CYBER TERRORISM

Bhawana

Asst.Prof. in Comp.Sci.,C.R.M. Jat College,Hisar, (India)

ABSTRACT

It is more than obvious that the way of conducting terrorism with the time is becoming more sophisticated. The cyber terrorism is real threat to fast technology developement. As internet usage is growing daily the world is coming closer. The world wide web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. Making the internet safer (and protecting internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. Implementing security involves assessing the possible threats to one's network, servers and information. This developing world of information technology has a negative side effect. It has opened the door to antisocial and criminal behavior. To understand cyber terrorism it is important to look at its background, to see how the terrorist organizations or individuals are using the advantage of new technology and what kind of measures governments and international organizations are taking to help the fight against cyber terrorism.

Keywords: Attack, Cyber , Dos, Systems, Terrorism

I. INTRODUCTION

The cyber terrorism as a concept has various definitions, mostly because every expert insecurity has its own definition. This term can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This may include the use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructure, and to exchange information and perform electronic threat. The threat of terrorism has posed an immense challenge in the pothreat can manifest itself in many ways, such as hacking computer systems, programming viruses and worms, Web pages attack, conducting denial of service (DoS) attacks, or conducting terrorist attacks through electronic communications. More common are claims that cyber terrorism does not exist and that actually it is a hacking and malicious attacks. Those who support these claims do not agree with the term "terrorism" because if we take into account the current technologies for prevention and care, the likelihood of creating fear, significant physical damage or death among population using electronic means would be very small. Considering the fact that the terrorists have limited funds, cyber attacks are increasingly attractive, because, their implementation requires a smaller number of people and certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to remain unknown, because they can be very far from the place where the act of terrorism is committed.

The articles envisages an understanding of the nature and effectiveness of cyber attacks and highlight what more could be done. The article is structured as given below:

- ♦ Definition of Cyber Terrorism
- ♦ Cyber Crime

  - Types of Cyber crime
  - Cyber Crime in Modern Society
  - How to Tackle Cyber Crime
- Cyber Security
- Recommendations

II. DEFINITION OF CYBER TERRORISM

Although there are a number of definitions which describe the term terrorism, one of the definitions that are frequently encountered is that terrorism is

"the unlawful use or threatening use of force or violence by a person or an organized group against people or property with the intention of intimidating or forcing societies or governments, often for ideological or political reasons."

Interactions between human motives and information technology for terrorist activities in cyberspace or in the virtual world can be addressed as cyber terrorism. Yet this is the definition of cyber terrorism that Sarah Gordon and Richard Ford from Symantec have used in their efforts to define "pure Cyber terrorism."

III. CYBER CRIME

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. However, before you can understand more about this system, let us find out more about cyber crimes.

3.1. Types of Cyber Crimes

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

3.1.1 Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

3.1.2 Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

3.1.3 Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

3.1.4 Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

3.1.5 Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

3.1.6 Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

3.2. History of Cyber Crime

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became more skillful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

3.3 Cyber Crime in Modern Society

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

3.4 Categories of Cyber Crime

Cyber crimes are broadly categorized into three categories:-

3.4.1. Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

3.4.2 .Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

3.4.3. Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

3.5. How to Tackle Cyber Crime

It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.

The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

Cross Domain Solution offers a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed. This security solution can be used by commercial and governmental organization to ensure an impenetrable network while still making sure that users can get access to the required information easily.

IV. CYBER SECURITY

Cyber security comprehensively refers to the set of safeguarding measures intended to maintain integrity of information as it passes through heterogeneous networks and becomes vulnerable to malicious attacks from viruses and scripts. It strategically deals with checking user identity, associated risks and incident management. It is structurally composed of processes, technologies and practices devised to optimally mitigate the risks to computers, programs and networks.

Extremely sensitive data like defense information needs to be critically protected from unauthorized access to prevent harmful tampering, corruption and misrepresentation.

An individual user can implement checks to thwart unwanted manipulation of his data by continually updating the antivirus program, putting strong passwords and strictly guarding personal information over networks that are not trusted.

Cyber-security is intimidated by rapidly and regularly evolving nature of risks. The conventional wisdom of devoting the bulk of resources on the most critical system aspects to safeguard against formidable threats, while leaving minor components unprotected cannot be justified in the present scenario. The threat is accelerating at a pace that is beyond control and is significantly deviating from set norms. An adaptive and proactive system is being fostered to regularly monitor and assess real time the emerging threats.

