-06). "Netcrime". Bjc.oxfordjournals.org. Retrieved 07th Oct 2015.

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

"Cyber Warfare And The Crime Of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield". Law.duke.edu. Retrieved on 01 Oct 2015.

"Sex,Lies and Cybercrime Surveys". Microsoft. 2011-06-15. Retrieved 02 Oct 2015.

"Future Crimes". Retrieved 8 Oct 2015.

http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154.Retrieved on 07th Oct 2015

1.