Cyber-security is meant for proactive detection of loopholes in the security policies of the computer systems which can be exploited by people engaged in information warfare to seek entry in critical system to alter, destruct or hold government to ransom by threatening to damage sensitive information infrastructure. Critical information should not be leaked to unauthorized people. A truly secure network will maintain the integrity of data stored in it and also allow government to access and regularly supervise the entire array of information in it.

Cyber-security or cyber assurance defines the mechanism to extend operational support for management and protection of networks, data and information. It also has provision for contingency support to facilitate safeguarding of cyber-dependent operations. The stress is on predicting potential cyber-attacks by simulating real time operating environment to understand the approach of intrusive elements and deter them. It calls for deployment of resources to backup critical information and survive any cyber-attack. The augmented operational capabilities will give a proactive response to any attempt of unauthorized access to information.

Cyber-security tactics recognize the fact that attacking a system is easier than defending it. The compromise of a system is contingent on the understanding gained by the hacker of a part of the system's technical architecture. The defenders however need to comprehensively analyze the entire infrastructural set-up and learn the specific needs of the managing organizations to better protect the system from internal and external attackers.

4.1. The Challenges Confronted by Cyber-Security Experts are

4.1.1. Multiple security models: A majority of large organizations need to manage numerous domains or data centers. Mostly, the management of such elements is entrusted to different enterprises and consequently there is no central cyber security governance mechanism. The situation can be simplified by implementing standardized processes as the management of heterogeneous architectures (application and infrastructure) makes things complicated.

4.1.2. Continuity of Operations: This has become complex owing to growing data center consolidation leaving little scope for redundant operations. The increasing architectural standardization has paved way for larger cross domain vulnerability. Besides, the shrinking numbers of regional 'continuity of operations' hubs has rendered it more fragile from network communications scenario.

4.1.3. Coordinated Help Desk: The demand for coordinated help desk operations deployed across organizations is on the rise after the scope of cyber security is getting clear. Coalition partners and related organizations have developed greater dependency on one another in respect to earlier times. However, the challenge of building a coordinated help desk has not been adequately addressed so far with the operations limited to particular domains and restricted to propagation of generalized threat/ incident reporting scenario only.

4.1.4. Social Engineering: It refers to activity category that concerns itself with combating non-traditional and non-security attacks and compromises. It can be deployed from internal or external perspective with the objective of exploiting inherent system weaknesses pertaining to security policies which paves the way for consequent technical exploitation.

4.1.5. Unstructured Data Security: Organizations have gradually moved from paper records to electronic versions. A majority of the data circulating within the organization is to an extent unstructured. Structure data sources can be covered with data security policies meant for formal record management. However unstructured data like emails, wikis etc. are less secure as unstructured data management policies have not fully evolved as yet.

V. RECOMMENDATIONS

Certain recommendations are given below:

(a) Need to sensitize the common citizens about the dangers of cyber terrorism. Cert-in should engage academic institutions and follow an aggressive strategy.

(b) Joint efforts by all Government agencies including defence forces to attract qualified skilled personnel for implementation of counter measures.

(c) Cyber security not to be given more lip service and the organisations dealing with the same should be given all support. No bureaucratic dominance should be permitted.

(d) Agreements relating to cyber security should be given the same importance as other conventional agreements.

(e) More investment in this field in terms of finance and manpower.

(f) Indian agencies working after cyber security should also keep a close vigil on the developments in the IT sector of our potential adversaries.

VI. CONCLUSIONS

There is a growing nexus between the hacker and the terrorist. The day is not far when terrorists themselves will be excellent hackers. That will change the entire landscape of terrorism. A common vision is required to ensure cyber security and prevent cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy.

REFERENCES

[1]. S. Best, DeÞ ning Terrorism**:** http://www.drstevebest.org/Essays/DeÞ ning%20Terrorism.htm www.symantec.com/avcenter/reference/cyberterrorism.pdf

[2]. M. Cereijo Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm

[3]. R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation, Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee Washington, DC, 05 April 2001, http://www.fbi.gov/news/testimony/issue-of-intrusions-intogovernment- computer-networks

[4]. www.terror.net: How Modern Terrorism Uses the Internet, 21 February 2007: http://www.asiantribune.com/index.php?q=node/4627

[5]. R. Lemos, Cyberterrorism: The real risk, 2002: http://www.crime-research.org/library/Robert1.htm D.Briere, P.Hurley, Wireless network hacks and mods for dummies, 2005, Wiley.

[6]. M. Bogdanoski, A. Risteski, & S. Pejoski, (2012, November). Steganalysis—A way forward against cyber terrorism.